SmartData v1.4.0.0 Security Target

Common Criteria: EAL2

Version 1.1

24-NOV-2014

Document management

Document identification

Document title	SmartData v1.4.0.0 Security Target
Document version	1.1
Document date	24-NOV-2014
Document Author	Muzamir Mohamad
Document Release Authority	K.K Chia

Document history

Version	Date	Description
0.1	13-AUG-2014	Released for internal review.
0.2	25-AUG-2014	Released to CSM MySEF
0.3	1-OCT-2014	Updated to address EOR01
0.4	20-OCT-2014	Minor changes to user role name and addressed comments from CSM MySEF.
0.5	10-NOV-2014	Updated to address EOR01d2
1.0	13-NOV-2014	Changes to TOE version 1.4.0.0
1.1	24-NOV-2014	Updated to address EOR03

Table of Contents

1 Security Target introduction (ASE_INT.1)

1.1 ST reference

ST Title	SmartData v1.4.0.0 Security Target
ST Version	1.1
ST Date	24-NOV-2014

1.2 TOE reference

TOE Title	SmartData
TOE Version	1.4.0.0

1.3 Document organization

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 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. It also describes the acronym used in this documentation.

Term	Description
Authentication Data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
Java EE	Java Platform Enterprise Edition
RDBMS	Relational database management system
TDES	Triple DES is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
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.
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 resource or 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 users of the TOE access the TOE through a web browser.
User data	Data created by and for the user, which does not affect the operation of the TSF.
Audit records	An individual item of information contained in an audit trail
Rijndael	A key for encryption that has a size of 128, 192 or 256 bits, which provides high protection against brute force attacks
MRP	Material Requirement Planning. This module provides function for production product preparation. It allow user to customize the raw material needed, production process to produce a final

Term	Description
	product and manage the Job in production environment.
OMM	Order Management Module. This module provides function to purchase raw material until delivery order to the customer.
VMM	Vault Management Module. This module provides all the stock movement and information in warehouse and in production.
PPM	Production Process Module. This module provides information capture from the machine and production information from each process
Work center	Work center is an operation room that contain production process in a factory. The work center may or may not contain any machine.
QCM	Quality Control Module. This module provides different QC checking state, Incoming QC, In Production QC and Quality Assurance checking of the product
Security Items	Security items can be defined as number of chips, passport data page and raw cards
Barcode Fonts	Storing numbers printed in a way that a computer can easily read

1.5 TOE overview

1.5.1 TOE usage and major security functions

The Target of Evaluation (TOE) is SmartData version 1.4.0.0. The TOE is an engine for a web application that tracks and manages security items in a production environment. It keeps track of the quantity of the security item(s) from warehouse (processing place for all the raw materials of the security item(s)) until it becomes a final product. The system is able to keep track of the security item(s) within the boundary of the warehouse (during processing of raw materials), within the process of delivery of the security item(s), production status and security item status. These process flow and monitoring systems by the TOE is operate with the integration of the production machine.

The TOE contains 6 system modules, which are MRP, OMM, VMM, PPM, QCM and Settings. The system module(s) can be configured to operate as a single function separately (MRP, OMM, VMM, PPM and QCM) in one server. Each system module controls, manage, monitor and enforce data protection on all information related to the security item(s) from being removed in the production environment unintentionally. Furthermore, the system is able to generate product information in an encrypted format and applied it in a secure packaging for delivery processes.

The TOE was made to increase the level of monitoring on security items in a production environment by providing an end-to-end monitoring solution. The TOE is suited for use in a close network environment (ad-hoc/intranet) or open environment (hosted at DMZ) as the system is deployed using secure communication via TLS/SSL.

As data residing in the production environment is crucial, card readers are integrated with the TOE and the production machine to capture and record product information. A barcode reader is used to capture raw information that is transacted and shared from the point of a check out at the warehouse up to the check in process at each work centre during production. To ensure the information in the system is accurate, manual processes and manual checks/verification by the operator(s) have been eliminated, forwarded and handled by the TOE. Data in the system is protected based on the user roles defined in Settings module under the User Access Control.

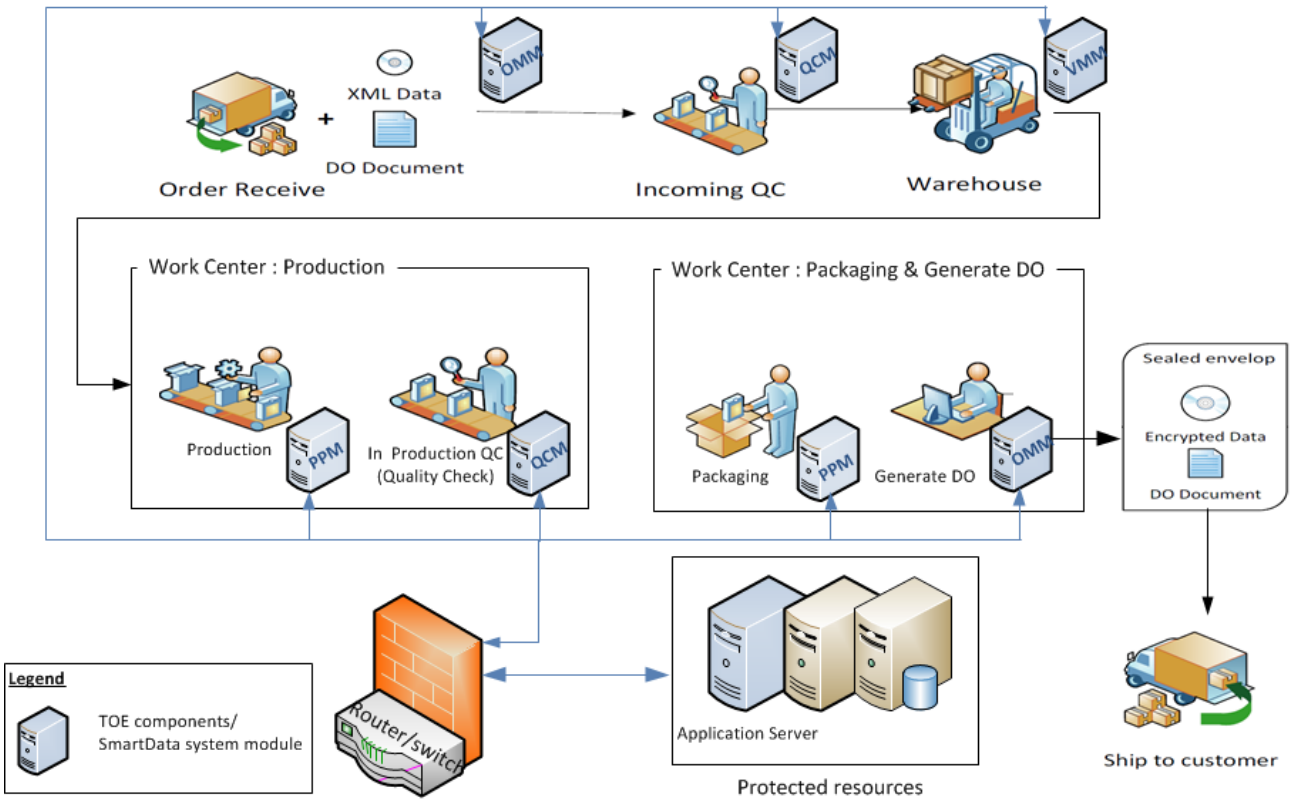

Figure 1: The TOE in a Typical Environment

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

Security function	Description
Security Audit	The TOE generates audit records for security events. The superuser is the only roles with access to the audit trail and has the ability to view the audit log in either pdf or csv files.
Identification and authentication	The TOE requires that each user is successfully identified (user IDs) and authenticated (password) before any interaction with protected resources is permitted.
Cryptographic Operation	The TOE supports TDES (192 bits) and Rijndael encryption (128 bits) method to protect against disclosure.
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 Communication	The TOE is able to protect the user data from disclosure and modification using SSL as a secure communication between users' browser and the TOE.

1.5.2 TOE Type

The TOE is an engine for a web application that manages and tracks the security items in a production environment. The TOE provides security functionality such as security audit, cryptographic operation, security management, identification and authentication and secure communication.

1.5.3 Supporting Hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
Software Prerequisite	
Operating System	Windows Server 2008
Software	• Microsoft Internet Information Services (IIS7.5) • Microsoft .NET Framework 4.0 • Microsoft SQL Server 2008 • Chrome Version 35.0.1916.153 • Note: The TOE is currently designed for google chrome browser only. • Java Version 7 Update 10
Hardware Prerequisite	
Processor (CPU)	Intel® Core™2 Quad Processors
Memory (RAM)	8 GB RAM
Storage Space (Hard disk)	1 Terabyte
Card Reader	• Contactless Card Reader - Dual Interface mode (support ISO/IEC 14443) • Contact Card Reader – Type A&B Transmission mode (support ISO/IEC 7816 and Microsoft PC/SC) Note: Support USB 2.0 and 3.0
Barcode Scanner	• USB 1D (Linear) barcode that support code 39 barcode (ISO/IEC 16388) Note: Support USB 2.0 and 3.0

1.6 TOE description

1.6.1 Physical scope of the TOE

The TOE is an engine for a web application that manages and tracks the security items in a production environment. A typical installation of the TOE can be found in Figure 2 below, which identifies the various components of the TOE architecture.

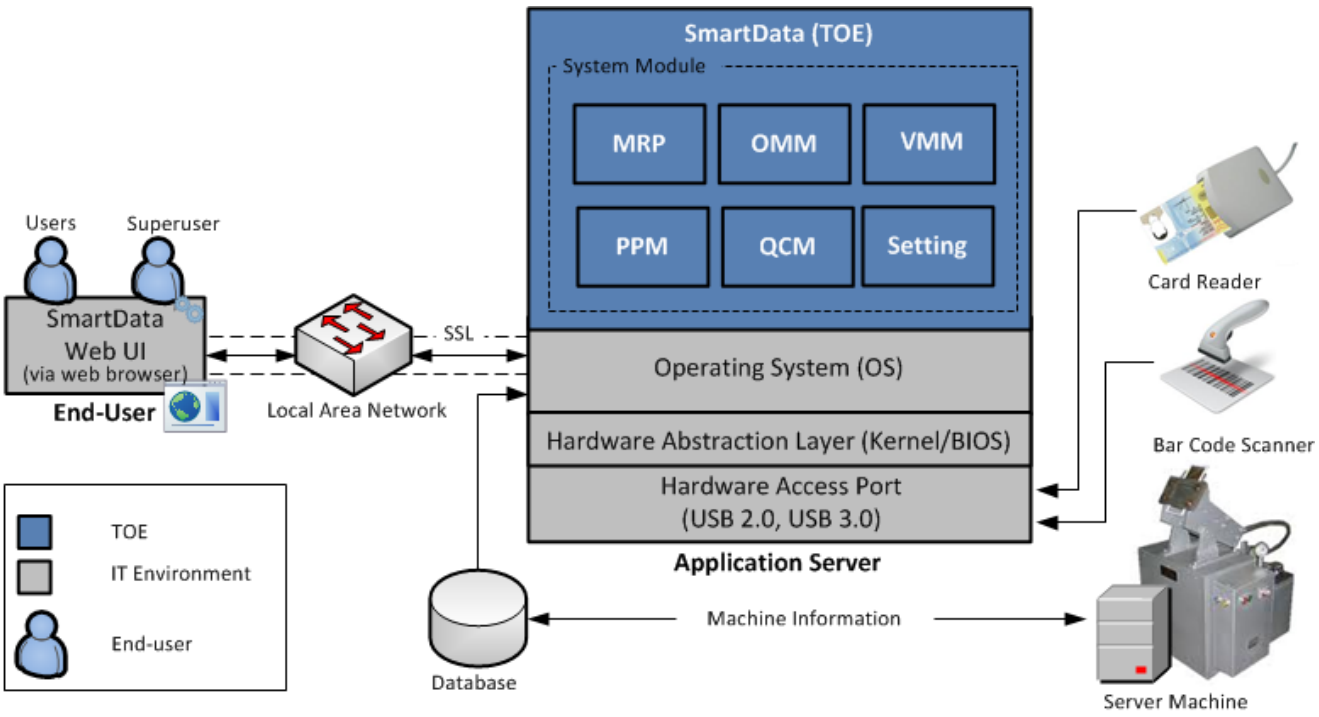

Figure 2: Physical Scope of the TOE

1.6.2 Logical scope of the TOE

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE is summarised below.

a) **Security Audit.** The TOE generates audit records for security events. The superuser is the only roles with access to the audit trail and has the ability to view the audit logs.

b) **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. The TOE checks the credentials (username and password) presented by the user at the login page against the authentication information stored in the database. Additionally, superuser or permissible users must be authenticated before performing any administrative functions.

- **Cryptographic Operations.** The TOE provides a cryptographic library that utilizes the following cryptographic algorithms/functions:

    - TDES (192 bit keys) – The TOE uses TDES key to encrypt the delivery order (DO) data. The system module OMM has the functionality to encrypt the delivery order (DO) data.
    - Rijndael Encryption (128 bit keys) – The TOE uses Rijndael encryption to encrypt user password and store it in the database.

c) **Security Management.** The TOE contains various management functions or modules to ensure efficient and secure management of the TOE. The license key determines the module users can access on SmartData. The license key only allows addition of new modules but not removal of modules. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The superuser has the ability to create users roles, assigning access privilege to user for specific functions. The functions above are restricted based on this role.

d) **Secure communications.** The TOE supports secure communications between the TOE and user's browser in order to authenticate users and access the TOE functionality. Encryption using SSL prevents modification and disclosure of this information.

2 Conformance Claim (ASE_CCL.1)

The ST and TOE are conformant to version 3.1 (REV 4) 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 (REV 4), September 2012
- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 4). Evaluation is EAL2, September 2012.

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*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.EAVESDROP	An unauthorized person may eavesdrop the communication between Client-Side and Server-side.
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_DATA	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 and management data.
T.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data.

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifier	Assumption statement
A.ADMIN	It is assumed that the superuser who manages the TOE is not hostile and is competent.

Identifier	Assumption statement
A.ENVIRONMENT	The TOE environment will provide appropriate authentication and authorisation controls for all users in the underlying environment (including the database, network, operating system and Application Server).
A.PASSWORD	It is assumed that users will keep their passwords secret and not write them down or disclose them to any other system or user. It is also assumed that the user password is between a minimum of 6 and a maximum of 30 alphanumeric characters.
A.UPDATE	The underlying platform on which the TOE operates will be updated when needed with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.
A.PHYSICAL	It is assumed that the servers hosting the application and database servers are in a secure operating facility with restricted physical access and non-shared hardware.
A.SSL_CONFIG	It is assumed that the web application has valid SSL certificates installed (not revoked or expired), and the source are from trusted certificate authorities (CAs).

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. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended 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.COMM	The TOE must ensure that TSF data traversing across the network to the application server is protected from disclosure and loss of integrity.
O.MANAGE	The TOE must allow superuser to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.PASSWORD_DATA	The TOE must ensure that passwords stored in the database are not in plaintext.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.ADMIN	The owners of the TOE must ensure that the superuser who manages the TOE is not hostile and is competent.
OE.AUTHDATA	The users of the TOE must not disclose their password that protects the TSF data.
OE.ENVIRONMENT	Those responsible for the TOE must ensure that there are appropriate authentication and authorisation controls for all users in the underlying environment (including the database, network, operating system and application Server).
OE.PHYSICAL	Those responsible for the TOE must ensure that the servers hosting the application and database servers are in a secure operating facility with restricted physical access and non-shared hardware.

Identifier	Objective statements
OE.UPDATE	Those responsible for the TOE must ensure that the underlying operating system, application server and database are updated when needed with the latest security patches and hardened to protect against known vulnerabilities and security configuration issues.
OE.SSL_CONFIG	Those responsible for the TOE must ensure that the application server has valid SSL certificates installed (not revoked or expired), and the source is from trusted certificate authorities (CAs).

4.4 Security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

OBJECTIVES / THREATS/ ASSUMPTIONS	T.EAVESDROP	T.MANAGEMENT	T.PASSWORD_DATA	T.UNAUTHORISED_ACCESS	A.ADMIN	A.ENVIRONMENT	A.PASSWORD	A.UPDATE	A.PHYSICAL	A.SSL_CONFIG
O.ACCESS		✔		✔						
O.COMM	✔									
O.MANAGE		✔								
O.USER		✔		✔						
O.PASSWORD_DATA			✔							
OE. ADMIN					✔					
OE.AUTHDATA							✔			
OE. ENVIRONMENT						✔				
OE. UPDATE								✔		
OE. PHYSICAL									✔	
OE.SSL_CONFIG										✔

4.4.1 TOE security objectives rationale

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

Threats/OSPs	Objectives	Rationale
T.EAVESDROP	O.COMM	The objective ensures that all user data from the user to the web application will be secured using SSL protecting the user data from unauthorized disclosure and loss of integrity.
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 superuser 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_DATA	O.PASSWORD_DATA	The objective ensures that all passwords stored in the database are encrypted using Rijndael encryption.
T.UNAUTHORISED_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.

4.4.2 Environment security objectives rationale

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

Assumptions	Objective	Rationale
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.ENVIRONMENT	OE.ENVIRONMENT	This objective ensures that those responsible for the TOE ensure that appropriate authentication and authorisation controls for all users in the underlying environment (including the database, network, operating system and application Server).
A.PASSWORD	OE.AUTHDATA	This objective ensures that those responsible for the TOE ensure that the user password is alphanumeric and user not discloses it to anyone else.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that those responsible for the TOE ensure that the servers that host the application and database are hosted in a secure operating facility with restricted physical access with non-shared hardware.
A.UPDATE	OE.UPDATE	This objective ensures that those responsible for the TOE ensure that the underlying operating system, application server and database are updated when needed with the latest security patches 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 application has SSL certificates installed and are valid (not revoked or expired) from trusted certificate authorities (CAs).

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 (REV 4) 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 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 are itemised in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCS_CKM.1a	Cryptographic key generation (TDES)
FCS_CKM.1b	Cryptographic key generation (Rijndael)

Identifier	Title
FCS_COP.1a	Cryptographic operation (TDES)
FCS_COP.1b	Cryptographic operation (Rijndael)
FCS_CKM.1c	Cryptographic key generation (SSL)
FDP_ACC.1	Subset access control (Web UI)
FDP_ACF.1	Security attribute based access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_SOS.1	Verification of Secret
FMT_MSA.1	Management of security attributes
FMT_MTD.1a	Management of TSF data (Settings)
FMT_MTD.1b	Management of TSF data (Password)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_TRP.1	Trusted path

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
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) [**the following auditable events:** • **User/Superuser login** • **User/Superuser logout** • **Data modification by user/Superuser**].
FAU_GEN.1.2	The TSF shall record within each audit record at last 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, [**none**]
Dependencies:	FPT_STM.1 Reliable time stamps
Note:	None

5.2.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**superuser or authorised user**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Note:	None

5.2.4 FCS_CKM.1a Cryptographic key generation (TDES)

Hierarchical to:	No other components.
FCS_CKM.1a.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Triple-DES**] and specified cryptographic key sizes [**192 bits**] that meet the following: [**RFC 2898 PKCS#5 Section 5.2**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	The TOE uses TDES keys to encrypt the delivery order (DO) data before submit it to the customer.

5.2.5 FCS_CKM.1b Cryptographic key generation (Rijndael)

Hierarchical to:	No other components.
FCS_CKM.1b.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Rijndael**] and specified cryptographic key sizes [**128 bits**] that meet the following: [**None**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	The TOE uses Rijndael encryption to encrypt user password and store it in the

	database.

5.2.6 FCS_COP.1a Cryptographic Operation (TDES)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**TDES encryption**] in accordance with a specified cryptographic algorithm [**TDES**] and cryptographic key sizes [**192 bits**] that meet the following: [**None**].
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:	None

5.2.7 FCS_COP.1b Cryptographic Operation (Rijndael)

Hierarchical to:	No other components.
FCS_COP.1b.1	The TSF shall perform [**Rijndael encryption**] in accordance with a specified cryptographic algorithm [**Rijndael]** and cryptographic key sizes [**128 bits**] that meet the following: [**None**].
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:	None

5.2.8 FCS_CKM.1c Cryptographic key generation (SSL)

Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1c.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**the cryptographic key generation algorithms supported by SSL/TLS**] and specified cryptographic key sizes [**cryptographic key sizes supported by TLS/SSL**] that meet the following: [**none**]**.**

Notes:	None

5.2.9 FDP_ACC.1 Subset access control (Web UI)

<table>
<tr><td>Hierarchical to:</td><td colspan="3">No other components.</td></tr>
<tr><td>FDP_ACC.1.1</td><td colspan="3">The TSF shall enforce the [access control SFP] on [objects listed in the table below].</td></tr>
<tr><td></td><td>Subject</td><td>Object</td><td>Operation</td></tr>
<tr><td></td><td>Superuser</td><td>Full access control to all modules</td><td>• Create and update user group
• View user group list
• Create, update and delete user
• View user list
• Assign module to user/user group
• Change user password
• Reset password
• Email Setting
• Modify account limitation
• Modify password policy selection
• View Log Action
• Full access control for modules; MRP, OMM, VMM, PMM, QCM and settings.</td></tr>
<tr><td></td><td rowspan="2">User (via user Profile)</td><td>Settings</td><td>• Create and update user group
• View user group list
• Create, update and delete user
• View user list
• Change user password
• Email Setting
• Modify account limitation
• Modify password policy selection</td></tr>
<tr><td>MRP</td><td>• View MRP Overview
• Create, update and remove Machine
• View Machines Setting
• Create, update and remove work center</td></tr>
</table>

			• View work center list • Create and update item • Upgrade item revision item and view item list. • Create and update product • Upgrade item revision product • View product list • Create, update and view production Process list • Create, update and remove product template • View product template list • Create, update and cancel Manufacturer Order • View Manufacturer list • Create, update, cancel, close and quarantine Job order • View job order list • Create Picking list
		OMM	• View OMM overview • Create, update and cancel purchase order • View purchase order list • Create, update, delete and upload order receive • View order receive list • Create , update and cancel client Contract • View client contract list • Create , update and cancel sales order • View sales order list • Create , update, cancel and print delivery order • View delivery order list • Generate and view XML • Create and update supplier • View supplier list

			• Create, update view client
		VMM	• View VMM overview • Inventory location setting • Stock Check In/ Check out • Generate report
		PMM	• View machine performance • Generate Machine Performance report • Create Manufacturer order • Create and update MO traveller • View supplier list • View, and activate/deactivate packaging setting list • Generate report
		QCM	• View IPQC list • Update IQC • Modify IPCQ • View IPQC quarantine • View, update, reject card, IPQC inspection information
	Table 1: Access Control List		
Dependencies:	FDP_ACF.1 – Security attribute based access control		
Notes:	The license key provided determines the module users can access on SmartData. The license key only allows addition of new modules but not removal.		

5.2.10 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: [**as listed 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: [**as listed in Table 1**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**as listed in Table 1**].

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
Notes:	None.

5.2.11 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:	None.

5.2.12 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.

5.2.13 FIA_SOS.1 Verification of Secrets

Hierarchical to:	No other components
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**a minimum of 6 to a maximum of 30 alphanumeric characters, case sensitive characters, symbols and prohibition of same words found in username**].
Dependencies:	No dependencies
Notes:	None

5.2.14 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 Superuser 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.

5.2.15 FMT_MTD.1a Management of TSF data (Settings)

Hierarchical to:	No other components
FMT_MTD.1a.1	The TSF shall restrict the ability to **[*modify, delete, [Create, update, assign]*]** the [**Access Control Lists in table 1, mapping of users to user group, user ID**] to [**Superuser**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.16 FMT_MTD.1b Management of TSF data (Password)

Hierarchical to:	No other components
FMT_MTD.1b.1	The TSF shall restrict the ability to [***change_default, modify, [Update]***] the [**User Password**] to [**user (all users) and Superuser (all users)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.17 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 group** **b) creation of users with default passwords** **c) reset password** **d) deletion of users/group**

	e) changing of passwords **f) management of Access Control lists** **g) report generation**]
Dependencies:	No dependencies.
Notes:	None.

5.2.18 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**users and Superuser**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	Superuser (ability to view the audit records, configuration the system login attempt fail, manage users and user accessibility). Refer also the access control list in table 1 section 5.2.9.

5.2.19 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 on the architecture of the TOE, to understand the security behaviours.

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 attackers with 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
	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

Assurance class	Assurance components
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security requirements rationale

5.4.1 Dependency rationale

The table below demonstrates the mutual supportiveness of the SFRs 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 of EAL2, as defined in the 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
FAU.GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform.
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control	FDP_ACC.1
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FIA_SOS.1	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 FMT_SMF.1 FMT_SMR.1
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2

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	FCS_CKM.1a FCS_CKM.4 has not been included as the TOE will only overwrite key when a new patch or version is applied.
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.1b FCS_CKM.4 has not been included as the TOE will only overwrite key when a new patch or version is applied.
FCS_CKM.1a	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1a FCS_CKM.4 has not been included as the TOE will only overwrite key when a new patch or version is applied.
FCS_CKM.1b	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1b FCS_CKM.4 has not been included as the TOE will only overwrite key when a new patch or version is applied.
FCS_CKM.1c	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1c FCS_CKM.4 has not been included as the TOE will only overwrite key when a new patch or version is applied.
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
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.ACCESS	FDP_ACC.1	The requirement helps meet the objective by identifying the objects and users subjected to the access control policy.
	FDP_ACF.1	The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy.
	FAU_GEN.1	The TOE ensures audit information is generated to indicate authorised and unauthorised access of every user.
	FAU_SAR.1	The TOE ensures audit information can be read by the authorised users.
	FCS_COP.1a	The requirement helps to meet the objective by encrypting the delivery order (DO) data using TDES before they are send to the customer
	FCS_CKM.1a	The TOE allows the generation of the cryptographic keys in accordance with a specified cryptographic key generation algorithm
O.USER	FIA_UID.2	The requirement helps meet the objective by identifying the users before any TSF mediated actions
	FIA_UAU.2	The requirement helps meet the objective by authenticating the users before any TSF mediated actions.
	FMT_SMR.1	The TOE maintains Superuser role and manages multiple user roles.
O.PASSWORD_DATA	FCS_COP.1b	The requirement helps to meet the objective by encrypting the passwords using Rijndael encryption before they are stored in the database.

	FCS_CKM.1b	The TOE allows the generation of the cryptographic keys in accordance with a specified cryptographic key generation algorithm
	FIA_SOS.1	The TOE verifies that the password supplied meets the standard for minimum and maximum length.
O.MANAGE	FMT_MSA.1	The TOE restricts the ability to modify, delete, or query the security attributes for the Authenticated User SFP to a superuser role.
	FMT_MTD.1a	This requirements helps meet the objective by allowing only the Superuser roles to create, delete, modify access control lists, and mapping users to roles and user accounts to the respective organisation database.
	FMT_MTD.1b	This requirement helps meet the objective by allowing users of all roles to change their passwords.
	FMT_SMF.1	The TOE allows the mapping of user to roles, creation of users, deletion of users, changing of passwords and management of ACLs.
	FMT_SMR.1	The TOE maintains Superuser role and manages multiple user roles.
O.COMM	FTP_TRP.1	This requirement helps meet the objective by establishing a SSL secure channel from the user's browser to the TOE, thus protecting the TSF data from disclosure and modification.
	FCS_CKM.1c	The TOE allows the generation of the cryptographic keys in accordance with a specified cryptographic key generation algorithm supported by SSL/TLS

5.4.3 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 manage and track the security items in a production environment. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

6 TOE summary specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

- **Security Audit**
- **Identification & Authentication**
- **Cryptographic Controls**
- **Security Management**
- **Secure Communications**

6.2 Security Audit

The TOE will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the event) when the following events occur (**FAU_GEN.1**):

- User/Superuser login
- User/Superuser logout
- Data modification by user/Superuser

Only Superuser has the capability to review these audit records via the web interface (**FAU_SAR.1**). Timestamps are generated for audit logs by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

6.3 Identification & 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 (Users and Superuser) identify and authenticate themselves (using username and password) before performing any TSF mediated action (**FIA_UID.2, FIA_UAU.2**). During Login function the TOE will perform encryption again on the password (**FCS_COP.1b**) that key in by the user and make comparison with the data in the database.

The TOE enforces a password policy that has 4 selections; weak, medium, strong and very strong. This mechanism is used to ensure that the TOE enforces a minimum of 6 to a maximum of 30 alphanumeric characters, case sensitive characters, symbols and prohibition of same words found in username (**FIA_SOS.1**).

6.4 Cryptographic Operations

The TOE provides a cryptographic library that utilizes the following cryptographic algorithms or functions:

- TDES (192 bit keys)

  This function is available on Order Management Module (OMM). The TOE has the ability to generate TDES (128-bit keys) (**FCS_CKM.1a**). The key will be provided by the customer to TOE administrator. The TOE uses TDES keys to encrypt the delivery order (DO) data before submit it to the customer (**FCS_COP.1a**). The customer will then use third party software to decrypt the document.

- Rijndael Encryption (128 bit keys)

  This function is available on Setting Module. The TOE has the ability to generate Rijndael keys (**FCS_CKM.1b**). The TOE uses Rijndael encryption to encrypt user password and store it in the database (**FCS_COP.1b**). The key generation for each user will be different. To generate the 16byte of the encryption key, the key format (1st 12byte of key generates using UTF8 encoding, last 4byte using Binary coded decimal).

  The TOE only perform encryption to encrypt the password that key in by the user during creating of user function and insert the encrypted password into the database. The TOE compares the credentials by checking the information presented by the user at the login page against the authentication information stored in the database.

  The TOE only performs key destruction when there is customer request or new patch or version is applied. However, after perform key destruction, all users will not able to access to the system.

6.5 Security Management

The TOE contains various management functions or modules to ensure efficient and secure management of the TOE (**FMT_SMF.1**). The license key determines the module users can access on SmartData. The license key only allows addition of new modules but not removal of modules.

Superuser role can modify the access control list and mapping of users to roles (**FMT_MSA.1**). TOE provides a suite of management functions to superuser and users. These functions allow for the

configuration of the TOE to suit the organization in which it is deployed. Additionally, management roles may perform the following tasks (**FDP_ACC.1 and FDP_ACF.1**);

- mapping user Ids to roles ,
- add, delete and edit user Ids and roles,
- delete, edit and view operation functions;
- view and download audit logs
- changing of password, and
- security settings

Superuser may assign and adjust the functions available to users; users may assign and adjust the functions based on organization's requirement(s) (**FMT_SMR.1**, **FMT_MTD.1a** and **FMT_MTD.1b**).

6.6 Secure communications

When a user accesses the TOE on their browser, by typing in the website address, 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 (**FCS_CKM.1c**).