XPORTALNET HS

SECURITY TARGET

VERSION 1.0
10-FEB-18

Document management

Document identification

Document ID	MicroEngine_EAL2_ST
Document title	xPortalNet HS Security Target
Document Version/Date	Version 1.0, 10-FEB-18

Document history

Version	Date	Description
0.1	12-JUL-17	Released for internal review.
0.2	10-AUG-17	Draft Release to certification Body
0.3	10-FEB-18	Revised Section 1, Section 4, Section 5 and Section 7
1.0	10-FEB-18	Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1) 5

1.1 ST Reference 5
1.2 TOE Reference 5
1.3 Document Organization 5
1.4 TOE Overview 6
1.5 TOE Description 11

2 Conformance Claim (ASE_CCL.1) 14

3 Security Problem Definition (ASE_SPD.1) 15

3.1 Overview 15
3.2 Threats 15
3.3 Organisational Security Policies 15
3.4 Assumptions 16

4 Security Objectives (ASE_OBJ.2) 17

4.1 Overview 17
4.2 Security Objectives for the TOE 17
4.3 Security Objectives for the Environment 17
4.4 TOE Security Objectives Rationale 18
4.5 Environment Security Objectives Rationale 20

5 Security Requirements (ASE_REQ.2) 21

5.1 Overview 21
5.2 Security Functional Requirements 22
5.3 Security Requirements Rationale 31

6 TOE Security Assurance Requirements (ASE_REQ.2) 34

6.1 Overview 34
6.2 Justification for SAR selection 35

7 TOE Summary Specification (ASE_TSS.1) 36

7.1 Overview 36
7.2 Security Audit 36
7.3 Identification and Authentication 37
7.4 Security Management 37

7.5 Secure Communication 38
7.6 Tamper Protection 39

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	xPortalNet HS Security Target
ST Identifier	MicroEngine_EAL2_ST
ST Version/Date	Version 1.0

1.2 TOE Reference

TOE Title	TOE consists of: • xPortalNet HS Server • xPortalNet HS Client • Xp-GLS5100 Controller
TOE Version	• xPortalNet HS Server v2.0.0.2 • xPortalNet HS Client v2.0.0.2 • Xp-GLS5100 Controller

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 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.2).

1.4 TOE Overview

1.4.1 TOE Usage and Major Security Functions

The Target of Evaluation is xPortalNet HS System which consists of xPortalNet HS Server, xPortalNet HS Client and Xp-GLS5100 Controller. The TOE provides a centralise management system to manage MicroEngine controller(s) and supporting device from unauthorized user access and/or physical temper on controllers or device such as access control system, alarm system, parking payment system, lift access control system and other. The TOE provides access control and manage users, controllers and card access control, where they can modify or change the Card ID and Card Serial Number. It also increased accountability by always knowing which assets are accessed when and by whom.

The TOE consists of three (3) parts:

1. **xPortalNet HS Server** – the TOE is a software that runs on Windows operating System and act as an centralise management system to manage xPortalNet HS client, controller, user and supporting device. Each user able to manage multiple controller and devices registered with the controller. TOE allow users to authenticate using the same user credential for xPortalNet HS Server and xPortalNet Client. Below are the features:

    - **20 Digits (Full DesFire 64-bit CSN and Card ID)**
      Higher Security by recording both DesFire Card Serial Number (CSN) and the Card ID (CID), with 20 digits each. This captures the Full 64-bit number. The system will track the CID with the CSN to ensure that the the card matches the full record.

    - **DesFire Security Profile Configuration**
      Full support of DesFire Security Profile Configuration in the software. This allows the user to have maximum control of the security key setting and change it whenever they want to. Programming of the cards can be done through the desktop card programming unit. Easy to operate with no local configurations required.

    - **Alarm Monitoring & Lift Controller**
      Supports up to 512 inputs / 256 outputs / 256 LED Mimic outputs with event programming. User notification can be achieved through client applications, email and SMS for maximum flexibility. Control of up to 96 floors per lift. Support multiple lobby implementations for large scale projects.

    - **CCTV Integration**
      Tightly integrated to MicroEngine's line of DVDs for viewing and capturing purposes. DVDs and CCTVs will be shown on the floor plan to ease identification and management.

    - **Floor Plan**
      Comprehensive floor plan control to enable easy viewing and control device of status.

2. **xPortalNet HS Client** - TOE is a software running on Windows operating System that can be deployed under xPortalNet HS servers. It enables the user to manage the registered controller(s) and supporting devices. It also provides monitoring activities, report generation as well as change tracking. Below are the features:

    - Flexible scheduling to control who can access which device or door when and for how long.
    - Full event and audit trail records with data export functions.
    - Use for a big scale deployment to manage and configure all device and users.

3. **Xp-GLS5100 Controller** – The TOE Controller is equipped with LAN connectivity at 10/100 Base-T using TCP/IP protocol. It supports push based communication to computer for faster speed. The communication between controller and card reader is encrypted for secure communication. The controller capable to centralised and distributed architecture flexible in one box. Below are the features:

    - Centralised Connection
    - Support DesFire Card System with advanced messaging security with 20 digit Card Serial Number (CSN and Card ID (CID). This provide a much reliable and secure identification.
    - Configurable to Distributed Architecture
    - The Controller uses the 32-bit ARM RISC dual-core processor at 72MHz.
    - Supports Door, Lift, Alarm Monitoring
    - Onboard IP with Encryption
    - Live Remote Firmware Download

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

Security functions	Descriptions
Security Audit	The TOE generates audit records for security events. The super user and authorised user have the ability to view/export the audit and transaction logs
Identification and Authentication	xPortalNet HS Server and xPortalNet HS users (super user and authorised user) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. Note: super user and authorised user have the ability to authenticate using same credential on server and/or client.

Security functions	Descriptions
Security Management	The TOE (xPortalNet HS Server) provides a wide range of security management functions. The super user able to configure the TOE via a software. Super user can configure the TOE, manage device, manage user account and view/export the transaction logs
Secure Communication	The TOE can protect the user data from disclosure and modification by using a secure communication
Tamper Protection	The TOE (Xp-GLS5100 Controller) includes tamper detection mechanisms that generate a log to alert the users

1.4.2 TOE Type

The TOE is consists of the following components; xPortalNet HS Server, xPortalNet HS Client and xP-GLS5100 Controller. The TOE provides security functionality such as Security Audit, Identification and Authentication, Security Management, Secure Communication and Tamper Protection. The TOE can be categorised as ***Access Control Devices and Systems*** in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

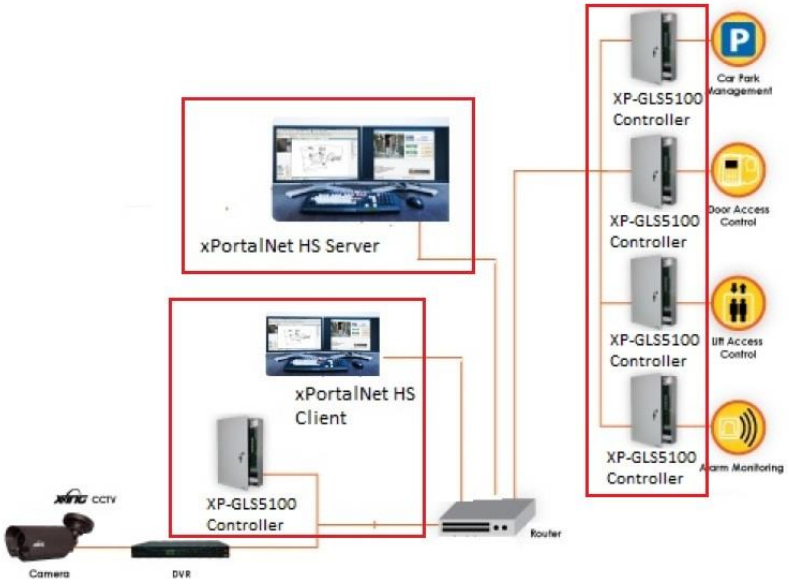
1.4.3 Supporting hardware, software and/or firmware

Minimum System Requirements	
xPortalNet HS Server	
CPU	Xeon E5506 2.15 Ghz
RAM	16GB
Operating System	Microsoft Windows Server 2008 (64-bit) Microsoft windows Server 2012 (64-bit)
Microsoft .NET Framework	Version 2.0 & 3.5
Ethernet & Serial Port	Yes
USB Port	Required for software license key
Hard Disk (Free Space)	500GB
Database	Microsoft SQL Server 2008
xPortalNet HS Client	
CPU	Intel Core 2 Duo E8400 3.0Ghz
RAM	4GB
Operating System	Microsoft Windows 7 Microsoft Windows 10
Microsoft .NET Framework	Version 2.0
Ethernet & Serial Port	Yes
USB Port	Optional for USB Desktop reader
Hard Disk (Free Space)	50GB
Database	Microsoft SQL Server 2008
XP-GLS5100	

Max Door	5
Relay Output	8(5 for Door Relay + 3 General Purpose) Relay rating: 1A
Sensor Input	16 Supervised (as door Status or General Purpose)
IP Support	Yes. LAN 100 Base T
Reader Support	MicroEngine Plato Readers: Max 10 (5 Entry + 5 Exit) Wiegand / ABA Readers : Max 5
Comm Port	Yes. RS485 to Remote Interface Module RS485 to Extension Boards
Up to 16 Digits	Up to 16 Digits
Max Card DB	25,000 / 50,000 / 100,000*
Max Transaction DB	100,000 / 100,000 / 200,000*
Access Mode	1. Card + Pin 2. Card Only 3. Pin Only 4. Facility Code 5. Fingerprint Only 6. Card + Fingerprint 7. Pin + Fingerprint 8. Automatic Lock Release 9. Inhibit Access
Processor	ARM RISC Processor at 72MHz
Power Requirement	12V @ 500mA (Base Board Only)
Remote Firmware Update	Yes. Can be done through application software at site.
Controller Package PSU	12VDC @ 5A with 12AH Battery

1.5 TOE Description

1.5.1 Physical scope of the TOE



Legend: TOE Boundary

Figure 1 – TOE Deployment Architecture

Below are the descriptions of the components stated in Figure 1 above.

Component	Descriptions
xPortalNet HS Server	The TOE is a software that runs on Windows operating System and act as a centralise management system to manage xPortalNet HS client, system user, controller and supporting system or device. Each user able to manage multiple controller and devices registered with the controller. The TOE allows users to authenticate using the same user account for xPortalNet HS client.
xPortalNet HS Client	TOE is a software running on Windows operating System that can be deployed under xPortalNet HS Server. It enables the user to manage the registered controller(s) and supporting devices. It also provides monitoring activities, report generation as well as change tracking.
XP-GLS5100 Controller	The TOE Controller is equipped with LAN connectivity at 10/100 Base-T using TCP/IP protocol. It supports push based communication to computer for faster speed. The communication between controller and card reader is encrypted for secure communication. The controller capable to centralised and distributed architecture flexible in one box.

Component	Descriptions
Car park management	Support Vehicle Count control and Car park payment management system
CCTV	Tightly integrated to MicroEngine's line of DVDs for viewing and capturing purposes. DVDs and CCTVs will be shown on the floor plan to ease identification and management.
Alarm Monitoring and Lift Access Control	Supports up to 512 inputs / 256 outputs / 256 LED Mimic outputs with event programming. User notification can be achieved through client applications, email and SMS for maximum flexibility. Control of up to 96 floors per lift. Support multiple lobby implementations for large scale projects.
Door Access Control	TOE can be integrated with door access control. Door access control is an electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded.

1.5.2 Logical scope of the TOE

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

- **Security Audit:** The TOE (xPortalNet HS Server and xPortalNet HS Client) generates audit records for security events. Only the super user and authorised user have the ability to view/export the audit logs. There are two types of audit event log:
    - ***xPortalNet HS Server*** – The Activity audit event is catered for the user's activities (Super user/authorised User) audit log. It captures events such as event date, Connection, Unit No, RdrNo, Controller, Door/Panel, ID No, Card CSN, Card Type, Name and Transaction.
    - ***xPortalNet HS Client*** – The Activity audit event list is catered for the client user's activities (authorised user) audit log. It captures events such as event date, Connection, Unit No, RdrNo, Controller, Door/Panel, ID No, Card CSN, Card Type, Name and Transaction.

  The exported audit logs can be either in CSV file format.

- **Identification and Authentication:** All users are required to perform identification and authentication with the TOE before any information flows are permitted.
    - ***xPortalNet HS Server*** – super user and authorised user must be authenticated to the server prior to performing any TOE functions by entering a username and password.
    - ***xPortalNet HS client*** – Authorised user must be authenticated to the client by entering the username and password before performing any TOE functions. Each user utilizes one device policy to prevent sharing of user IDs and passwords.

- **Security Management**: The TOE provides a wide range of security management functions. For xPortalNet HS Server, the super user and/or authorised user able to configure the TOE via software. Super user can manage the TOE controller (Xp-GLS5100), manage user account and view/export the audit logs.
- **Secure Communication:** The TOE can protect the user data from disclosure and modification using a secure communication between:
    - xPortalNet HS Server,
    - xPortalNet HS Client, and
    - Xp-GLS5100 Controller

- **Tamper Protection:** The TOE (Xp-GLS5100 Controller) includes tamper detection mechanisms that generate a log records to alert users

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*** 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

Identifier	Threat statement
T.MANAGEMENT	An unauthorized user modifies configuration 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.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE (such as Brute Force Attacks) resulting the exploitation of protected resources
T.CONFIG	An unauthorized person may read, modify, or destroy TOE configuration data.
T.TOECOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.

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.PLATFORM	The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionality.
A.SUPERUSER	One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the TOE super user, and do so using and abiding by guidance documentation.
A.USER	Users are not wilfully negligent or hostile, and use the device within compliance of a reasonable enterprise security policy.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

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 and to explicitly deny access to specific users when appropriate
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data. Only authorized TOE Super user shall have access to TOE management interface.
O.MANAGE	The TOE must allow super user to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.
O.NOAUTH	The TOE shall protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.

4.3 Security Objectives for the Environment

Identifier	Objective statements
OE.PLATFORM	The TOE relies upon the trustworthy platform and hardware to provide policy enforcement as well as cryptographic services and data protection.
OE.SUPERUSER	The owners of the TOE must ensure that the super user who manages the TOE is not hostile, competent and apply all super user guidance in a trusted manner.

Identifier	Objective statements
OE.USER	Users of the TOE are trained to securely use the system, controller and device and apply all guidance in a trusted manner.
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

4.4 TOE Security Objectives Rationale

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

OBJECTIVES \ THREATS/ ASSUMPTIONS/OSPs	T.MANAGEMENT	T.UNAUTHORISED_ACCESS	T.CONFIG	T.TOECOM	A.PLATFORM	A.SUPERUSER	A.USER	A.TIMESTAMP	A.PHYSICAL
O.ACCESS	✔	✔							
O.CONFIG			✔						
O.MANAGE	✔								
O.USER	✔	✔							
O.TOECOM				✔					
O.NOAUTH		✔							
OE.PLATFORM					✔				
OE.SUPERUSER						✔			
OE.USER							✔		

THREATS/ ASSUMPTIONS/OSPs / OBJECTIVES	T.MANAGEMENT	T.UNAUTHORISED_ACCESS	T.CONFIG	T.TOECOM	A.PLATFORM	A.SUPERUSER	A.USER	A.TIMESTAMP	A.PHYSICAL
OE. TIMESTAMP								✔	
OE. PHYSICAL									✔

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.CONFIG	O.CONFIG	The objective ensures that the TOE only allowed authorized person such as TOE Super user to access TOE functions and configuration data.
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 system admin 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 and deny access to specific users when appropriate
T.UNAUTHORISED_ACCESS	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
	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
	O.NOAUTH	The objective ensures that the TOE protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.
T.TOECOM	O.TOECOM	The objective ensures that the TOE protect the confidentiality of its dialogue between distributed components.

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.PLATFORM	OE.PLATFORM	This objective ensures that the underlying platforms are trustworthy and hardened to protect against known vulnerabilities and security configuration issues.
A.SUPERUSER	OE.SUPERUSER	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.USER	OE.USER	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of operating the TOE and the security of the information it contains in a secure manner.
A.TIMESTAMP	OE.TIMESTAMP	This objective ensures that reliable timestamps are provided by the TOE.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that the appliance that hosts the operating system and database are hosted in a secure operating facility with restricted physical access with non-shared hardware.

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 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
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1a	User attribute definition (Server)
FIA_ATD.1b	User attribute definition (Client)
FIA_UAU.2	User authentication before any action (Server & Client)
FIA_UID.2	User identification before any action (Server & Client)
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1a	Management of TSF data (Server)
FMT_MTD.1b	Management of TSF data (Client)
FMT_MOF.1	Management of security functions behaviour (Server)
FMT_SMF.1	Specification of Management Functions (Server)
FMT_SMR.1	Security Roles
FTP_TRP.1	Trusted Path
FPT_PHP.2	Notification of physical attack (Controller)

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 report 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) [**Specifically defined auditable events listed in the Notes section below**].
FAU_GEN1.2	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 • 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
Notes:	Auditable events within the TOE: xPortalNet HS Server a) Log In, b) Shut Down, c) System Device Setting, d) Software Setting, e) Staff Profile f) Software User g) Manage User connection xPortalNet HS Client a) Screen Alarm b) System Device Setting c) Device Operation Settings d) Software Setting e) Time Setting f) Staff Profile g) Staff Attendance Schedule h) Staff Security Setting i) Staff Records j) Floor Plan

	k) Download/Upload Settings l) Transaction Report m) Software User n) Manage User connection

5.2.3 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**Super user and authorised user**] with the capability to read [**all audit information**] 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.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.4 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table below**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	xPortalNet HS Server

Subject	Object	Operation
Super user	Manage user connection	Execute
	Software User	Add/Delete/Change/View
	Staff Profile	Add/Delete/Change/View
	Software Testing	Change/View
	System Device Settings	Add/Delete/Change/View
	Shut Down	Execute

	Log IN	Execute
Authorised User (based on assigned privilege)	Software User	Add/Delete/Change/View
	Staff Profile	Add/Delete/Change/View
	Software Testing	Change/View
	System Device Settings	Add/Delete/Change/View
	Shut Down	Execute
	Log IN	Execute

xPortalNet HS Client

Subject	Object	Operation
Authorised user	Card personalization	Execute
	Personalization Settings	Add/Delete/Change/Print/View
	Key Management for Personalization	Add/Delete/Change/Print/View
	Guard Tour Report 1	Print/View
	Guard Tour	Add/Delete/Change/Print/View
	CCTV Camera View	Execute
	Download/Upload Visitor Card Settings	Execute
	Visitor Sign IN/Out	Execute

5.2.5 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 the Notes section of FDP_ACC.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: [**a) First Time login to xPortalNet Server, super user and authorised user must set their password before performing any action for the first time**

	b) Super user and authorised user must enter their username and password before performing any action on the xPortalNet Server **c) Super user and authorised user can change their password once they have authenticated with the TOE**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.2.6 FIA_ATD.1a User attribute definition (Server)

Hierarchical to:	No other components.
FIA_ATD.1a.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password**]
Dependencies:	No dependencies.
Notes:	None.

5.2.7 FIA_ATD.1b User attribute definition (Client)

Hierarchical to:	No other components.
FIA_ATD.1b.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password**]
Dependencies:	No dependencies.
Notes:	None.

5.2.8 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.

5.2.9 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.

5.2.10 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 [***change_default, modify, delete]*** the security attributes [**Super user Account, Authorised user Account**] to [**Super user**].
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.

5.2.11 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 [***permissive***] 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.

5.2.12 FMT_MTD.1a Management of TSF data (Server)

Hierarchical to:	No other components.
FMT_MTD.1a.1	The TSF shall restrict the ability to [***manage***] the [**Access Control Lists, assign users to roles, User ID**] to [**Super user]**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.13 FMT_MTD.1b Management of TSF data (Client)

Hierarchical to:	No other components.
FMT_MTD.1b.1	The TSF shall restrict the ability to [***modify***] the [**password**] to [**Super User, Authorised user**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.14 FMT_MOF.1 Management of security functions behaviour (Server)

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, modify the behaviour of***] the functions [**xPortalNet HS Alarm Trigger Pattern**] to [**Super user and Authorised user**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.15 FMT_SMF.1 Specification of Management Functions (Server)

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**xPortalNet HS Server** **a) Log In,** **b) Manage user connection**

	c) Software User **d) Staff Profile** **e) Software Testing** **f) System Device Settings** **g) Shut Down**].
Dependencies:	No dependencies.
Notes:	None.

5.2.16 FMT_SMR.1 Security Roles

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

5.2.17 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 or 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 user authentication***, [**and all further communication after authentication**]].
Dependencies:	No dependencies
Notes:	None

5.2.18 FPT_PHP.2 Notification of physical attack (Controller)

Hierarchical to:	FPT_PHP.1 Passive detection of physical attack

FPT_PHP.2.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3	For [**the xp-GLS5100 controller casing**], the TSF shall monitor the devices and elements and notify [**authorised user**] when physical tampering with the TSF's devices or TSF's elements has occurred.
Dependencies:	FMT_MOF.1 Management of security functions behaviour
Notes:	The TSF shall detect physical tampering performed by opening the cover or forcedly removing the device

5.3 Security Requirements Rationale

5.3.1 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
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. This has been addressed in Section 3.4 by A.TIMESTAMP.
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 FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1a	No dependencies	NA
FIA_ATD.1b	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	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_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1

SFR	Dependency	Inclusion
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A
FPT_PHP.2	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1

5.3.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.USER	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_UID.2	The requirement helps meet the objective by identifying user before any TSF mediated actions
O.ACCESS	FAU_GEN.1	The TOE allows set of rules to be applied to indicate authorised and unauthorised access of every user.
	FAU_SAR.1	The TOE maintains a profile of system usage and suspicion rating to each profile along with threshold condition to indicate possible security violation.
	FIA_ATD.1a/b	The requirement helps meet the objective by ensuring user security attributes are maintained.
	FMT_SMF.1	The requirement helps meet the objective by providing management functions of the TOE for authenticated user.
	FMT_SMR.1	The requirement helps meet the objective by providing user timing of identification.

Security objective	Mapped SFRs	Rationale
O.MANAGE	FMT_MTD.1a	The requirement helps meet the objective by restricting the ability to modify the user password.
	FMT_MSA.1	The requirement helps to meet the objective by restricting the ability to modify the security attributes for the super user.
O.CONFIG	FMT_MTD.1a	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MTD.1b	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MSA.1	The requirement helps meet the objective by restricting user access to security attributes.
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
	FMT_SMR.1	The requirement helps meet the objective by defining the security roles used within the TOE.
	FDP_ACC.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FMT_MOF.1	This requirement helps meet the objective by restricting the modification of the TOE behaviour to Super User
O.TOECOM	FTP_TRP.1	The requirement ensures that data sent by users is protected from modification or disclosure.
O.NOAUTH	FPT_PHP.2	The requirement ensures that the TOE provide notification of physical attack to Super User.

6 TOE Security Assurance Requirements (ASE_REQ.2)

6.1 Overview

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 behaviour.

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
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements

Assurance class	Assurance components
	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

6.2 Justification for SAR selection

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

TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

7 TOE Summary Specification (ASE_TSS.1)

7.1 Overview

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

- Security Audit;
- Identification and Authentication;
- Security Management;
- Secure Communication; and
- Tamper Protection

7.2 Security Audit

The TOE (xPortalNet HS Server) will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the transaction event) for the following auditable events (FAU_GEN.1):

xPortalNet HS Server

h) Log In,
i) Shut Down,
j) System Device Setting,
k) Software Setting,
l) Staff Profile
m) Software User
n) Manage User connection

xPortalNet HS Client

o) Screen Alarm
p) System Device Setting
q) Device Operation Settings
r) Software Setting
s) Time Setting
t) Staff Profile

u) Staff Attendance Schedule

v) Staff Security Setting

w) Staff Records

x) Floor Plan

y) Download/Upload Settings

z) Transaction Report

aa) Software User

bb) Manage User connection

The TOE's (xPortalNet HS Server) Super user have the capability to review these audit records via the software interface (FAU_SAR.1). Timestamps for the server and client 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.

7.3 Identification and Authentication

The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

- xPortalNet HS Server maintains two types of users which are Super user and Authorised user (FMT_SMR.1). These users may access the Server via the web interface that the platform provides. Super user and Authorised user must be authenticated to the server prior performing any TOE functions by entering a username and password (FIA_ATD.1a, FIA_UAU.2, FIA_UID.2, FDP_ACF.1). Upon first time login to the server, Super user and Authorised user must set their new password before performing any action (FDP_ACF.1).

- xPortalNet HS Client maintains one type of user which is Authorised user (FMT_SMR.1). These users must be authenticated to the software application by entering username and password before performing any TOE functions (FIA_ATD.1b, FIA_UAU.2, FIA_UID.2, FDP_ACF.1).

7.4 Security Management

The TOE provides a suite of management functions only to Super user and Authorised user. These functions allow for the configuration of Server and client to suit the environment in which it is deployed. Additionally, management roles may perform the following tasks (FMT_SMF.1, FMT_MTD.1a, FMT_MTD.1b, FMT_MSA.1 and FMT_MSA.3):

xPortalNet HS Server

- Manage user connection,

- Software User,
- Staff Profile
- Software Testing
- System Device Settings
- Shut down
- Log In

xPortalNet HS Client

- Card personalization
- Personalization Settings
- Key Management for Personalization
- Guard Tour Report 1
- Guard Tour
- CCTV Camera View
- Download/Upload Visitor Card Settings
- Visitor Sign IN/OUT

Both xPortalNet Server and Client implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1 and FDP_ACF.1).

7.5 Secure Communication

The TOE establishes a trusted path (FPT_TRP.1) using the proprietary encryption method as a secure communication between:

- Remote Super user/ system user and xPortal HS Server
- xPortal HS Server and xPortal HS Client

The TOE also able to protect the user data from disclosure and modification using controller encryption as a secure communication between the controller and card reader.

7.6 Tamper Protection

The TOE (Xp-GLS5100 Controller) includes motion tamper detection mechanisms that trigger an alarm response mechanisms to alert the users (FPT_PHP.2). There is one sensors used in the Controller to perform tamper detection.

- Motion Sensor is used to detect the changes on orientation and position of the Device.

A dedicated output signal line is allocated to connect to external alarm/reporting system. This signal will be triggered upon tampering is detected. The super user has the ability to manage the behaviour of the TOE alarm trigger pattern (FMT_MOF.1) via the xPortalNet HS server.