C092 Certification Report

xPortalNet HS Server version 2.0.0.2, xPortalNet HS Client version 2.0.0.2 and Xp-GLS5100 Controllers

File name: ISCB-3-RPT-C092-CR-v1
Version: v1
Date of document: 16 March 2018
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

C092 Certification Report

xPortalNet HS Server version 2.0.0.2, xPortalNet HS Client version 2.0.0.2 and Xp-GLS5100 Controllers

16 March 2018

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 □Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C092 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C092-CR-v1
ISSUE:	v1
DATE:	16 March 2018

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 16 March 2018, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	1 March 2018	All	Initial draft
v1	5 March 2018	All	Change SEF name and finalize the document
v1	16 March 2018	All	Change dates

Executive Summary

The TOE is the xPortalNet HS system which consist of xPortalNet Server version 2.0.0.2, xPortalNet HS Client version 2.0.0.2 and Xp-GLS5100 Controllers. The TOE provides a centralise management system to manage MicroEngine controller(s) and supporting device from unauthorised 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.

xPortalNet HS server is the software that runs on Windows Operating System and act as a centralise management system to manage xPortalNet HS client, controller, user and supporting device. Each user is 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.

xPortalNet HS Client is a software that 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.

While XP-GLS5100 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.

The xPortalNet HS system consists of following security features which are:

a) Security Audit

b) Identification and Authentication

c) Security Management

d) Secure Communication

e) Tamper Protection.

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 xPortalNet HS System is the Target of Evaluation (TOE) which consists of xPortalNet HS Server, xPortalNet HS Client and Xp-GLS5100 Controller. It provides a centralise management system to manage MicroEngine controller(s) and supporting device from unauthorised 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.

2 xPortalNet HS System consist of three (3) functionalities such as:

a) **xPortalNet HS Server:** The software that runs on Windows Operating System and act as a centralize management system in order to manage xPortalNet HS client, controller, user and supporting device. Each user is 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.

b) **xPortalNet HS Client:** The software that 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.

c) **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 centralized and distributed architecture flexible in one box.

3 The TOE scope of evaluation covers various major security functions described as below:

- **Security Audit:** The TOE generates audit records for security events. The super user and authorized user have the ability to view/export the audit and transaction logs.

- **Identification & Authentication:** xPortalNet HS Server and xPortalNet HS users (super user and authorized user) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. Note: super user and authorized user have the ability to authenticate using same credential on server and/or client.
- **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.

1.2 TOE Identification

4 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C092
TOE Name	• 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
Security Target Title	xPortalNet HS Security Target
Security Target Version	1.0
Security Target Date	10 February 2018
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])

Methodology	The Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor and Developer	MicroEngine Technology Sdn Bhd Unit 11-06, Block A, Phileo Damansara 2, Section 16, Jalan 16/11, Off jalan Damansara, 46350 Petaling Jaya, Selangor Darul Ehsan.
Evaluation Facility	Securelytics – SEF

1.3 Security Policy

5 There are no organisational security policies.

1.4 TOE Architecture

6 The TOE includes both logical and physical boundaries which are described in Section 1.5 of the Security Target (Ref [6])

1.4.1 Logical Boundaries

7 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality in Table 3:

Table 2: Logical Boundaries

Security function	Description
Security Audit	The TOE (xPortalNet HS Server and xPortalNet HS Client) generates audit records for security events. Only the super user and authorized 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/authorized 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 (authorized 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 authorized 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 • Xp-GLS5100 Controller
Tamper Protection	The TOE (Xp-GLS5100 Controller) includes tamper detection mechanisms that generate a log records to alert users.

1.4.2 Physical Boundaries

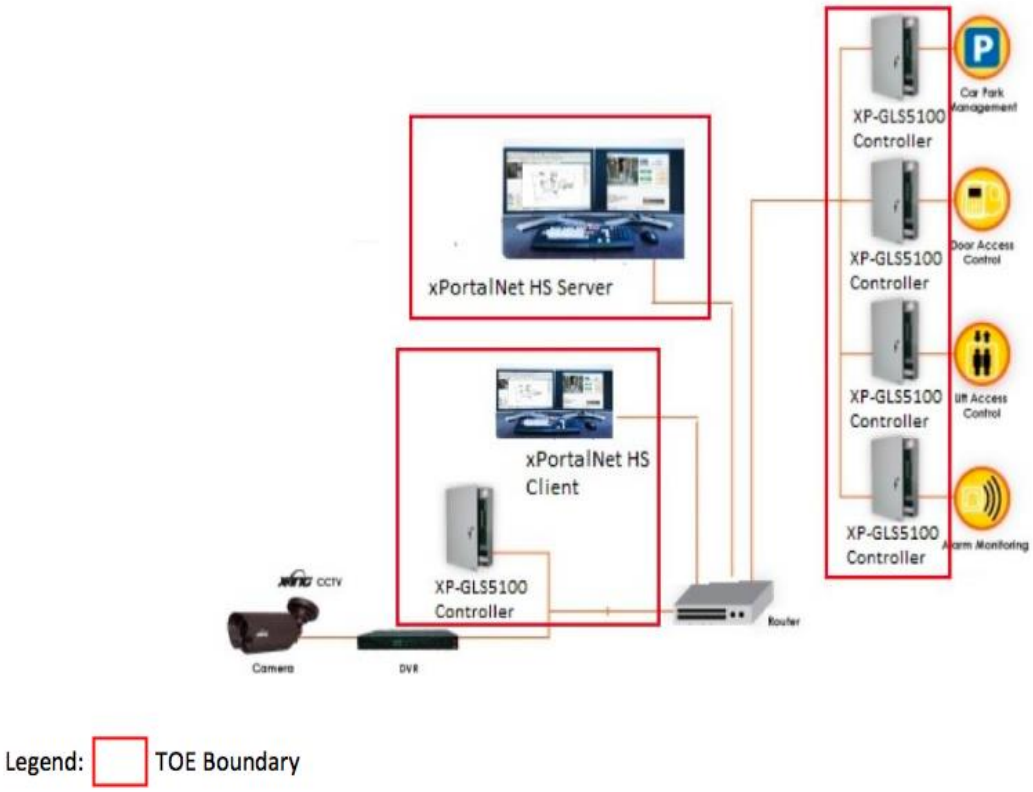

Figure 1: TOE Deployment Architecture

8 The TOE consists of the following components stated in Figure 1 above:

Table 3: Description of Physical Boundaries

Component	Description
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.
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 Clarification of Scope

9 The TOE is designed in order to provide a centralise management system to manage MicroEngine controller(s) and supporting device from unauthorised 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.

10 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is xPortalNet HS System that provides access control and manage users, controllers and card access control, where they can modify or change Card ID and Card Serial Number. It also increased accountability by always knowing which assets are accessed when and by whom.

11 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

12 This section summarises the security aspects of the environment/configuration in which it product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE which has defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

13 Assumption for the TOE usage as listed in Security Target:

a) One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorised as the TOE super user, and do so using and abiding by guidance documentation.

b) Users are not wilfully negligent or hostile, and use the device within compliance of a reasonable enterprise security policy.

1.6.2 Environment assumptions

14 Assumption for the TOE environment listed in Security Target are:

a) 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.

b) The platforms on which the TOE operate shall be able to provide reliable time stamps.

c) 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.

1.7 Evaluated Configuration

15 There are four main components of the TOE to be evaluated which are:

1.7.1 ADMIN Interface

16 The admin interface provides super user with a GUI interface that allows them to manage and configure the TOE.

1.7.2 USER Interface

17 The user interface provides the authorised user with a GUI interface that allows them to perform user operations such as user account management and DNS management.

1.7.3 Encrypt Interface

18 The encrypt interface is used to engage the various functions provided to enable secure communications between the end-user and the web-server. The encrypt interface is called programmatically by the presentation layer of the TOE. TOE users do not directly interact with this interface.

1.7.4 Tamper Interface

19 The tamper interface provides protection boundary to protect the Controller and its components. Monitors and sensor readings and raise flag when tamper detected.

1.8 Delivery Procedures

20 Delivery process of the TOE to the customer for installation and use is as follows:

21 The following is the customer's ordering and delivery process handling for TOE from manufacturing until the TOE is delivered to customer for installation and use

1.8.1 Receiving Customer Order

22 The sales department received in written/verbally order from customers through fax/email/telephone conversation.

1.8.2 Evaluate Customer's Order

23 Head of Sales Department will evaluate the product requirements, quantity and pricing with the customer.

1.8.3 Planning Stock Delivery

24 Head of Sales Department/Production Manager will determine the stock delivery schedule and executive.

1.8.4 Product Requisition

25 Sales/Sales Coordinator will determine the stock delivery schedule and executive to raise Sales Requisition to Production/Stock Controller and inform product delivery schedule to Production and Store Personnel.

1.8.5 Product Delivery Arrangement

26 Sales/Store Personnel will prepare product model and quantity required.

1.8.6 Product Delivery

27 Sales/Sales Coordinator will execute the product delivery to customer based on the quantity required and schedule agreed.

1.8.7 Invoicing

28 Sales/Sales Coordinator/Store Personnel will ensure the product model and quantity are correct and deliver according the agreed delivery schedule. Then, it will proceed to invoice when product being delivered.

1.8.8 End

29 If any issues occur during the delivery process, the Product Owner (PO) and MicroEngine Technology Sdn Bhd's authorised sales representative or appointed account manager can communicate via email, phone call or face-to-face to resolve the issue via contact information in MicroEngine Technology Sdn Bhd's website.

2 Evaluation

30 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

31 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

32 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

33 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

34 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

35 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

36 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate

with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

37 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

37.1.4 IT Product Testing

38 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from Securelytics – SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of developer Tests

39 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

40 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

41 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

42 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 4: Independent Functional Test

Identifier	Description	Results
F001 – Identification and Authentication (Server & Client) ADMIN Interface USER Interface	1. To test that the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. • To test that the TOE maintains Username and password security attributes belonging to individual users (server and client)	PASS. Result as expected.

Identifier	Description	Results
F002 – Security Management User Data Protection ADMIN Interface USER Interface	1. To test that the TOE enforces the access control SFP to restrict the ability to change_default/modify/delete the security attributes Superuser Account/system Users Account to Superuser 2. To test that the TOE enforces the access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 3. To test that the TOE restricts the ability to manage the TSF data on the xPortalNet HS Server to Superuser 4. To test that the TOE restricts the ability to modify the password to system user/another user 5. To test that the TOE restricts the ability to determine the behaviour of/modify the behaviour of the functions xPortalNet HS Alarm Trigger Pattern to superuser and system user 6. To test that the TOE capable of performing the following management functions: a) xPortalNet HS Server • Log In • Shut Down • System Device Setting • Software Setting	PASS. Result as expected.

Identifier	Description	Results
	• Staff Profile • Software User • Manage User connection b) xPortalNet HS Client • Screen Alarm • System Device Setting • Device Operation Settings • Software Setting • Time Setting • Staff Profile • Staff Attendance Schedule • Staff Security Setting • Staff Records • Floor Plan • Download/Upload Settings • Transaction Report • Software User • Manage User connection 7. To test that the TOE maintains the roles Superuser and authorised user. 8. To test that the TOE be able to associate users with roles	

Identifier	Description	Results
	9. To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the Security Target (Ref [6]). 10. To test that the TOE enforces 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 system users must set their password before performing any action for the first time b) Super user and system users must enter their username and password before performing any action on the xPortalNet Server c) Supervisor and Operator can change their password once they have authenticated with the TOE	
F003 – Secure Communication Encrypt Interface	1. To test that the TOE provides 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 2. To test that the TOE permits remote users to initiate communication via the trusted path 3. To test that the TOE requires the use of the trusted path for initial user authentication and other services for which trusted path is required	PASS. Result as expected.

2.1.4.3 Penetration Testing

43 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources

and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

44 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

45 The penetration tests focused on:

a) SQL Injection

b) Password Cracking

c) Reverse Engineering

d) Configuration File Contains Sensitive Information

46 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

47 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification.

3 Result of the Evaluation

48 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of xPortalNet HS Server version 2.0.0.2, xPortalNet HS Client version 2.0.0.2 and Xp-GLS5100 Controllers performed by Securelytics – SEF.

49 Securelytics – SEF, found that xPortalNet HS Server version 2.0.0.2, xPortalNet HS Client version 2.0.0.2 and Xp-GLS5100 Controllers upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

50 Certification is not guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

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

52 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.

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

3.2 Recommendation

54 In addition to ensure secure usage of the product, below are additional recommendations for TOE users:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The user should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

c) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.

d) The TOE User keeps updated the administrator to review the audit trail generated and exported by the TOE periodically.

e) The users must ensure appropriate network protection and firmware is maintained, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1a, CyberSecurity Malaysia, June 2017.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1, June 2017.

[6] XPortalnet HS Security Target, Version 1.0, 10 February 2018.

[7] XPortalnet HS Evaluation Technical Report, Version 1.0, 20 February 2018.

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---