KECS-CR-19-11

Pass-Ni SSO v4.0

Certification Report

Certification No.: KECS-CISS-0918-2019

2019. 3. 4.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2019.03.04.	-	Certification report for Pass-Ni SSO v4.0 - First documentation

This document is the certification report for Pass-Ni SSO v4.0 of UbiNtisLab Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

1. Executive Summary

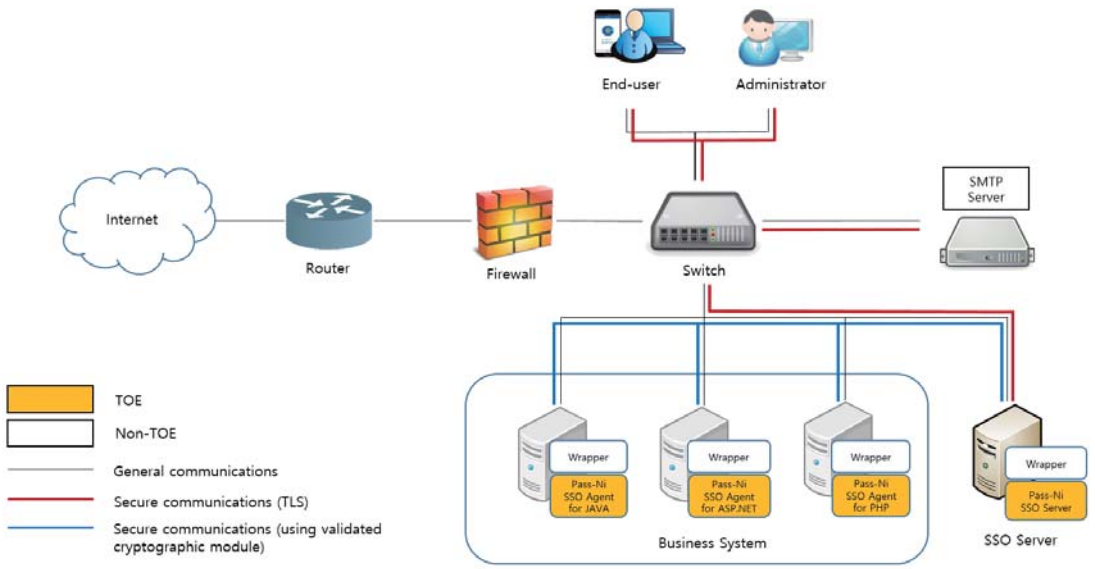
This report describes the certification result drawn by the certification body on the results of the evaluation of Pass-Ni SSO v4.0 of UbiNtisLab Co., Ltd with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is Single Sign-On (SSO) software to be used to enable the user to access various business systems and use the service through a single user login without additional login action. The TOE is comprised of four software components: Pass-Ni SSO Server, Pass-Ni SSO Agent for JAVA, Pass-Ni SSO Agent for ASP.NET, and Pass-Ni SSO Agent for PHP. Pass-Ni SSO Server performs functions such as user login processing, authentication token issuance and policy setting, while Pass-Ni SSO Agent that is installed in each business system validates the authentication token through interworking with Pass-Ni SSO Server. It also includes preparative procedures that describe the procedures for secure acceptance and installing the TOE, and operational guidance that specify how to use the TOE safely. The TOE includes a cryptographic module validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on February 21, 2019. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to the Korean National Protection Profile for Single Sign On V1.0 [7]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of the PP [7]. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and newly defined components in the Extended Component Definition chapter of the PP, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Category		Contents
Pass-Ni SSO Server	CPU	Intel® Xeon E5 2.0 GHz or higher
	RAM	8 GB or higher
	HDD	50 GB or higher space for installation of Pass-Ni SSO Server
	NIC	Ethernet 100/1000 Mbps X 1port or higher
	OS	Windows Server 2008 Standard 32-bit Windows Server 2012 Standard 64-bit CentOS 6.9 (kernel 2.6.32) 64-bit Ubuntu Server 16.04 (kernel 4.4.0) 64-bit
	S/W	jdk-8u152 Apache Tomcat 8.5.23 CUBRID 9.3.9
Pass-Ni SSO Agent for JAVA	CPU	Intel® Core™ i5 2.6 GHz or higher
	RAM	8 GB or higher
	HDD	10 GB or higher space for installation of Pass-Ni SSO Agent for JAVA
	NIC	Ethernet 100/1000 Mbps X 1port or higher

	OS	Windows Server 2008 Standard 32-bit Windows Server 2012 Standard 64-bit CentOS 6.9 (kernel 2.6.32) 64-bit Ubuntu Server 16.04 (kernel 4.4.0) 64-bit
	S/W	jdk-8u152
Pass-Ni SSO Agent for ASP.NET	CPU	Intel® Core™ i5 2.6 GHz or higher
	RAM	8 GB or higher
	HDD	10 GB or higher space for installation of Pass-Ni SSO Agent for ASP.NET
	NIC	Ethernet 100/1000 Mbps X 1port or higher
	OS	Windows Server 2012 Standard 64-bit
	S/W	.NET Framework 4.7.1
Pass-Ni SSO Agent for PHP	CPU	Intel® Core™ i5 2.6 GHz or higher
	RAM	8 GB or higher
	HDD	10 GB or higher space for installation of Pass-Ni SSO Agent for PHP
	NIC	Ethernet 100/1000 Mbps X 1port or higher
	OS	CentOS 6.9 (kernel 2.6.32) 64-bit
	S/W	PHP 5.3.3

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator's PC to access Pass-Ni SSO Server.

Category	**Contents**
CPU	Intel® Core™2 Duo 1.6 GHz or higher
RAM	4 GB or higher
HDD	500 GB or higher
NIC	Ethernet 100/1000 Mbps X 1port or higher
OS	Windows 10 Pro 64-bit
S/W	Internet Explorer 11 Google Chrome 65

[Table 2] The minimum requirements for the administrator's PC

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is software consisting of the following software components and related guidance documents.

TOE	Pass-Ni SSO v4.0	
Version	v4.0.005	
TOE Components	Pass-Ni SSO Server	Pass-Ni SSO Server v4.0.005 (PassNi-SSO-Server-v4.0.005.zip)
	Pass-Ni SSO Agent	Pass-Ni SSO Agent for JAVA v4.0.005 (PassNi-SSO-Agent-for-JAVA-v4.0.005.zip) Pass-Ni SSO Agent for ASP.NET v4.0.005 (PassNi-SSO-Agent-for-ASP.NET-v4.0.005.zip) Pass-Ni SSO Agent for PHP v4.0.005 (PassNi-SSO-Agent-for-PHP-v4.0.005.zip)
Guidance Document	Pass-Ni SSO v4.0 Preparative Procedures V1.0 R5 (PassNi-SSO-v4.0-PRE-V1.0.R5.pdf) Pass-Ni SSO v4.0 Operational Guidance V1.0 R5 (PassNi-SSO-v4.0-OPE-V1.0.R5.pdf)	

[Table 3] TOE identification

Note that the TOE and the guidance documents are delivered contained in a CD-ROM. The wrapper that may be used to support various types of business systems is excluded from the physical scope of the TOE.

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)

	Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Protection Profile	Korean National Protection Profile for Single Sign On V1.0, KECS-PP-0822-2017, August 18, 2017
Developer	UbiNtisLab Co., Ltd
Sponsor	UbiNtisLab Co., Ltd
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	February 21, 2019
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [6] for the TOE claims strict conformance to the Korean National Protection Profile for Single Sign On V1.0 [7], and complies security policies defined in the PP [7] by security requirements. Thus, the TOE provides security features defined in the PP [7] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up/shutdown of the audit functions and all auditable events listed in ST [6] such as the results of the TOE security functionality (TSF) self-tests and modifications to the values of TSF data. The TOE stores the audit recodes in the DBMS and provides the recodes for the authorized administrator.
- Cryptographic support: The TOE performs cryptographic key management such as key generation, distribution, and destruction, and cryptographic operations such as encryption, decryption, and hash using the cryptographic module (Pass-Ni Crypto V1.1) validated under the KCMVP.
- Identification and authentication: The TOE identifies and authenticates the

administrators and end-users using their ID/password and mutually authenticates TOE components. The TOE performs authentication token management such as token issuance, verification, and destruction. The TOE authenticates end-users based on the authentication tokens issued during the initial authentication procedure using their ID/password.

- Security management: The TOE allows only authorized administrators to access the management interface provided by the TOE.
- Protection of the TSF: The TOE implements secure communications between the TOE components to protect the transmitted data. The TOE encrypts the stored TSF data to protect them from unauthorized exposure and modification. The TOE performs self-tests on the TOE components, which includes the self-test on the validated cryptographic module.
- TOE access: The TOE manages authorized administrators' sessions based on attributes such as connection IP address. The TOE terminates administrators' and end-users' sessions after predefined time interval of inactivity.
- Trusted channel: The TOE implements secure communications between the TOE and the SMTP server in the operational environment.

4. Assumptions and Clarification of Scope

There is no explicit Security Problem Definition chapter, therefore no Assumptions section, in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [7] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [6], chapter 3.).

5. Architectural Information

The TOE is software consisting of the following components:

- Pass-Ni SSO Server provides security features of audit data generation, identification and authentication of users (administrators and end-users), cryptographic key management, cryptographic operations, security management to the TOE and TSF data, protection of TSF data, access control to Pass-Ni SSO Server, and the trusted channel between the TOE and the

SMTP server.

- Pass-Ni SSO Agent (Pass-Ni SSO Agent for JAVA, Pass-Ni SSO Agent for ASP.NET, Pass-Ni SSO Agent for PHP) authenticates end-users based on their authentication tokens issued by Pass-Ni SSO Server, performs cryptographic key management and cryptographic operations related to the mutual authentication and the internal TSF data transfer protection, and protects transmitted and stored TSF data.

For the detailed description on the architectural information, refer to the ST [6], chapter 1.4.3.

6. Documentation

The following documentations are evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
Pass-Ni SSO v4.0 Preparative Procedures V1.0 R5 (PassNi-SSO-v4.0-PRE-V1.0.R5.pdf)	V1.0 R5	January 3, 2019
Pass-Ni SSO v4.0 Operational Guidance V1.0 R5 (PassNi-SSO-v4.0-OPE-V1.0.R5.pdf)	V1.0 R5	January 3, 2019

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions and modules to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing

- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator installed and prepared the TOE in accordance to the preparative procedures, and conducted independent testing based upon test cases devised by the evaluator. In addition, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator confirmed that all the actual testing results correspond to the expected testing results.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is Pass-Ni SSO v4.0 (version number 4.0.005). See table 3 for detailed information on the TOE components.

The TOE is installed from a CD-ROM distributed by UbiNtisLab Co., Ltd. After the installation of the TOE, an administrator can identify the TOE version through the product's Info check menu. The guidance documents listed in this report chapter 6, [Table 5] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] which references Single Evaluation Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PP and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The functional specifications provided by the developer specify a high-level description of at least the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.
The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore, the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore, the verdict PASS is assigned to ATE_IND.1.
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.
Thus, potential vulnerabilities identified, during the evaluation of the development and

anticipated operation of the TOE, don't allow attackers possessing basic attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 6] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.
- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.
- The administrator should periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prevent audit data loss.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

11. Security Target

Pass-Ni SSO v4.0 Security Target V1.0 R6 [6] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
KCMVP	the Korea Cryptographic Module Validation Program
PP	Protection Profile
SAR	Security Assurance Requirement

SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSO	Single Sign-On
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

Authentication data	Information used to verify a user's claimed identity
Authentication token	Authentication data that authorized end-users use to access the business system
Authorized Administrator	Authorized user to securely operate and manage the TOE
Authorized User	The TOE user who may, in accordance with the SFRs, perform an operation
Business System	An application server that authorized end-users access through ‘SSO’
Decryption	The act that restoring the ciphertext into the plaintext using the decryption key
Encryption	The act that converting the plaintext into the ciphertext using the cryptographic key
end-user	Users of the TOE who want to use the business system, not the administrators of the TOE
Self-test	Pre-operational or conditional test executed by the cryptographic module
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority
Wrapper	Interfaces for interconnection between the TOE and various types of business systems

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (September 12, 2017)

[5] Pass-Ni SSO v4.0 Evaluation Technical Report V3.00, February 21, 2019

[6] Pass-Ni SSO v4.0 Security Target V1.0 R6, February 18, 2019

[7] Korean National Protection Profile for Single Sign On V1.0 (KECS-PP-0822-2017, August 18, 2017)