KECS-CR-24-10

Pass-Ni SSO v5.0

Certification Report

Certification No.: KECS-CISS-1288-2024

2024. 02. 07.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.02.07.	-	Certification report for Pass-Ni SSO v5.0 - First documentation

This document is the certification report for Pass-Ni SSO v5.0 of UbiNtisLab Co., Ltd

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

Table of Contents

1. Executive Summary

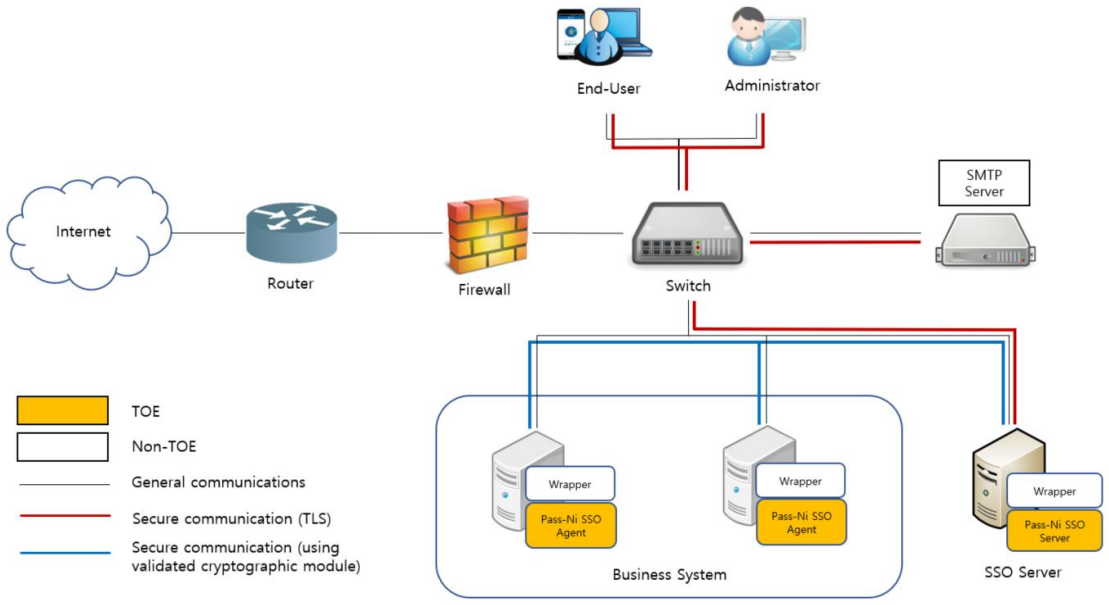
This report describes the evaluation result drawn by the evaluation facility on the results of the E AL1+ evaluation of Pass-Ni SSO v5.0 with reference to the Common Criteria for Information Technology Security Evaluation(“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

Pass-Ni SSO v5.0(“TOE” hereinafter) is an ‘Single Sign On (SSO)' that is used for the purpose of providing a user with services from various application servers (business systems) without additional login by single login. The TOE provides users with access to information of various business systems through single authentication.

The major features of the TOE are to issue, store, verify, and revoke the authentication token. It issues an authentication token when the user, who requests the login, is regarded as valid by identifying and authenticating. Then, when the user accesses the other business system, the access of the user is controlled through validation of the authentication token. In the initial authentication phase, the TOE performs ID / PW authentication for doing identification and authentication functionality.

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on January 17, 2024. The ST claims conformance to the Korean National PP for Single Sign On V1.1[4]. 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 Evaluation Assurance Level EAL1+. 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 a newly defined component 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.

The operational environment of the TOE is shown in the following figure.



[Figure 1] Operational environment of the TOE

The TOE comprised of the Pass-Ni SSO Server that performs functions such as processing user login, issuing authentication token and managing policy, and the Pass-Ni SSO Agent that is installed in each business system and verifies the validity of the authentication token.

The major roles of the operational services other than the TOE evaluation target required for the TOE operation are as follows.

- SMTP server: The mail server that sends an administrator notification mail, such as handling authentication failures and saturation of audit storage

The TOE, in the form of software, is installed in a server or a PC and operated on an operating system (OS) such as Windows or Linux. The hardware / software, which is out of the TOE evaluation target, required for SSO server operation is identified as follows.

Type		Requirements for SSO Server
H/W	CPU	Intel® Xeon™ E5 2.0Ghz or higher
	HDD	Space required for installation of TOE 50GB or higher
	Memory	8GB or higher
	NIC	Ethernet 100/1000 Mbps * 1 port or higher
OS		Red hat Enterprise Linux 8.5 x64

S/W	OpenJDK 11.0.21 Apache Tomcat 9.0.84 MariaDB 10.6.16

[Table 1] Hardware/Software Requirements for SSO Server

The hardware / software, which is out of the TOE evaluation target, required for the SSO Agent operation is identified as follows.

Type		Requirements for SSO Agent
H/W	CPU	Intel® Core™ i3 3.6 Ghz or higher
	HDD	Space required for installation of TOE 10GB or higher
	Memory	8GB or higher
	NIC	Ethernet 100/1000 Mbps * 1 port or higher
OS		Red hat Enterprise Linux 8.5 x64 Windows Server 2019 x64
S/W		OpenJDK 11.0.21 Apache Tomcat 9.0.84

[Table 2] Hardware/Software Requirements for SSO Agent

The software requirements of the PC used by the authorized administrator to manage the TOE are as follows.

Type	Requirements for administrator's PC
S/W	Google Chrome 110

[Table 3] Software Requirements for 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 reference is identified as follows.

TOE		Pass-Ni SSO v5.0
TOE Version		v5.0.002
TOE Components	SSO Server	Pass-Ni SSO Server v5.0.002 (PassNi-SSO-Server-v5.0.002.zip)
	SSO Agent	Pass-Ni SSO Agent v5.0.002 (PassNi-SSO-Agent-v5.0.002.zip)
Guidance Document	Preparative Procedures	Pass-Ni SSO v5.0 Preparative Procedures V1.0 R3 (PassNi-SSO-v5.0-PRE-V1.0.R3.pdf)
	Operational Guidance	Pass-Ni SSO v5.0 Operational Guidance V1.0 R3 (PassNi-SSO-v5.0-OPE-V1.0.R3.pdf)

[Table 4] TOE identification

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	Pass-Ni SSO v5.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign-On V1.1,KECS-PP-0822a-2017, December 11, 2019
Developer	UbiNtisLab Co., Ltd
Sponsor	UbiNtisLab Co., Ltd
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	January 17, 2024
Certification Body	IT Security Certification Center

[Table 5] Additional identification information

3. Security Policy

The TOE complies security policies pertaining to the following security functional requirenents defined in the ST [5].

- Security Audit
- Cryptographic support
- Identification and authentication
- Security Management
- Protection of the TSF
- TOE access

4. Assumptions and Clarification of Scope

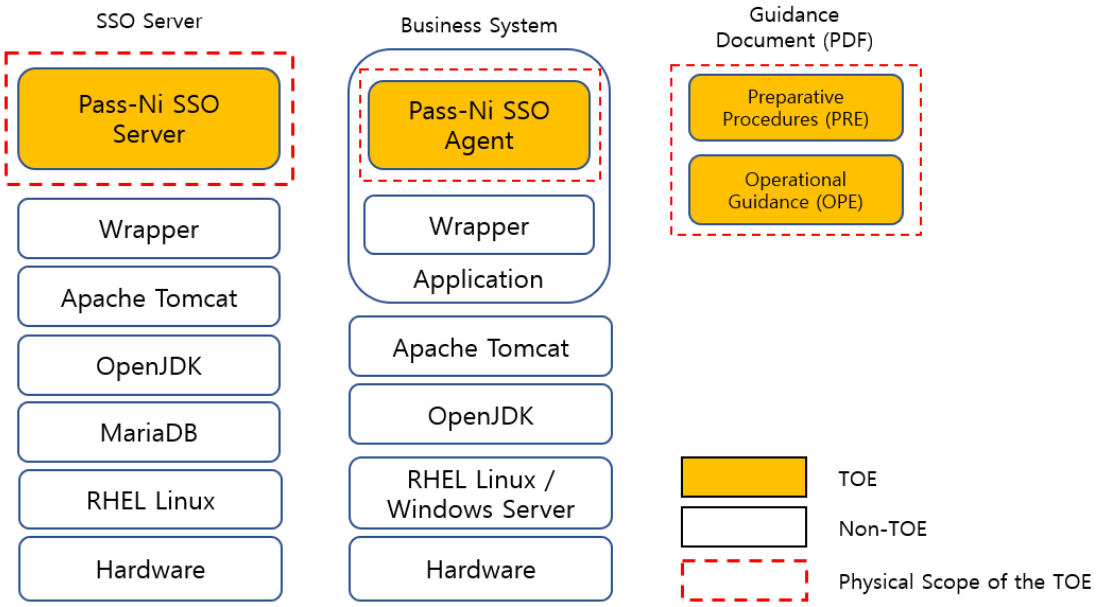
There is no explicit Security Problem Definition chapter, therefore no Assumptions section, in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [4] in which the TOE will be used or is intended to be used (For the detailed and precise definition of the security objectives of the operational environment, refer to the ST [5], chapter 3.).

5. Architectural Information

The physical scope of the TOE consists of Pass-Ni SSO Server which performs functions such as user login processing, authentication token issuance and policy setting, and Pass-Ni SSO Agent which is installed in each business system and validates the authentication token through interworking with 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.

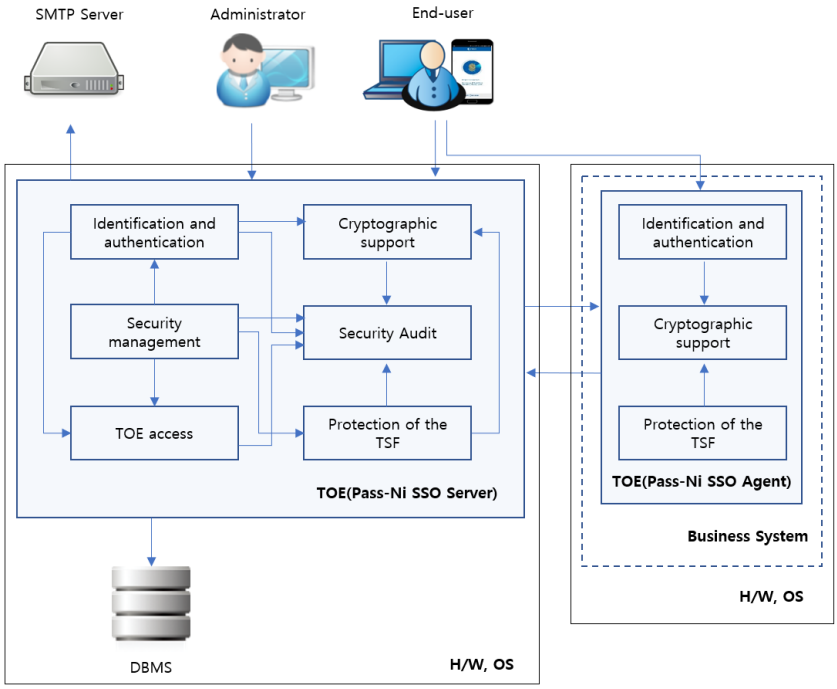
The hardware and operating system where the TOE is installed, an administrator PC connect as privileged mode for the TOE security management, the DBMS storing the security policy and audit data, and the Wrappers which may be used to support various types of compatibility with business systems are excluded from the TOE physical scope.

The physical scope of the TOE is shown in the following figure.



[Figure 2] Physical scope of the TOE

The logical scope of the TOE is shown in following figure. The TOE provides security audit, cryptographic support, identification and authentication, security management, TSF protection, and TOE access functions according to the TOE components. For the detailed description on the architectural information, refer to the ST [5].



[Figure 3] Logical scope of the TOE

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Date
Pass-Ni SSO v5.0 Preparative Procedures V1.0 R3	December 28, 2023
Pass-Ni SSO v5.0 Operational Guidance V1.0 R3	December 28, 2023

[Table 6] Documentation

7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.
The evaluator performed all the developer's tests, and conducted independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [5]. The evaluator considered the followings when devising a test subset:

- TOE security functionality: The TOE is software used to enable the user to access various business systems and use the service through a single user login without additional login action, and
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_FUN.1, and ATE_IND.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL1+(ATE_FUN.1), and the evaluator tried to balance time and effort of evaluator's activities between EAL1+ assurance components.

In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.
The evaluator testing effort, the testing approach, configuration, depth, and results are

summarized in the ETR [3].

8. Evaluated Configuration

The TOE is software consisting of the following components:

- TOE : Pass-Ni SSO v5.0 (v5.0.002)
- TOE Components : Pass-Ni SSO Server v5.0.002, Pass-Ni SSO Agent v5.0.002

The TOE is identified by TOE name and version number. The TOE identification information is provided via GUI. And the guidance documents listed in this report chapter 6, [Table 6] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR [3] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation(EAL1+).

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 Development Evaluation (ADV)

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 Life Cycle Support Evaluation (ALC)

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 processing 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_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	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	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 7] 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 administrator must change the password when logging in for the first time after installing the TOE, and must periodically change all passwords set while operating the TOE.
- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators.
- When the audit storage space is filled, audit data may be lost, so periodic monitoring and periodic backup are required.
- 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.

11. Security Target

Pass-Ni SSO v5.0 Security Target V1.0 R3 [5] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
Authentication token	Authentication data that authorized end-users use to access the business system
Business System	An application server that authorized end-user access through ‘SSO’
Korea Cryptographic Module Validation Program(KCMVP)	A system to validate the security and implementation conformance of cryptographic modules used for protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions
Self-test	Pre-operational or conditional test executed by the cryptographic module
Wrapper	Interfaces for interconnection between the TOE and various types of business systems or authentication systems

13. Bibliography

The evaluation facility 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

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

[3] Pass-Ni SSO v5.0 Evaluation Technical Report V2.0, February 5, 2024

[4] Korean National Protection Profile for Single Sign-On V1.1, December 11, 2019

[5] Pass-Ni SSO v5.0 Security Target V1.0 R3, December 28, 2023

[6] Pass-Ni SSO v5.0 Independent Testing Report(ATE_IND.1) V3.0, February 2, 2024

[7] Pass-Ni SSO v5.0 Penetration Testing Report (AVA_VAN.1) V3.0, February 2, 2024