KECS-CR-21-52

Bandi SSO v7.0

Certification Report

Certification No.: KECS-CISS-1122-2021

2021. 09. 08.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2021.09.08.	-	Certification report for Bandi SSO v7.0 - First documentation

This document is the certification report for Bandi SSO v7.0 of Bandi S&C 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 EAL1+ evaluation of Bandi SSO v7.0 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

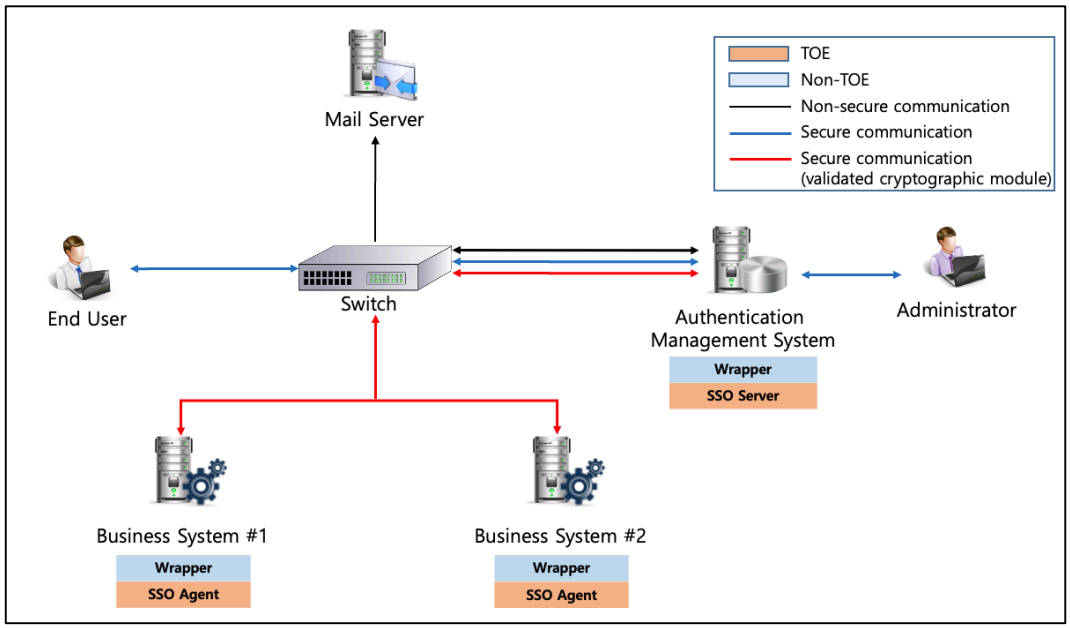
Bandi SSO v7.0 (“TOE” hereinafter) is a Single Sign-On (SSO) product used to enable an end user to access various business systems (systems in which the SSO Agent has been installed) to use services through a single login (Single Sign-On) without additional login actions. The TOE implements authentication tokens in accordance with universal standard specifications to ensure stronger security and higher flexibility, which makes it applicable to various types of business systems. The TOE performs the user identification and authentication, and then issues authentication tokens in accordance with the user authentication policies to identify the user and verify the validity without a separate login process.

Furthermore, the TOE provides the security audit function that manages major events by recording them as audit data when the security function and the management function are invoked; the identification and authentication function such as verification of an identity of an authorized user and continuous authentication failures, the cryptographic support function for secure communication and storage, the TSF protection function that ensures TOE internal communication and performs TSF self-tests, the security management function that supports an authorized administrator to perform administrative functions, and the TOE access function that controls access sessions of the authorized administrator.

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on September 1, 2021. 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.

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



[Figure 1] Operational environment of the TOE

TOE consists of the SSO Server and the SSO Agent. The SSO Server uses user information stored in DBMS to provide functions such as user login verification, generation of authentication tokens and policy establishment. The SSO Agent

performs functions related to request for user authentication to the SSO Server, including issuance of authentication tokens and request for verification, and is provided in the form of API, a library file format, for each business system.

Wrapper, which may be used to ensure the compatibility among the SSO Server, the SSO Agent and various types of business systems, is out of the scope of the TOE.

For the encryption of the communication used in data transfer between TOE components (including mutual authentication between components), MagicJCrypto V2.0.0.0, which is a cryptographic module validated under the Korea Cryptographic Module Validation Program (KCMVP), is used. When logging in via a web browser on a personal computer, administrators and end users communicate through a secure channel (HTTPS) supported in the operational environment for the purpose of secure communications.

The TOE is a software-type product installed on a server. The requirements for hardware and software necessary for the operation of the TOE are described below, as well as the requirements for hardware and software of a personal computer used by an end user or an administrator for the management of the TOE.

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

Component			Minimum Requirement
SSO Server	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	1GB or higher
		RAM	8GB or higher
		NIC	10/100/1000 Mbps Ethernet * 1 port or more
	OS		Linux CentOS 7.8 (Kernel 3.10.0) 64bit
	Mandatory Software		JDK : openJDK-1.8.0-262.b10(OpenJSSE 1.1.4) WAS : Tomcat 9.0.50 DBMS : MariaDB 10.6.3 Stable
SSO Agent	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	1GB or higher
		RAM	8GB or higher

		NIC	10/100/1000 Mbps Ethernet * 1 port or more
	OS		Linux CentOS 7.8 (Kernel 3.10.0) 64bit
	Mandatory Software		JDK : openJDK-1.8.0-262.b10(OpenJSSE 1.1.4)

[Table 1] The minimum requirements for TOE

[Table 2] shows minimum requirements for the User(end user, administrator)'s PC.

Component			Minimum Requirement
End User PC and Administrator PC	H/W	CPU	Intel Core2Duo 2.4 GHz or higher
		HDD	100 GB or higher
		RAM	4GB or higher
		NIC	10/100/1000 Mbps Ethernet * 1Port or more
	OS		Windows 10 Pro 64Bit
	Mandatory Software		Chrome v83.0

[Table 2] The minimum requirements for the User(end user, administrator)'s PC

[Table 3] shows external IT entity necessary for the operation of the TOE.

Component	Description and Roles
Mail Server	A server interlinked to send an alarm email to an administrator if an administrator authentication fails, a repository of audit trail is full, or an event that compromises the integrity is detected. The Mail Server supports general commercial mail servers.

[Table 3] External IT entity necessary for the operation of the TOE

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		Bandi SSO v7.0
Version		v7.0.1
TOE Components	SSO Server	Bandi SSO Server v7.0.3
	SSO Agent	Bandi SSO Agent v7.0.1
Guidance documents		Bandi SSO v7.0 OPE v004 Bandi SSO v7.0 PRE v004

[Table 4] TOE identification

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	Bandi SSO v7.0
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
Developer	Bandi S&C Co., Ltd.
Sponsor	Bandi S&C Co., Ltd.
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	September 1, 2021
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 requirements defined in the ST [5].

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

4. Assumptions and Clarification of Scope

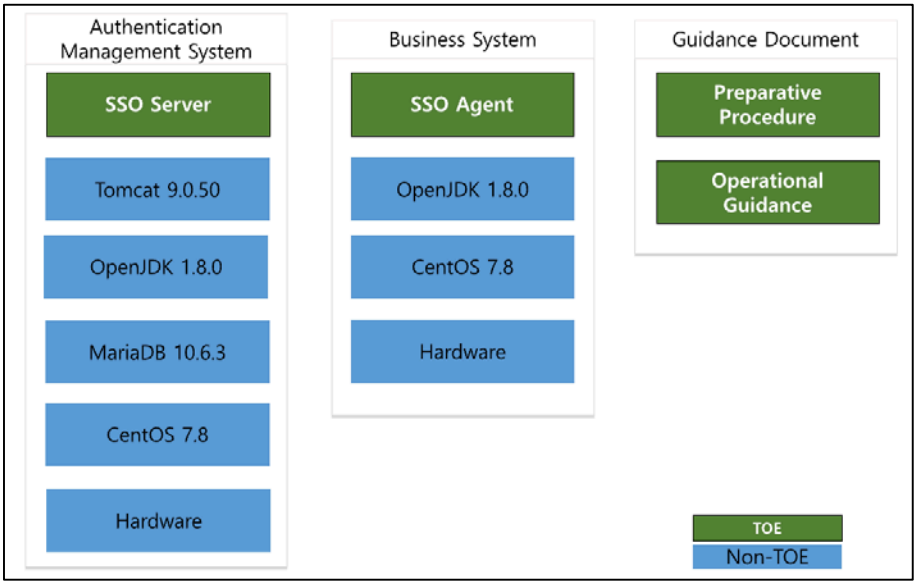
There is no explicit Security Problem Definition chapter, therefore no Assumptions section, in the low assurance ST. Some security aspects of the operational environment are added to those of the PP [4] in which the TOE will be used or is intended to be used (For the detailed and precise definition of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

5. Architectural Information

The physical scope of the TOE includes installation files (SSO Server and SSO Agent) and guidance documents (operational guidance and preparative procedure) provided in the form of software, as described in [Table 4].

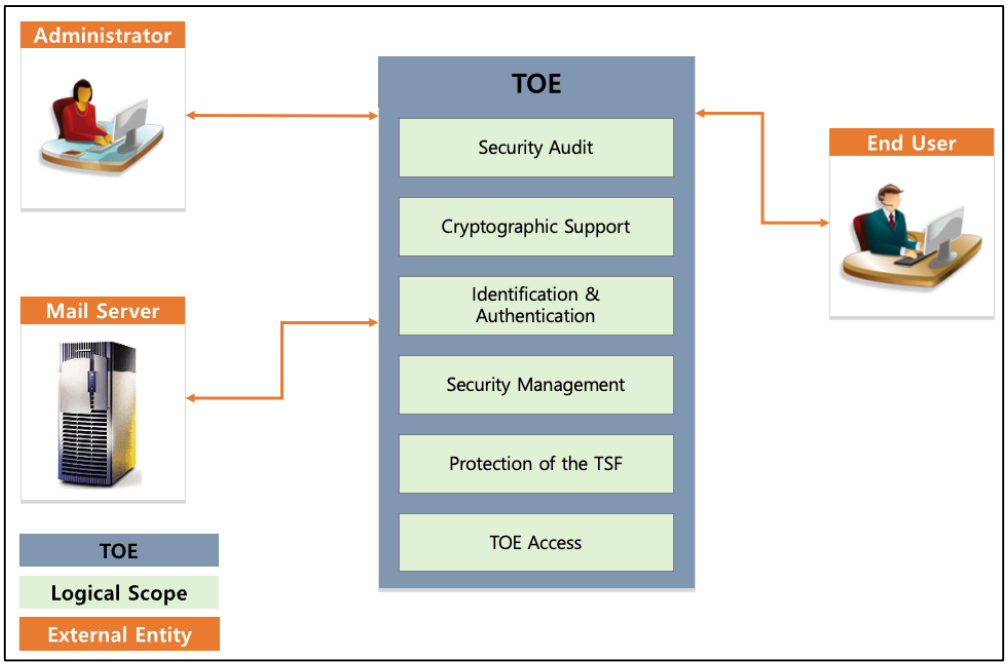
As shown in [Figure 2], hardware, operating system (CentOS 7.8), DBMS (MariaDB 10.6.3), WAS (Tomcat 9.0.50) and openJDK 1.8.0 (OpenJSSE 1.1.4), which are necessary for the operation of the TOE, are out of the physical scope of the TOE.

The physical scope of the TOE is shown in [Figure 2] below:



[Figure 2] Physical scope of the TOE

The logical scope of the TOE is shown in [Figure 3] below:



[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.

Identification	Date
Bandi SSO v7.0 OPE v004 (Bandi_SSO_v7.0_OPE_v004.pdf)	July 13, 2021
Bandi SSO v7.0 PRE v004 (Bandi_SSO_v7.0_PRE_v004.pdf)	July 13, 2021

[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 : Bandi SSO v7.0 (v7.0.1)
- TOE Components : Bandi SSO Server v7.0.3(SSO Server), Bandi SSO Agent v7.0.1 (SSO Agent)

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 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 PPs 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 they are 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 functional specifications specify a high-level description of 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.

9.3 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 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. Also, the evaluator confirmed that the correct version of the software is installed in device. The verdict PASS is assigned to the assurance class ALC.

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 penetrating 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 or by other methods (e.g. by flaw hypotheses), 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 Summar

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
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
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	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 full, 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

Bandi SSO v7.0 Security Target v006 [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
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 3.1 Revision 5, CCMB-2017-04-004, April, 2017

[3] Bandi SSO v7.0, Evaluation Technical Report V1.0, September 1, 2021

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

[5] Bandi SSO v7.0 Security Target v006, August 26, 2021