KECS-CR-21-63

SafeIdentity v5.1

Certification Report

Certification No.: KECS-CISS-1133-2021

2021. 11. 5.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2021.11.05.	-	Certification report for SafeIdentity v5.1 - First documentation

This document is the certification report for SafeIdentity v5.1 of Hancom WITH Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

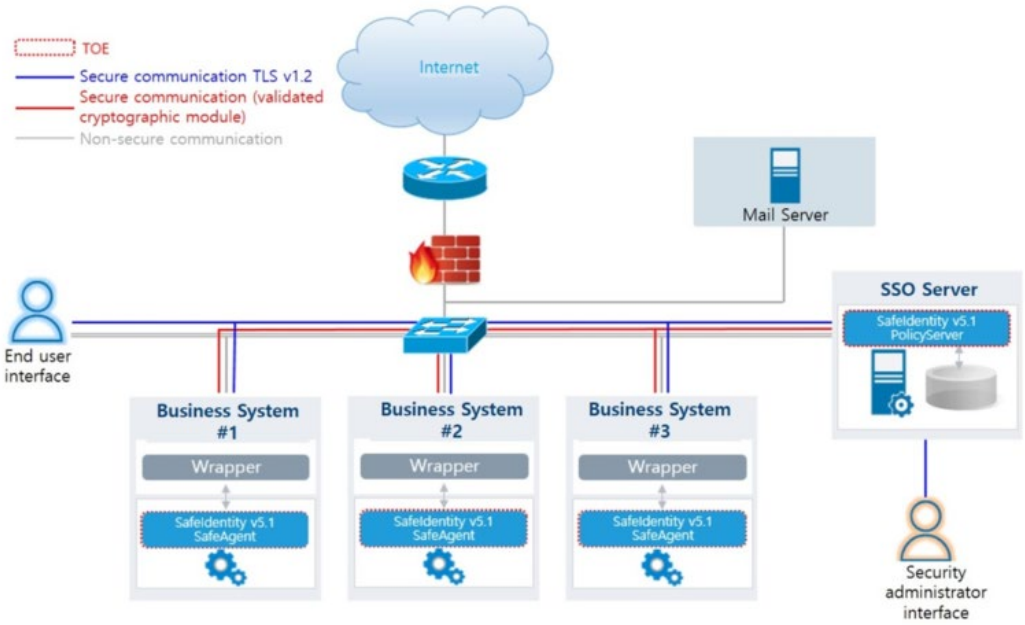
1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the SafeIdentity v5.1 developed by Hancom WITH Inc. 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” hereinafter) 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. Also, the TOE provides a variety of security features: security audit, cryptographic operation using cryptographic module (XecureCrypto v2.0.1.1), identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on October 22, 2021. This report grounds on the Evaluation Technical Report (ETR) [6] KOSYAS had submitted and the Security Target (ST) [7].

The ST claims strict conformance to the Korean National Protection Profile for Single Sign On V1.1 [5]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. 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, therefor the ST, 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. The TOE consists of PolicyServer that processes user login, manages authentication tokens, and establishes the policy, and SafeAgent that is installed in each business system and performs the function of token issuance and verification. PolicyServer is a process type and SafeAgent is an API+ type. The TOE uses cryptographic module validated under Korea Cryptographic Module Validation Program (KCMVP). Wrappers which may be to compatibility with business systems are out of the TOE scope.



[Figure 1] Operational Environment of the TOE

The minimum requirements for hardware, software to install and operate the TOE are shown in [Table 1] below:

Component			Requirement
SafeIdentity v5.1 PolicyServer	HW	CPU	Intel ® Core™ i7 3.4 GHz or higher
		RAM	8 GB or higher
		HDD	100GB or more necessary for the TOE installation
		NIC	100/1000 Ethernet Card 1 port or more
	SW	OS	Solaris 10 (x86_64, 64 bit)
		DBMS	Oracle 12c Version 12.2.0.1.0
		Java	Java(JDK) 1.8.0_301
		WAS	Apache Tomcat 8.5.72
SafeIdentity v5.1 SafeAgent	HW	CPU	Intel ® Core™ i7 3.4 GHz or higher
		Memory	8 GB or higher
		HDD	100GB or more necessary for the TOE installation
		NIC	100/1000 Ethernet Card 1 port or more
	SW	OS	Solaris 10 (x86_64, 64 bit)
		Java	Java(JDK) 1.8.0_301
		WAS	Apache Tomcat 8.5.72

[Table 1] TOE Hardware and Software specifications

Administrator uses the pc that can operate web browser to use the security management. Administrator pc minimum requirements are shown in [Table 2] below:

Component			Requirement
Administrator system	SW	Web Browser	Chrome 94.0

[Table 2] Administrator PC Requirements

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	SafeIdentity v5.1
Version	5.1.02.211001
TOE Components	SafeIdentity v5.1 PolicyServer 5.1.02.211001 SafeIdentity v5.1 SafeAgent 5.1.02.211001
Guidance Documents	SafeIdentity v5.1 Preparative Procedure(PRE) v1.1 SafeIdentity v5.1 Operational Guidance(OPE) v1.1

[Table 3] TOE identification

[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 Regulation for IT Security (May 17, 2021)
TOE	SafeIdentity v5.1
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 V1.1, KECS-PP-0822a-2017
Developer	Hancom WITH Inc.
Sponsor	Hancom WITH Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	October 22, 2022
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [7] by security requirements.

Thus the TOE provides following security features. For more details refer to the ST [7].

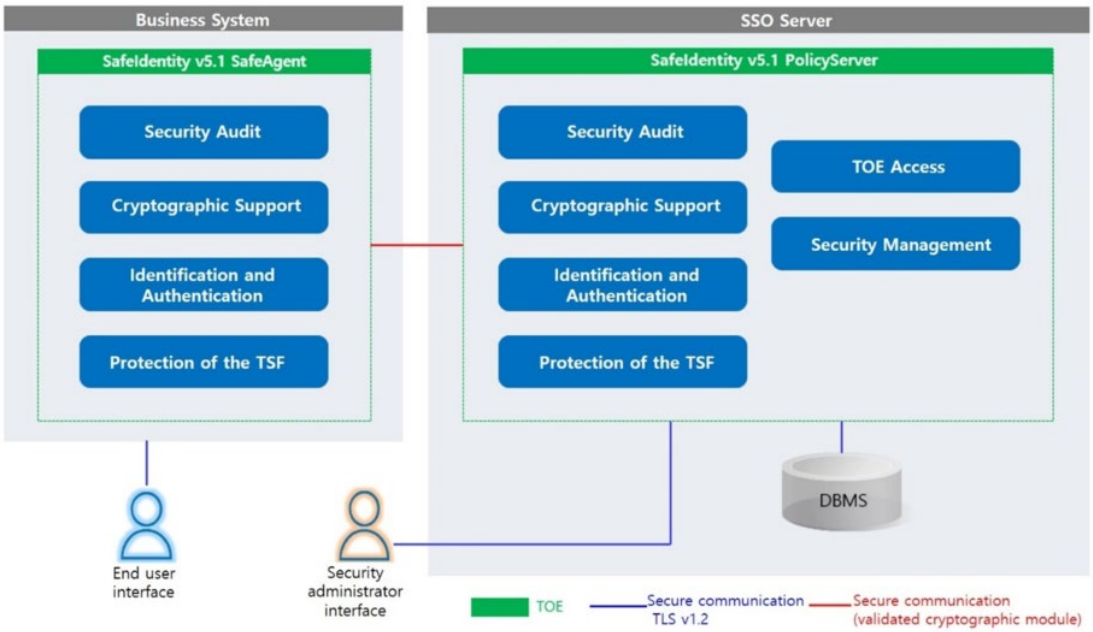
- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Prtoection of the TSF
- TOE Access

4. Assumptions and Clarification of Scope

There are 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 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, chapter 3)

5. Architectural Information

The physical scope of the TOE consists of the SafeIdentity v5.1 PolicyServer 5.1.02.211001, SafeIdentity v5.1 SafeAgent 5.1.02.211001 and guidance. The following security functions are provided by the TOE Logical scope and boundary of TOE is shown in [Figure 2]



[Figure 1] TOE Logical scope

6. Documentation

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

Identifier	Date
SafeIdentity v5.1 Preparative Procedure(PRE) v1.1 (SafeIdentity v5.1 Preparative Procedure(PRE) v1.1.pdf)	October 1, 2021
SafeIdentity v5.1 Operational Guidance(OPE) v1.1 (SafeIdentity v5.1 Operational Guidance(OPE) v1.1.pdf)	October 1, 2021

[Table 5] 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. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- 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 has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: SafeIdentity v5.1(5.1.02.211001)

- SafeIdentity v5.1 PolicyServer 5.1.02.211001
- SafeIdentity v5.1 SafeAgent 5.1.02.211001

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. 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 provided the evaluation result in the ETR [6] 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 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 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.

9.3 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 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.

9.5 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 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		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	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	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	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 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 check 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

SafeIdentity v5.1 Security Target v1.2(ST) 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 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 (May 17, 2021)

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

[6] SafeIdentity v5.1 Evaluation Technical Report Lite V1.00, October 22, 2021

[7] SafeIdentity v5.1 Security Target(ST) v1.2, October 1, 2021