KECS-CR-23-64

INISAFE Nexess V4.3

Certification Report

Certification No.: KECS-CISS-1270-2023

2023. 10. 19.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.10.19.	-	Certification report for INISAFE Nexess V4.3 - First documentation

This document is the certification report for INISAFE Nexess V4.3 of INITECH Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory Co., Ltd. (KSEL)

Table of Contents

1. Executive Summary

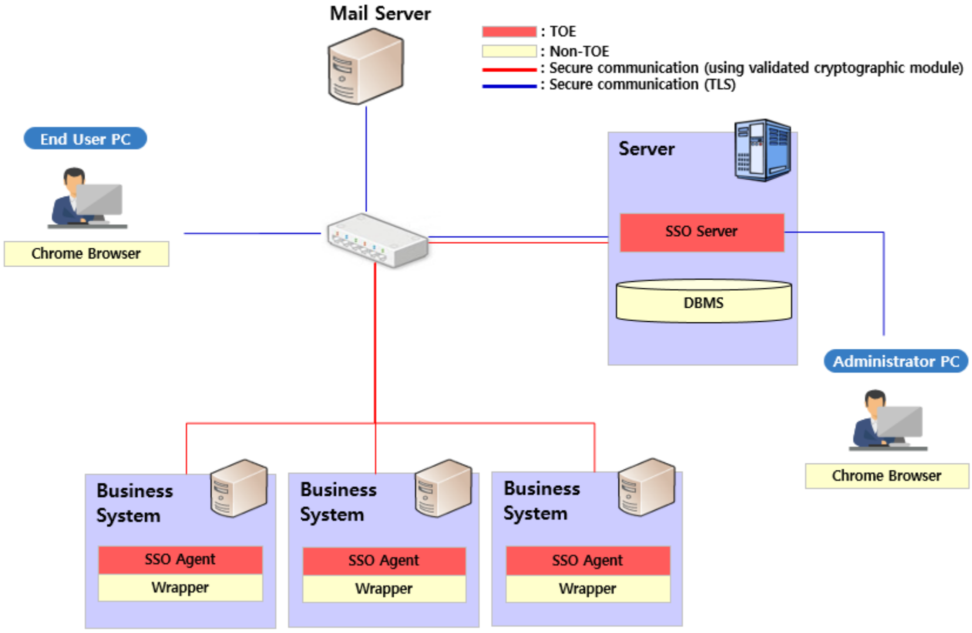
This report describes the certification result drawn by the certification body on the results of the evaluation of INISAFE Nexess V4.3 of INITECH Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and 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 activities. The TOE consists of software components operating as SSO server and SSO Agent. The SSO Server verifies user login attempts using the user information stored in the DBMS. The SSO Agent is installed in each business system and requests user login verification to the SSO Server. The authorized administrator performs the security management by accessing the SSO Server via a web browser. Wrappers which are used to support compatibility with business systems are out of the TOE scope. A mail server is used as an external entity for the operation of the TOE. The TOE uses cryptographic modules validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on 26 September 2023. This report grounds on the evaluation technical report (ETR) KSEL had submitted [5] and the Security Target (ST) [6][7].

The ST claims strict conformance to the Korean National Protection Profile for Single Sign On V1.1 [9]. 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 [9]. 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 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.



[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
SSO Server	CPU	Intel(R) Core(TM) i7-1165G7 2.8Ghz or higher
	RAM	16GB or higher
	HDD	50GB or higher space for installation of SSO Server
	NIC	10/100/1000 X 1Port or higher
	OS	Windows 10 Pro 64bit
	Required S/W	JDK 1.8.0_202 Apache Tomcat 9.0.80 Oracle 19c(19.3)
SSO Agent	CPU	Intel(R) Core(TM) i7-6500U 2.5GHz or higher
	RAM	8GB or higher
	HDD	50GB or higher space for installation of SSO Agent
	NIC	10/100/1000 X 1Port or higher
	OS	Windows 10 Pro 64bit
	Required S/W	JDK 1.8.0_202 Apache Tomcat 9.0.80

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator's PC.

Category	Contents
Required S/W	Chrome 114

[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	INISAFE Nexess V4.3	
Version	V4.3.1.2	
TOE Components	SSO Server	Nexess Server V4.3.1.2 (Nexess_Server_4.3.1.2.zip)
	SSO Agent	Nexess Agent V4.3.1.2 (Nexess_Agent_4.3.1.2.zip)
Guidance Document	CCP.C_NX43_PreparativeProcedure(PRE)_V1.1 (CCP.C_NX43_PreparativeProcedure(PRE)_V1.1.pdf) CCP.C_NX43_OperationalGuidance(OPE)_V1.1 (CCP.C_NX43_OperationalGuidance(OPE)_V1.1.pdf)	

[Table 3] TOE identification

Note that the TOE is delivered contained in a CD-ROM.

[Table 4] 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 Scheme for IT Security (May 17, 2021)
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, December 11, 2019
Developer	INITECH Co., Ltd.
Sponsor	INITECH Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	September 26, 2023
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [6][7] for the TOE claims strict conformance to the National Protection Profile for Single Sign On V1.1 [9], and complies security policies defined in the PP [9] by security requirements. Thus, the TOE provides security features defined in the PP [9] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up/shutdown of the audit functions, integrity violation and self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic operation and cryptographic key management using cryptographic modules (INISAFE Crypto for Java V4.2.0, INISAFE Crypto for C v5.4) validated under the KCMVP.
- Identification and authentication: The TOE identifies and authenticates the administrators and end users using ID/password, mutually authenticate TOE components when they communicate each other, and authenticates end-users based on the authentication token after initial identification and authentication using ID/password.

- Security management: Security management of the TOE is restricted to only the authorized administrator who can access the management interface provided by TOE.
- Protection of the TSF: The TOE provides secure communications amongst TOE components to protect confidentiality and integrity of the transmitted data between them. The TOE also protects TSF data against unauthorized exposure and modification through encryption.
- TOE access: The TOE manages the authorized administrator’s and end user’s access to itself by terminating interactive sessions after defined time interval of their inactivity.

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 [9] 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][7], chapter 3.):

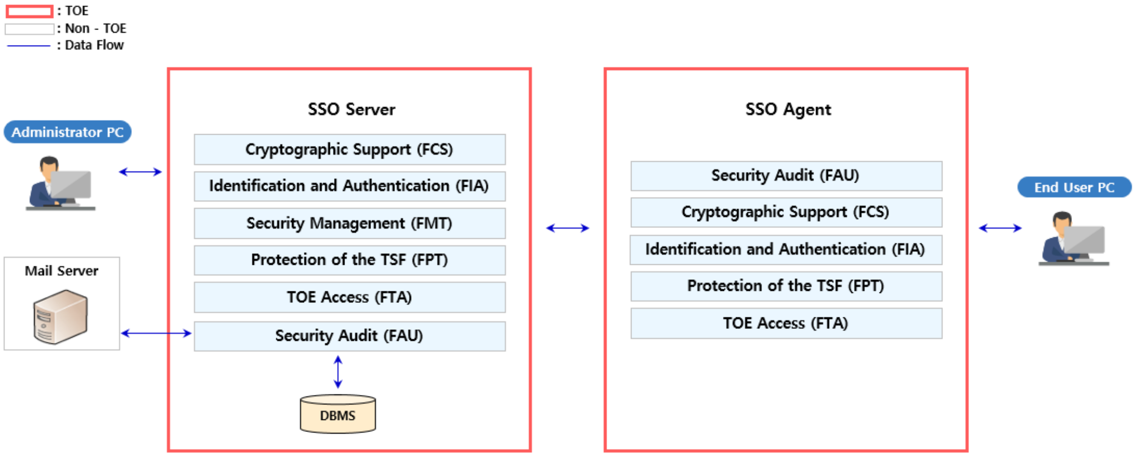
This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4])

5. Architectural Information

The TOE is software consisting of the following components:

- SSO Server, and
- SSO Agent.

Cryptographic modules (INISAFE Crypto for Java V4.2.0, INISAFE Crypto for C v5.4) validated under the KCMVP are embedded in the TOE components.


: TOE
: Non - TOE
: Data Flow
Administrator PC
Mail Server
SSO Server
Cryptographic Support (FCS)
Identification and Authentication (FIA)
Security Management (FMT)
Protection of the TSF (FPT)
TOE Access (FTA)
Security Audit (FAU)
DBMS
SSO Agent
Security Audit (FAU)
Cryptographic Support (FCS)
Identification and Authentication (FIA)
Protection of the TSF (FPT)
TOE Access (FTA)
End User PC

[Figure 2] Architectural Information of the TOE

6. Documentation

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

Identifier	Release	Date
CCP.C_NX43_PreparativeProcedure(PRE)_V1.1	V1.1	August 29, 2023
CCP.C_NX43_OperationalGuidance(OPE)_V1.1	V1.1	August 29, 2023

[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. 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, performed all tests provided by developer, and conducted independent testing based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [6].

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 [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:

- TOE: INISAFE Nexess V4.3
- TOE Components: Nexess Server V4.3.1.2, Nexess Agent V4.3.1.2

The TOE is identified by TOE name and version number including release number. The TOE identification information is provided via GUI and API.

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 [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 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 functional specifications specify the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their purpose, method of use and all 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 uniquely identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration list includes the TOE itself, the evaluation evidence required by the SARs, and the parts that comprise the TOE (required by the PP). Therefore, the verdict PASS is assigned to ALC_CMS.1.

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 TSF, 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	Assurance	Evaluator	Verdict

Class	Component	Action Elements	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 is implemented to ignore audit data without saving it if the audit data storage is saturated. Therefore, when an authorized administrator receives an e-mail notification due to exceeding or saturation of the audit data storage threshold, an audit log backup must be performed immediately to prevent audit data from being lost.
- The authorized administrator must ensure that the password used to generate the key encryption key (KEK) is different from the password used for administrator login, and must not use information that can be easily inferred by an attacker, such as personal information. To ensure the safety of the KEK, it is recommended to set and use the KEK at a level equivalent to the security strength of the administrator's password (set a rule combination of 3 or more of English letters/numbers/special characters and use 9 or more characters).
- SSL communication is implemented to perform secure communication between SSO Server and mail server to send warning mails for security violation events. Authorized administrators should note that a public certificate must be used as the SSL certificate of the mail server that works with SSO Server to send warning mails normally.

11. Security Target

INISAFE Nexess V4.3 Security Target V1.1 [6] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [7] according to the CCRA supporting document ST sanitizing for publication [8].

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level

ETR	Evaluation Technical Report
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

Attack potential	Measure of the effort to be expended in attacking a TOE, expressed as an attacker's expertise, resources and motivation
Authentication token	Authentication data that authorized end-users use to access the business system
Business System	An application server that authorized end users access through 'SSO'
Database Management System (DBMS)	A software system composed to configure and apply the database
Decryption	The act that restores the ciphertext into the plaintext using the decryption key
Encryption	The act of converting the plaintext into the ciphertext using the encryption key
End user	Users of the TOE who want to use the business system, not the administrator of the TOE
Self-test	Pre-operational or conditional test executed by the cryptographic module
TOE Security Functionality (TSF)	Combined functionality of all hardware, software and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs
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 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 (24 August 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] KSEL-CC-2022-07 INISAFE Nexess V4.3 Evaluation Technical Report V1.00, 26 September 2023

[6] INISAFE Nexess V4.3 Security Target V1.1, 4 September 2023 (Confidential Version)

[7] INISAFE Nexess V4.3 Security Target (ST Lite) V1.0, 22 September 2023 (Sanitized Version)

[8] ST sanitizing for publication, CCDB-2006-04-004, April 2006

[9] Korean National Protection Profile for Single Sign On V1.1 (KECS-PP-0822a-2017, December 11, 2019)