KECS-CR-18-36

INISAFE Nexess V4

Certification Report

Certification No.: KECS-CISS-0885-2018

2018. 8. 20.

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2018.08.20.	-	Certification report for INISAFE Nexess V4 - First documentation

This document is the certification report for INISAFE Nexess V4 of INITECH.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

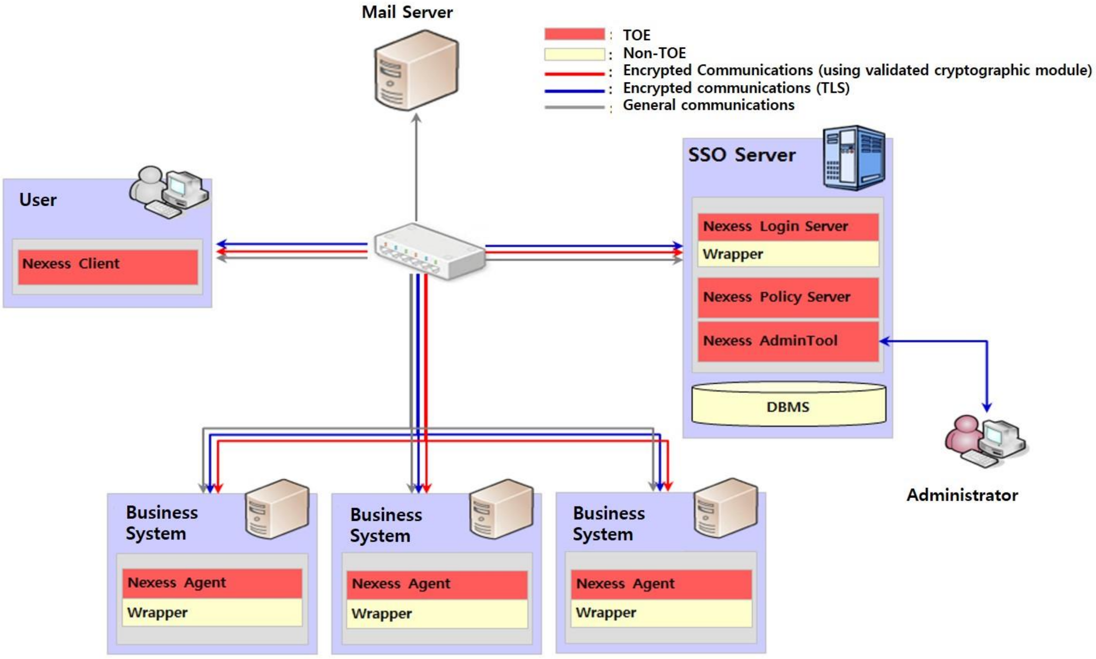
This report describes the certification result drawn by the certification body on the results of the evaluation of INISAFE Nexess V4 of INITECH with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness 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 is comprised of software components operating as Agent - SSO server - Client. The SSO server is comprised of Nexess Policy Server that takes charge of authentication policies, Nexess Login Server that issues and manages authentication tokens, and Nexess AdminTool that takes charge of management/monitoring. It also includes Nexess Client that stores and destroys authentication key/cryptographic key, and Nexess Agent that verifies authentication tokens. The TOE uses cryptographic modules validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on July 13, 2018. This report grounds on the evaluation technical report (ETR) TTA 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 V1.0 [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/DualCore 2.0GHz or higher
	RAM	8GB or higher
	HDD	50GB or higher space for installation of SSO Server
	NIC	10/100/1000 X 1Port or higher
	OS	LINUX - CentOS 7.2 (Kernel 2.6.4) 64bit Windows Server 2012 R2 Standard 64bit
	Required S/W	Java2 Runtime v1.7.0_80 Apache Tomcat 7.0.88 Oracle 12.1.0.2
Nexess Agent	CPU	Intel/DualCore 2.0GHz or higher
	RAM	8GB or higher
	HDD	50GB or higher space for installation of Nexess Agent
	NIC	10/100/1000 X 1Port or higher
	OS	LINUX - CentOS 7.2 (Kernel 2.6.4) 64bit Windows Server 2012 R2 Standard 64bit

	Required S/W	Java2 Runtime v1.7.0_80 Apache Tomcat 7.0.88
Nexess Client	CPU	Intel/DualCore 2.0GHz or higher
	RAM	8GB or higher
	HDD	50GB or higher space for installation of Nexess Client
	NIC	10/100/1000 X 1Port or higher
	OS	Windows 7 Home SP1 32bit
	Required S/W	Microsoft Internet Explorer 11

[Table 1] Hardware and software requirements for the TOE

[Table 2] shows minimum requirements necessary for the administrator's PC to access Nexess AdminTool.

Category	Contents
CPU	Intel/DualCore 2.0GHz or higher
RAM	8GB or higher
HDD	50GB or higher
NIC	10/100/1000 X 1Port or higher
OS	Windows 7 Home SP1 64bit
Required S/W	Internet Explorer 11

[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 libraries consisting of the following software components and related guidance documents.

TOE	INISAFE Nexess V4
Version	V4.2.0.13

TOE Components	SSO Server	Nexess Policy Server V4.2.0.13 Nexess Login Server V4.2.0.13 Nexess AdminTool V4.2.0.13
	Nexess Agent	Nexess Agent V4.2.0.13
	Nexess Client	Nexess Client V4.2.0.13
Guidance Document	CCP.C_NX42_ Preparative Procedures (PRE)_V1.4.pdf CCP.C_NX42_Operational Guidance(OPE)_V1.6.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 (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	INITECH
Sponsor	INITECH
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	July 13, 2018
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 V1.0 [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 such as encryption/decryption and hash, and cryptographic key management such as key generation/distribution/destruction using cryptographic modules (NISAFE Crypto for Java v4.1, INISAFE Crypto for C v5.2.0) 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.

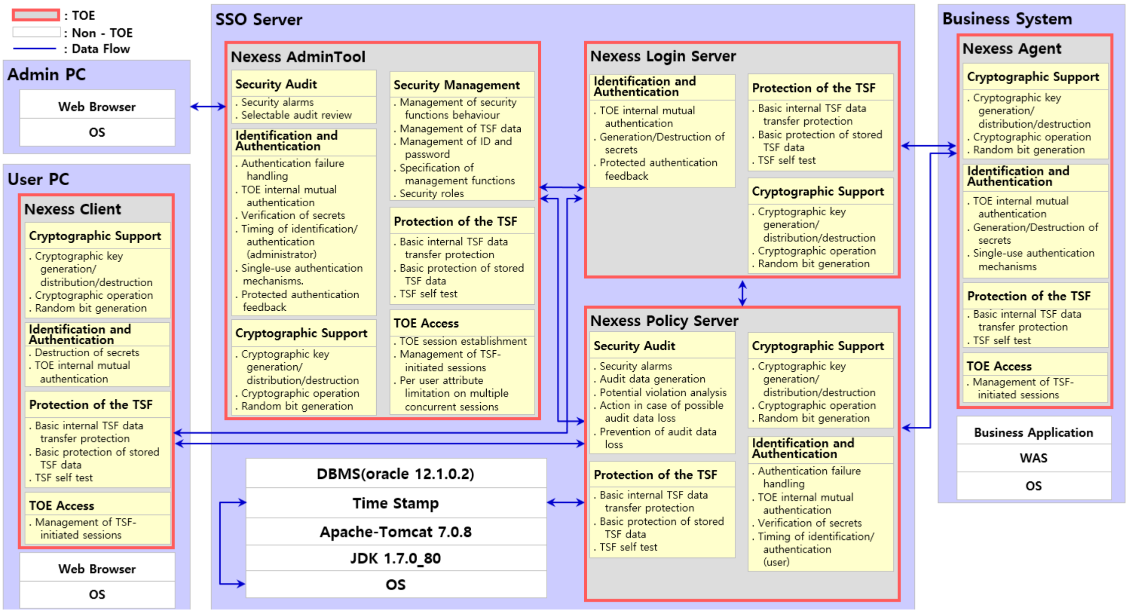
4. Assumptions and Clarification of Scope

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.):

5. Architectural Information

The TOE is software consisting of the following components:

- SSO Server (Nexess Policy Server, Nexess Login Server, Nexess AdminTool),
- Nexess Agent, and
- Nexess Client.


: TOE
: Non - TOE
: Data Flow
Admin PC
Web Browser
OS
User PC
Nexess Client
Cryptographic Support
. Cryptographic key generation/ distribution/destruction
. Cryptographic operation
. Random bit generation
Identification and Authentication
. Destruction of secrets
. TOE internal mutual authentication
Protection of the TSF
. Basic internal TSF data transfer protection
. Basic protection of stored TSF data
. TSF self test
TOE Access
. Management of TSF-initiated sessions
Web Browser
OS
SSO Server
Nexess AdminTool
Security Audit
. Security alarms
. Selectable audit review
Identification and Authentication
. Authentication failure handling
. TOE internal mutual authentication
. Verification of secrets
. Timing of identification/ authentication (administrator)
. Single-use authentication mechanisms.
. Protected authentication feedback
Cryptographic Support
. Cryptographic key generation/ distribution/destruction
. Cryptographic operation
. Random bit generation
Security Management
. Management of security functions behaviour
. Management of TSF data
. Management of ID and password
. Specification of management functions
. Security roles
Protection of the TSF
. Basic internal TSF data transfer protection
. Basic protection of stored TSF data
. TSF self test
TOE Access
. TOE session establishment
. Management of TSF-initiated sessions
. Per user attribute limitation on multiple concurrent sessions
DBMS(oracle 12.1.0.2)
Time Stamp
Apache-Tomcat 7.0.8
JDK 1.7.0_80
OS
Nexess Login Server
Identification and Authentication
. TOE internal mutual authentication
. Generation/Destruction of secrets
. Protected authentication feedback
Protection of the TSF
. Basic internal TSF data transfer protection
. Basic protection of stored TSF data
. TSF self test
Cryptographic Support
. Cryptographic key generation/ distribution/destruction
. Cryptographic operation
. Random bit generation
Nexess Policy Server
Security Audit
. Security alarms
. Audit data generation
. Potential violation analysis
. Action in case of possible audit data loss
. Prevention of audit data loss
Protection of the TSF
. Basic internal TSF data transfer protection
. Basic protection of stored TSF data
. TSF self test
Cryptographic Support
. Cryptographic key generation/ distribution/destruction
. Cryptographic operation
. Random bit generation
Identification and Authentication
. Authentication failure handling
. TOE internal mutual authentication
. Verification of secrets
. Timing of identification/ authentication (user)
Business System
Nexess Agent
Cryptographic Support
. Cryptographic key generation/ distribution/destruction
. Cryptographic operation
. Random bit generation
Identification and Authentication
. TOE internal mutual authentication
. Generation/Destruction of secrets
. Single-use authentication mechanisms
Protection of the TSF
. Basic internal TSF data transfer protection
. TSF self test
TOE Access
. Management of TSF-initiated sessions
Business Application
WAS
OS

[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_NX42_ Preparative Procedures (PRE)_V1.4	V1.4	July 5, 2018
CCP.C_NX42_Operational Guidance(OPE)_V1.6	V1.6	July 10, 2018

[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. 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 installed and prepared the TOE in accordance to the preparative procedures, and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests.

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

8. Evaluated Configuration

The TOE is INISAFE Nexess V4 (version number V4.2.0.13). See table 3 for detailed information on the TOE components.

The TOE is installed from the CD-ROM distributed by INITECH. After installing the TOE, the customer can check the TOE version by command to view each TOE component version and executable file attribute. And the guidance documents listed in this report chapter 5, [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 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 uniquely identified the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.

The configuration list includes the TOE and the evaluation evidence required by the

SARs in the ST. 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 developer has provided 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 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 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.2	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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 shall be located in a physically secure environment to which only the authorized administrator is allowed to access and the protective facilities are provided.
- When the internal network environment changes due to the change in network configuration, increase/decrease of host and increase/decrease of service, etc., the changed environment and security policies must be immediately reflected to the TOE operational policies in order to maintain the same level of security as before.
- When operating the product, the administrator's password should be changed periodically to keep its security.
- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by enhancing against the latest vulnerabilities of the operating system in which the TOE is installed and operated.
- 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 features of the TOE are securely applied in accordance with the requirements of the guidance documents provided with the TOE.
- The authorized administrator shall periodically checks a spare space of audit

data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.

- After installing the product, the administrator must register the administrator's e-mail address in the product so that warning e-mail can be normally sent out in the event of a potential security violation, and confirm that the e-mail address is registered correctly so that the function operates.

11. Security Target

INISAFE Nexess V4 Security Target V1.13 [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
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-users access through ‘SSO’
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 (September 12, 2017)

[5] TTA-CCE-17-012 INISAFE Nexess V4 Evaluation Technical Report V1.5, August 16, 2018

[6] INISAFE Nexess V4 Security Target V1.13, August 13, 2018 (Confidential Version)

[7] INISAFE Nexess V4 Security Target(ST Lite) V1.13, August 13, 2018 (Sanatized Version)

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

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