INITECH
1st Financial & Security Service

Security Target

INISAFE Nexess V4

INITECH Co., Ltd.

Revision History

Ver	Date	Author	Revision
1.0	Oct.11, 2017	Yujong Min	Initial release
1.1	Mar.30, 2018	Yujong Min	Modification to incorporate findings of the observation report (EOR-1st)
1.2	Apr. 6, 2018	Yujong Min	Modification to incorporate findings of the observation report (EOR -2nd)
1.3	May 2, 2018	Yujong Min	Modification to incorporate findings of the observation report (EOR -4th)
1.4	May 23, 2018	Yujong Min	Partial modification (cryptographic key distribution, etc.)
1.5	May 25, 2018	Yujong Min	Modification of encryption (mutual authentication)-related content
1.6	Jun. 1, 2018	Yujong Min	Incorporation of the review result dated May 29
1.7	Jun. 25, 2018	Yujong Min	Incorporation of the review result and updates
1.8	Jun. 29, 2018	Yujong Min	Incorporation of the review result and updates
1.9	Jul. 3, 2018	Yujong Min	Incorporation of the review result and updates
1.10	Jul. 5, 2018	Yujong Min	Incorporation of the review result and updates
1.11	Jul. 10, 2018	Yujong Min	Incorporation of the review result and updates
1.12	Jul. 27, 2018	Yujong Min	Incorporation of the result of review by the Certificate Authority (1st)
1.13	Aug. 13, 2018	Yujong Min	Incorporation of the result of review by the Certificate Authority (2nd)

Table of Contents

List of Figures

List of Tables

1. ST Introduction

This chapter introduces the Security Target (ST) of INISAFE Nexess V4 of INITECH Co., Ltd.

1.1. ST Reference

[Table 1] ST Reference

Title	INISAFE Nexess V4 Security Target (ST_lite)
Version	V1.13
Author	Yujong Min of INITECH Co., Ltd.
Publication Date	August 13, 2018
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 • Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5 (CCMB-2017-04-001, April, 2017) • Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5 (CCMB-2017-04-002, April, 2017) • Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5 (CCMB-2017-04-003, April, 2017)
Evaluation Assurance Level	EAL1+(ATE_FUN.1)
Configuration Management No.	CCP.C_NX42_Security Target (ST_lite)_V1.13
Product Classification	Single Sign-On (SSO)
Keywords	Single Sign-on, SSO

1.2. TOE Reference

[Table 2] TOE Reference

TOE Identification	INISAFE Nexess V4
TOE Version	V4.2.0.13
TOE Developer	INITECH Co., Ltd.
TOE Component	Nexess Policy Server V4.2.0.13 Nexess Login Server V4.2.0.13 Nexess Client V4.2.0.13 Nexess Agent V4.2.0.13 Nexess AdminTool V4.2.0.13
Final release	July 10, 2018

1.3. TOE Overview

1.3.1. Single Sign-On Overview

INISAFE Nexess V4 (hereinafter referred to as the TOE) is used to provide services from various application servers (business systems) for a user with a single login (Single Sign-On) without additional login activities. The TOE performs user identification and authentication, authentication token issuance and validation in accordance with user authentication policies.

1.3.2. TOE Type and Scope

The TOE consists of the software necessary for constructing Single Sign-On. The TOE is built with an agent - SSO server - client method. SSO server is comprised of Nexess Policy Server in charge of authentication policies, Nexess Login Server that issues and manages authentication tokens and Nexess AdminTool that performs the administration/monitoring function. It also includes Nexess Client that is in charge of storing and destroying authentication key/cryptographic key and Nexess Agent that verifies authentication tokens. The TOE is required to use a validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP).

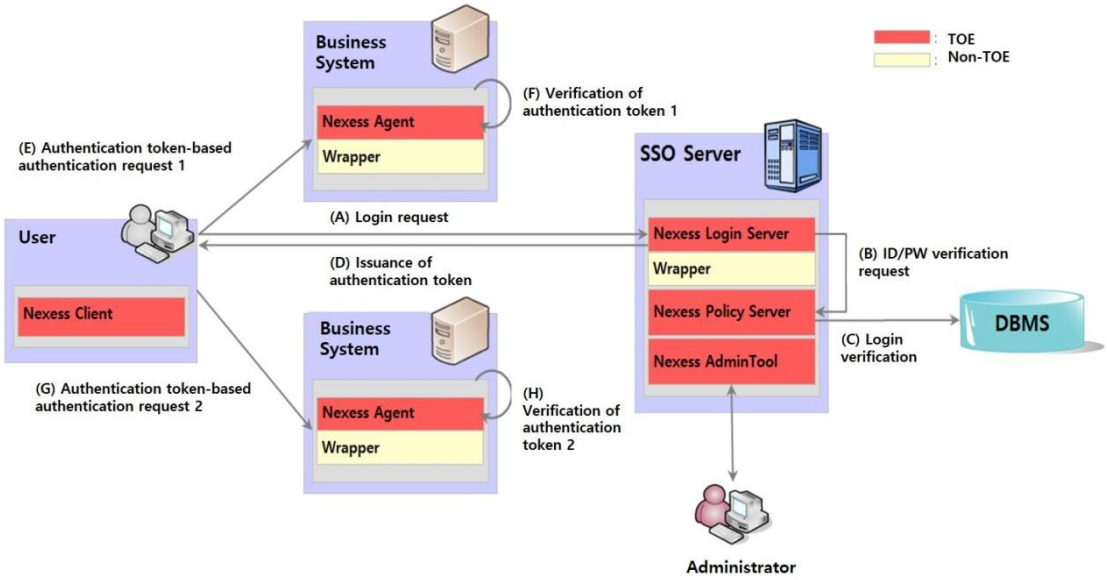
1.3.3. TOE Usage and Major Security Features

The TOE is a Single Sign-On system in the form of software that permits access to multiple application servers with a single user login. A user who uses SSO requests a login with

ID/password. Then, Nexess Policy Server and Nexess Login Server are linked with DBMS where user information is stored and perform login verification. If the login is valid, Nexess Login Server issues an authentication token and sends it to Nexess Client and the user's web browser cookie, thereby controlling the access by verifying the authentication token when the user requests access to another business system. In this case, the verification of the authentication token and parts of authentication token update (the time of authentication) can be performed in Nexess Agent.

Furthermore, the TOE provides the security audit function that manages major events by recording them as audit data when the security function and the administrative function are invoked; the identification and authentication function such as verification of an identity of an authorized user and continuous authentication failure; the function that protects data stored inside and outside the TOE; and the TSF protection function such as TSF self tests. Also, it offers the cryptographic support function that performs cryptographic key management and cryptographic operation; the security management function for the definition of security functions/roles and configuration; and the TOE access function to control access sessions of the authorized administrator.

The user identification and authentication procedure of the TOE is shown below in (Figure 1) and can be mainly divided into two stages: the stage in which a user is authenticated through ID and password input in the beginning and then an authentication token is generated, and the stage in which access to the relevant business system is made after the authentication token is generated, the authentication token is verified and then the user accesses the business system.



(Figure 1) User Identification and Authentication Procedure

The initial user accesses Nexess Login Server through a web browser. Then, ID and password are received from the user and verified through Nexess Policy Server. Once the authentication succeeds, an authentication token is issued to the user through Nexess Login Server. The generated authentication token is stored in the web browser cookie and Nexess Client in a distributed manner. A cryptographic key necessary for generating an authentication token is generated per user in Nexess Policy Server at the time of login. When an authentication token is generated through the initial user authentication, the user accesses a business system that he/she wants to access through his/her web browser. Nexess Agent in the API form verifies an authentication token that was completed in combination of the browser's authentication token and Nexess Client's authentication token. As to a cryptographic key and an authentication key necessary for the authentication token verification, a key that was generated in Nexess Policy Server upon login is provided. The authentication token is automatically destroyed upon logout from Nexess Client.

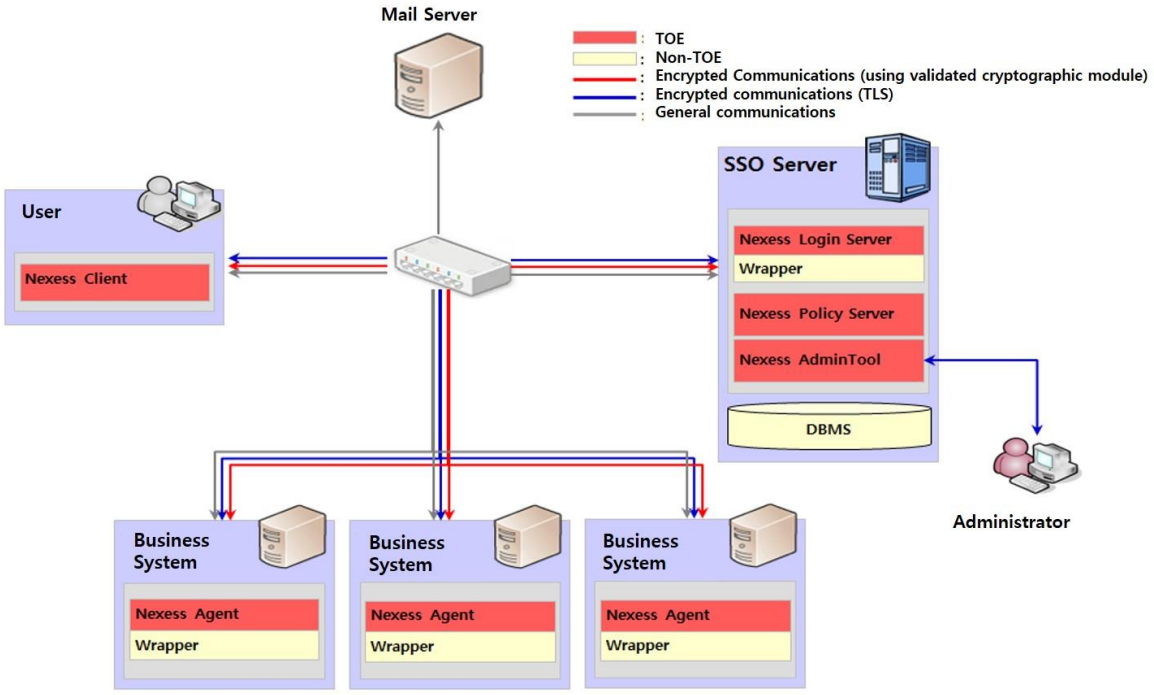
[Table 3] Procedure for Actions in Each Authentication Stage

Authentication Stage	Procedure for Actions
Initial Authentication	(A)Login request → (B)ID/PW verification request → (C)Login verification → (D)Issuance of authentication token
Authentication Token-based Authentication	(E)Authentication token-based authentication request 1 → (F)Authentication token verification 1
	(G)Authentication token-based authentication request 2 → (H)Authentication token verification 2

In addition, the subjects that issue/store/verify an authentication token are as described below. The encryption communications and technologies applied to the systems necessary for the issuance of authentication tokens are described in [Table 7] that shows encryption communications and technologies of the TOE components.

- Subject of the issuance of authentication token: Nexess Login Server
- Container of authentication token: User PC web browser + Nexess Client
- Subject of the verification of authentication token: Nexess Agent

1.3.4. Non-TOE and TOE Operational Environment



(Figure 2) TOE Operational Environment

The operational environment of the TOE is shown in (Figure 2) TOE Operational Environment. It consists of SSO Server, Nexess Agent and Nexess Client. SSO Server uses user information stored in DBMS to offer the functions such as verification of user's login, generation of authentication tokens and policy establishment. Nexess Policy Server is in charge of generating/distributing/destroying cryptographic keys necessary for the generation of authentication tokens. Nexess Agent performs the verification of issued authentication tokens and is provided in the form of API, a library file format, for each business system.

The TOE is a software-type product installed and operated on commercial hardware and an operating system platform. The requirements for non-TOE hardware/software that is essential elements in operating the product but does not fall under the scope of the TOE are as follows.

[Table 4] Requirements for Non-TOE Operational Environment

Type	TOE Name	Requirements for Operational Environment	
SSO Server	Nexess Policy Server Nexess Login Server Nexess AdminTool	S/W	- Java2 Runtime v1.7.0_80 - Apache Tomcat 7.0.88 - Oracle 12.1.0.2
		H/W	- Processor: Intel/DualCore 2.0GHz or higher - Memory: 8GB or higher - Hard disk: 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
Agent	Nexess Agent	S/W	- Java2 Runtime v1.7.0_80 - Apache Tomcat 7.0.88
		H/W	- Processor: Intel/DualCore 2.0GHz or higher - Memory: 8GB or higher - Hard disk: 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
Client	Nexess Client	S/W	- Microsoft Internet Explorer 11
		H/W	- Processor: Intel/DualCore 2.0GHz or higher - Memory: 8GB or higher - Hard disk: 50GB or higher space for installation of Nexess Client - NIC: 10/100/1000 X 1Port or higher
		OS	- Windows 7 Home SP1 32bit

[Table 5] External Entity for the Performance of Security Functions of the TOE

Type	Description and Role
Mail Server	3rd Party Mail Server A link is established to send an alarm email to an administrator in case an administrator authentication is failed, the repository of audit trail is full or an event that compromised the integrity occurs. Mail Server supports general commercial mail servers.

An administrator requires the following operational environment in order to access the TOE. Microsoft Internet Explorer 11 must be installed on the administrator PC in order to access Nexess AdminTool through which the administrator performs a role of SSO Server configuration, status check, audit log search, etc.

[Table 6] Requirements for Operational Environment for Administrator

Type	Item	Description
Administrator PC	S/W	- Microsoft Internet Explorer 11
	H/W	- Processor: Intel/DualCore 2.0GHz or higher - Memory: 8GB or higher - Hard disk: 50GB or higher - NIC: 10/100/1000 X 1Port or higher
	OS	- Windows 7 Home 64bit

For the encryption of the communications used in data transfer between TOE components (mutual authentication between components), cryptographic algorithms from INISAFE Crypto for Java V4.1 and INISAFE Crypto for C V5.2, which are cryptographic modules validated by KCMVP, are used. The confidentiality and the integrity of the communication section is ensured by using a private certificate method. When logging in through a web browser on a PC, administrators and users perform communications through a secured channel (HTTPS) supported in the operational environment for the purpose of secured communications.

[Table 7] Validated Cryptographic Module and Cryptographic Algorithm Identification of TOE Component

Type	Description		Remarks
Validated Cryptographic Module	Java	NISAFE Crypto for Java v4.1	Validation date: Dec. 16, 2014 Validation No.: CM-97-2019.12
	C/C++	INISAFE Crypto for C v5.2.0	Validation date: Apr. 25, 2014 Validation No.: CM-89-2019.4
Mutual Authentication between Component	-	Private Key/Public Key-based RSA	- Nexess Policy Server ↔ Nexess Login Server - Nexess Policy Server ↔ Nexess AdminTool - Nexess Policy Server ↔ Nexess Agent - Nexess Policy Server ↔ Nexess Client
Data Protection on Web	-	SSL(TLSv1.2)	- Web browser on Admin PC ↔ Nexess AdminTool - Web browser on User PC ↔ Nexess Login Server
Cryptograp	Symmetric	SEED/CBC	Encryption and decryption of authentication

hic Algorithm	Key Cryptographic Operation	128bit	token Encryption and decryption of TSF data
	Asymmetric Key Cryptographic Operation	RSA 2048 bit	Mutual authentication and session key exchange between TOE components
	HMAC	HMAC-SHA256	Integrity of authentication token
	Random	HASH-DRBG-SHA256	Issuance of authentication token key Generation of cryptographic key
	HASH	SHA-256	User password hash TSF data integrity verification

1.4. TOE Description

The TOE is a Single Sign-On system in the form of software that permits access to multiple application servers with a single user login.

A user who uses the TOE requests a login with ID/password. Then, Nexess Policy Server and Nexess Login Server, linked with the area where user information is stored, perform login verification. If the login is valid, Nexess Login Server issues an authentication token and sends it to Nexess Client, thereby controlling the access by verifying the authentication token when the user requests access to another business system. In this case, some of the issuance and the verification of authentication tokens can be performed in Nexess Agent.

[Table 8] TOE Components

Classification	Description	
Nexess Policy Server	Type	Software
	Function	1. Cryptographic key management - Cryptographic key management in relation to authentication token generation and encryption/decryption of TSF data

		2. Nexess Agent verification 3. Monitoring/log management - TOE status monitoring - Log policy change and establishment 4. Cryptographic key generation/distribution/destruction 5. Cryptographic operation for mutual authentication
Nexess Login Server	Type	Software
	Function	1. Cryptographic operation - Authentication token generation/modification /deletion 2. User identification - Provision of GUI for user identification 3. Audit log generation 4. Cryptographic operation for mutual authentication
Nexess Client	Type	Software
	Function	1. User identification and authentication 2. Cryptographic operation for mutual authentication
Nexess Agent	Type	Software
	Function	1. Cryptographic operation - Verification of authentication token 2. Cryptographic operation for mutual authentication
Nexess AdminTool	Type	Software
	Function	1. Administrator identification and authentication 2. Nexess Agent management - Registration/deletion 2. User/administrator management - Addition/modification/deletion 3. Monitoring/log query - TOE status monitoring - Action log query 5. Audit log query 4. Cryptographic operation for mutual authentication

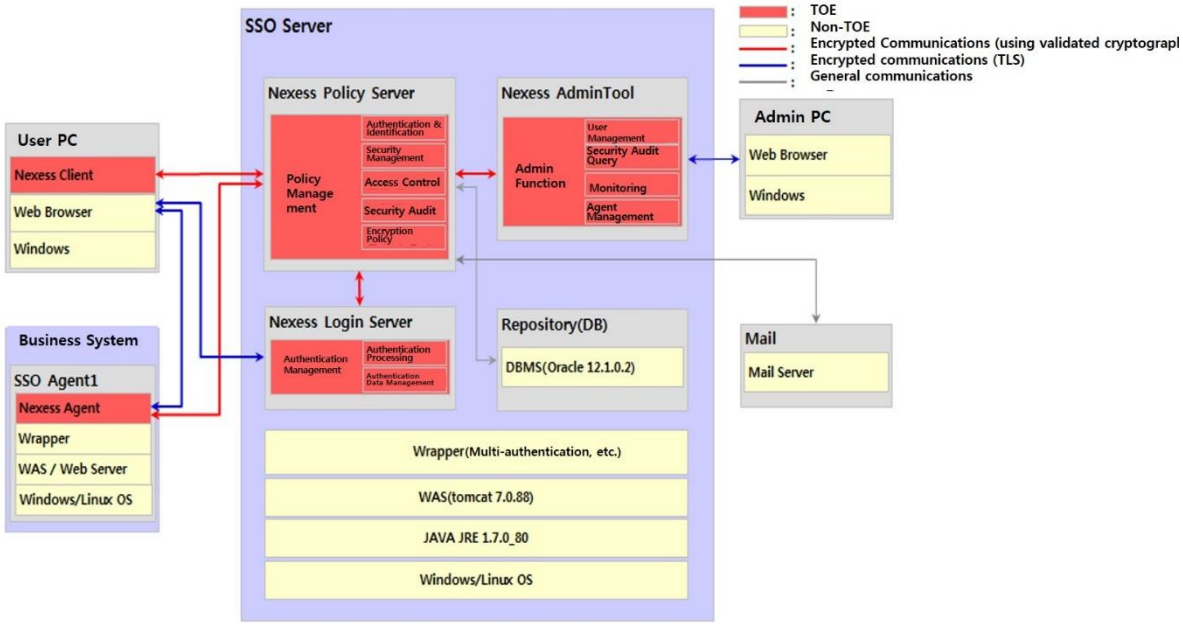
1.4.1. Physical Scope of the TOE

The product offered to consumers and the TOE components are divided into essential software for Nexess Policy Server, Nexess Login Server, Nexess AdminTool and Nexess Agent, preparative procedures, operational guidance and wrapper as shown below.

[Table 9] Physical Composition of the Product and the TOE

Composition	Type	Element			Within TOE Scope
CD-ROM (1EA)	S/W	Installation Program	Nexess Policy Server	Nexess_PolicyServer_4.2.0.13.zip	O
			Nexess Login Server	Nexess_LoginServer_4.2.0.13.zip	O
			Nexess AdminTool	Nexess AdminTool_4.2.0.13.zip	O
			Nexess Client	Nexess Client_4.2.0.13.zip	O
			Nexess Agent	Nexess_Agent_4.2.0.13.zip	O
			Nexess Agent Wrapper	Nexess_Agent_Wrapper.zip	X
			Nexess Login Server Wrapper	Nexess_LoginServer_Wrapper.zip	X
	Electronic Document (PDF)	Guidance Document	CCP.C_NX42_ Preparative Procedures (PRE)_V1.4.pdf		O
			CCP.C_NX42_Operational Guidance(OPE)_V1.6.pdf		O
Certificate	Certificate	Software License Certificate			X

The physical scope of the TOE refers to the physical boundary of the TOE covered by the evaluation. It consists of software necessary for the operation, which are Nexess Policy Server, Nexess Login Server, Nexess AdminTool, Nexess Agent and Nexess Client, and non-TOE operational environment, and is structured as follows.

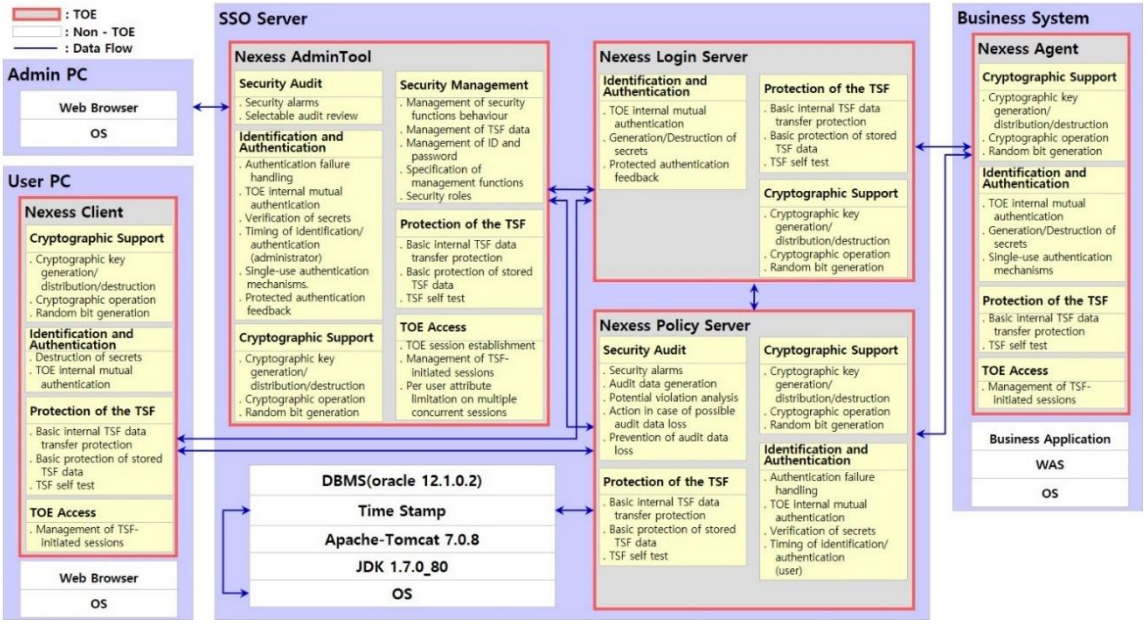


(Figure 3) Physical Scope of the TOE

INISAFE Nexess V4 product includes Nexess Policy Server, Nexess Login Server, Nexess AdminTool, Nexess Agent and Nexess Client, which are the software developed by INITECH, together with the preparative procedures, the operational guidance document for users and Wrapper. Its CD does not provide separate WAS and DBMSD, the 3rd party software necessary for the installation and the operation.

Non-TOE operational environments such as hardware, operating system, web application server, database, java runtime environment, SSL environment and web browser are excluded from the physical scope of the TOE.

1.4.2. Logical Scope of the TOE



(Figure 4) Logical Scope of the TOE

The security functions provided by the TOE are as follows:

1) Nexess Policy Server

- Security Audit (FAU)

  Nexess Policy Server provides the functions of detecting potential violations regarding security relevant actions and generating audit records. Records are generated for all actions made by users in a chronological order. Audit records are stored in the DBMS through Nexess Policy Server. Also, in case the audit data reaches the threshold (90%), it is notified to the administrator via email, and in case the audit data exceeds the threshold, audited events are ignored. Regarding the time used in audit records, timestamps are provided by the reliable operating system.

- Cryptographic Support (FCS)

  Nexess Policy Server uses an approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP) and provides the functions of cryptographic key management (generation, distribution and destruction) and cryptographic operation including symmetric/asymmetric key cryptography and hash performed for TOE internal mutual authentication, protection of transmitted data, protection of stored TSF data (Nexess Policy Server configuration file) and generation of cryptographic keys to authentication tokens. Also, it uses a random bit generator validated by the Korea Cryptographic Module Validation Program (KCMVP) in generating cryptographic keys and generating authentication tokens.

- Identification and Authentication (FIA)

  Nexess Policy Server performs the identification and authentication based on ID and password in order to verify the end users. If the identification and authentication attempts are unsuccessful for a defined number of times (five times by default), the TOE performs the function of locking an end user account so that the TOE is protected against adverse attempts of user authentication. Locked user accounts are unlocked by an authorized administrator or are automatically unlocked after a specified period of time (10 minutes by default).

  Nexess Policy Server performs mutual authentication by means of certificate through public key cryptographic algorithm (RSA) using the validated cryptographic module approved by the KCMVP in order to ensure secure communications and mutual authentication among TOE components (Nexess Login Server, Nexess AdminTool, Nexess Agent and Nexess Client).

- Protection of the TSF (FPT)

  Nexess Policy Server offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the validated cryptographic module approved by the KCMVP.

  Nexess Policy Server performs TSF self tests and conducts the integrity verification for configuration files and TSF executable code. The integrity verification is conducted upon the initial execution, on a periodic basis and at the request of the administrator. If a test result finds abnormal performance, it is notified to the administrator. In addition, it protects stored TSF data such as TOE set value.

2) Nexess Login Server

- Identification and Authentication (FIA)

  Nexess Login Server does not provide feedback on authentication failure during the authentication of an end user.

  Nexess Login Server performs mutual authentication by means of certificate through public key cryptographic algorithm (RSA) using the validated cryptographic module approved by the KCMVP in order to ensure secure communications and mutual authentication between Nexess Policy Servers.

  Nexess Login Server generates authentication tokens in accordance with the defined criteria, enforces the use of authentication tokens during the user identification and authentication and destroys used tokens so that they cannot be re-used.

- Cryptographic Support (FCS)

  Nexess Login Server uses an approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP) and provides the functions of cryptographic key management (generation, distribution, destruction) and cryptographic operation including symmetric/asymmetric key cryptography and hash performed for TOE

internal mutual authentication, protection of transmitted data, protection of stored TSF data (Nexess Login Server configuration file) and generation of cryptographic keys. Also, it uses a random bit generator validated by the Korea Cryptographic Module Validation Program (KCMVP) in generating cryptographic keys and generating authentication tokens.

- Protection of the TSF (FPT)
  Nexess Login Server offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the validated cryptographic module confirmed by the KCMVP.
  Nexess Login Server performs TSF self tests and conducts the integrity verification for configuration files and TSF executable code. The integrity verification is conducted upon the initial execution, on a periodic basis and at the request of the administrator. If a test result finds abnormal performance, it is notified to the administrator. In addition, it protects stored TSF data such as TOE set value.

3) Nexess AdminTool

- Security Audit (FAU)
  Nexess AdminTool provides the authorized administrator with the function of reviewing all audit data, and the function of selective viewing of audit data according to the logic relation criteria .

- Identification and Authentication (FIA)
  Nexess AdminTool performs the identification and authentication based on ID and passwords in order to verify the administrators. In the process of the identification and authentication, passwords being entered are masked (password masking with *) to prevent them from being disclosed. The TOE verifies the combination rules and lengths of passwords that will be used for authentication and does not provide feedback on authentication failure during the authentication. Also, it prevents the reuse of the administrator authentication data. If identification and authentication attempts are unsuccessful for a defined number of times (five times by default), the TOE performs the function of account locking so that the TOE is protected against adverse attempts of administrator authentication. Locked administrator accounts are unlocked automatically after a specified period of time (10 minutes by default). It performs mutual authentication between Nexess Policy Servers.

- Security Management (FMT)
  The security management function allows for setting and management of security functions provided by the TOE, TSF data and so forth.
  - Security Management Function: It enables an administrator to manage security functions. The TOE provides the function of managing and monitoring security policies (user

management, business system management, etc.) and viewing audit data.

- TSF Data Management: The TOE manages TSF data. TSF data provides the function of managing security policies (user management, business system management, XML setting, etc.) and viewing audit data.
- Security Password Management: It provides the authorized administrator with the function of managing changes in the password combination rules, and enforces the change of the default password upon the initial authentication of the administrator.
- Security Role Management: The authorized roles of the TOE are classified into security administrator (top administrator, general administrator). Top administrator can perform all web security management functions while a general administrator has the read access right to parts of web security policies only.

- Cryptographic Support (FCS)

  Nexess AdminTool uses an approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP) and provides the functions of cryptographic key management (generation, distribution, destruction) and cryptographic operation including TOE internal mutual authentication, protection of transmitted data and protection of stored TSF data (Nexess AdminTool configuration file). Also, it uses a random bit generator validated by the Korea Cryptographic Module Validation Program (KCMVP) in generating cryptographic keys and generating authentication tokens.

- TSF Protection (FPT)

  Nexess AdminTool offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the validated cryptographic module confirmed by the KCMVP.

  Nexess AdminTool performs TSF self tests and conducts the integrity verification for configuration files and TSF executable code. The integrity verification is conducted upon the initial execution, on a periodic basis and at the request of the administrator. If a test result finds abnormal performance, it is notified to the administrator. In addition, it protects stored TSF data such as TOE set value.

- TOE Access (FTA)

  Nexess AdminTool terminates the session by making a request to WAS if the session is not active for a certain period of time (default value : 10 minutes). The maximum number of concurrent sessions of management access by an administrator that belong to the same administrator is limited to one. An administrator's management session establishment is denied based on access IP.

4) Nexess Agent

- Identification and Authentication (FIA)

  Nexess Agent performs the verification of the authentication token that is transmitted when an end user accesses the business system so that only an authorized user can access the business system. After the verification, it destroys an authentication token whose use was terminated in order to prevent the reuse of the authentication data of end user. The TOE also performs mutual authentication among Nexess Policy Servers.

- Cryptographic Support (FCS)

  Nexess Agent uses an approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP) and provides the functions of cryptographic key management (generation, distribution, destruction) and cryptographic operation including TOE internal mutual authentication, protection of transmitted data and encryption of symmetric/asymmetric key performed for the verification of authentication tokens and hash. Also, it uses a random bit generator validated by the Korea Cryptographic Module Validation Program (KCMVP) in generating cryptographic keys.

- TSF Protection (FPT)

  Nexess Agent offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the validated cryptographic module confirmed by the KCMVP, and performs TSF self tests (cryptographic module self-testing).

- TOE Access (FTA)

  Nexess Agent terminates the end user session if the end user does not access the business system for a certain period of time (default value: 50 minutes).

5) Nexess Client

- TSF Protection (FPT)

  Nexess Client offers the confidentiality and the integrity for the communication of inter-TOE components by performing cryptographic communication through the validated cryptographic module confirmed by the KCMVP.

  Nexess Client performs TSF self tests and conducts the integrity verification for configuration files and TSF executable code. The integrity verification is conducted upon the initial execution, on a periodic basis and at the request of the administrator. In addition, it protects stored TSF data such as TOE set value.

- Identification and Authentication (FIA)

  Nexess Client performs mutual authentication between Nexess Policy Servers. An authentication token is destroyed upon the end user logout or process termination.

- Cryptographic Support (FCS)
  Nexess Client uses an approved cryptographic algorithm of the validated cryptographic module whose security and implementation conformance have been confirmed by the Korea Cryptographic Module Validation Program (KCMVP) and provides the functions of cryptographic key management (generation, distribution, destruction) and cryptographic operation including symmetric/asymmetric key cryptography and hash performed for TOE internal mutual authentication, protection of transmitted data and protection of stored TSF data. Also, it uses a random bit generator validated by the Korea Cryptographic Module Validation Program (KCMVP) in generating cryptographic keys.

- TOE Access (FTA)
  Nexess Client terminates the session if it is inactive for a certain period of time (default value : 10 minutes).

1.5. Conventions

The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.
The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

Iteration
Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.). For example, it is indicated as FAU_SAR.3(1) and FAU_SAR.3(2).

Assignment
This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

Selection
This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

Refinement
This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text.**

1.6. Terms and Definitions

Terms used in this ST, which are the same as in the CC, must follow those in the CC.

Private Key
A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Object
Passive entity in the TOE, that contains or receives information, and upon which subjects

perform operations

Approved mode of operation

Operation mode of a cryptographic module using an approved cryptographic algorithm

Approved cryptographic algorithm

Cryptographic algorithm selected by the cryptographic module verification institution, considering the safety, the reliability, the interoperability and other factors in relation to block cipher, hash function, message authentication code, random bit generator, key setting, public key cryptography and digital signature cryptographic algorithm

Validated Cryptographic Module

Cryptographic module validated and approved by the cryptographic module verification institution, and to which a validation number was assigned

Public Security Parameters (PSP)

Security-relevant public information whose modification may compromise the security of a cryptographic module

Public Key

Cryptographic key used together with an asymmetric cryptographic algorithm and is uniquely combined with a single entity (the subject that uses the public key). It can be disclosed.

Public Key (Asymmetric) Cryptographic Algorithm

Cryptographic algorithm that uses a pair of a public key and a private key

Attack Potential

Measure of the effort to be expended in attacking the TOE, expressed in terms of an attacker's expertise, resources and motivation

Management Access

Access attempts made by an administrator using HTTPS, SSH, TLS, etc. for the purpose of the management of the TOE

Management Console

Application program that provides an administrator with graphic user interface (GUI) or command line interface (CLI) for system management, configuration and so forth

Random Bit Generator (RBG)

Device or algorithm that outputs statistically independent and unbiased binary digits. The RBG used for cryptographic application generally generates 0 and 1 bit strings, and the sequence can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic types. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a "seed key," and the non-deterministic type RBG generates the output dependent on unpredictable physical sources.

Symmetric Cryptographic Technique

Cryptographic technique that uses the same secret key on both encryption and decryption mode. It is also called secret key cryptographic technique.

Iteration

Use of the same component to express two or more distinct requirements

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Security Policy Document

Document presented in the list of the validated cryptographic modules, together with the module names. This document summarizes and specifies cryptographic module types, approved cryptographic algorithms and operational environments provided by cryptographic modules.

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Decryption

Restoration of the ciphertext into the original plaintext by using a decryption key

Secret Key

Cryptographic key used together with a secret key cryptographic algorithm and uniquely

combined with one or multiple entities. It must not be disclosed.

User

See "external entity." In the TOE, user means authorized administrator and authorized end user.

Selection

Specification of one or more items from a list in a component

Identity

Representation uniquely identifying authorized users. It can be a real name, abbreviated name or alias of the user.

Encryption

An act of converting the plaintext into the ciphertext using an encryption key

Korea Cryptographic Module Validation Program (KCMVP)

Scheme to validate the security and implementation conformance of cryptographic modules used for the protection of important but not classified information among the data communicated through the information and communication network of the government and public institutions

Business System

Application server that an authorized end user intends to access through Single-Sign On

Element

Indivisible statement of a security need

Role

Predefined set of rules establishing the allowed interactions between a user and the TOE

Operation (on a component of the CC))

Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on a subject)

Specific type of action performed by a subject on an object

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Threat Agent

Unauthorized external entity that can pose illegitimate threats such as adverse access, modification or deletion to an asset

Authorized Administrator

Authorized user who securely operates and manages the TOE

Authorized User

User who may, in accordance with the Safety Functional Requirements (SFR), perform an operation

End User

User, not an authorized administrator of the TOE, who intends to use a business system

Authentication Data

Information used to verify the claimed identity of a user

Authentication Token

Authentication data used for access by an authorized end user to a business system

Self-test

Pre-operational or conditional test executed by the cryptographic module

Assets

Entities that the owner of the TOE presumably places value upon

Refinement

Addition of details to a component

Dependency

Relationship between components such that if a requirement based on the depending

component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Subject

Active entity in the TOE that performs operations on objects

Sensitive Security Parameters (SSP)

Critical security parameter (CSP) and public security parameter (PSP)

Augmentation

Addition of one or more requirement(s) to a package

Component

Smallest selectable set of elements on which requirements may be based

Client

Application program that can access SSO server or an agent service through a network

Class

Set of CC families that share a common focus

Family

Set of components that share a similar goal but differ in emphasis or rigor

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

Evaluation Assurance Level (EAL)

Set of assurance requirements drown from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Assignment

The specification of an identified parameter in a component (of the CC) or requirement

Critical Security Parameters (CSP)

Security-related information whose disclosure or modification can compromise the

security of a cryptographic module (e.g. secret key/private key, password or authentication data such as PINs)

Application Programming Interface (API)

A set of system libraries that exist between the application layer and the platform system and enables the easy development of the application running on the platform

Database Management System (DBMS)

Software system that was built to construct and apply the database

Kerberos

Centralized authentication protocol that provides user authentication by using symmetric key cryptography in a distributed computing environment. It is defined in RFC 1510.

Remote Authentication Dial-In User Services (RADIUS)

Execution of user identification and authentication by sending user ID, password, IP address or other information upon access request from a user in a remote place

Secure Sockets Layer (SSL)

Security protocol adopted by Netscape in order to provide the security including confidentiality and integrity in a computer network

Terminal Access Controller Access Control System (TACACS)

Common authentication protocol in UNIX network in which a remote access server sends user logon password to an authentication server. It is defined in RFC 1492.

Transport Layer Security (TLS)

SSL-based cryptographic authentication communication protocol between a server and a client. It is defined in RFC 2246.

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 (Security Functional Requirements)

TSF Data

Data generated by the TOE and for the TOE, which can affect the operation of the TOE

Wrapper

Interface to connect the TOE and various types of business systems or authentication systems

1.7. Security Target Contents

This document is structured as below:

Chapter 1 Introduction describes the Security Target and TOE reference, TOE overview, TOE description, convention and terms and definitions.

Chapter 2 Conformance Claims describes the conformance with the Common Criteria, protection profile and package and presents the conformance rationale and protection profile conformance statement.

Chapter 3 explains threats that can be posed to the TOE assets or environments, organizational security policies such as rules, procedures or guidelines that the TOE shall comply with for the security, and the security regarding the TOE environment.

Chapter 4 defines the security objectives for the operational environment supported by the operational environment in order to provide the security functionality of the TOE in an accurate manner.

Chapter 5 defines the extended components additionally needed according to the features of Single Sign-On.

Chapter 6 Security Requirements describes security functional requirements and security assurance requirements.

Chapter 7 describes the TOE summary specification.

2. Conformance Claim

2.1. CC Conformance Claim

This ST conforms to the Common Criteria for Information Technology Security Evaluation V3.1 Part 2 and Part 3 (Notification No. 2013-51 of the Ministry of Science, ICT and Future Planning).

[Table 10] CC Conformance Claim

Common Criteria		Common Criteria for Information Technology Security Evaluation V3.1R5 - Common Criteria Part 1: Introduction and General Model V3.1r5, (CCMB-2017-04-001, 2017. 4) - Common Criteria Part 2: Security Functional Components V3.1r5, (CCMB-2017-04-002, 2017. 4) - Common Criteria Part 3: Security Assurance Components V3.1r5, (CCMB-2017-04-003, 2017. 4)
Conformance Claim	**Part 2 Security Functional Requirements**	Extended: FCS_RBG.1, FIA_IMA.1, FIA_SOS.3, FMT_PWD.1, FPT_PST.1, FTA_SSL.5
	Part 3 Security Assurance Requirements	Conformant
	Package	Augmented: EAL1 augmented(ATE_FUN.1)

2.2. PP Conformance Claim

This ST strictly conforms to the "National Protection Profile for Single Sign-On V1.0."

- PP Title and Version: National Protection Profile for Single Sign-On V1.0
- Certificate No/Date: KECS-PP-0822-2017/2017-08-18
- Publication Date: 2017-08-18
- Evaluation Assurance Level: EAL1+
- Conformance Type: Strict PP conformance

2.3. Package Conformance Claim

This ST claims conformance to assurance requirement package EAL1 and additionally defines some assurance requirements.

- Assurance package: EAL1 augmented(ATE_FUN.1)

2.4. Conformance Claim Rationale

Since this ST adopts the TOE type, security problem definition, security objectives and security requirements in the same way as the Protection Profile, it is demonstrated that this ST strictly conforms to the "National Protection Profile for Single Sign-On V1.0."

2.5. PP Conformance Statement

Since this ST adopts the TOE type, security objectives and security requirements in the same way as the Protection Profile, it is demonstrated that this ST strictly conforms to the "National Protection Profile for Single Sign-On V1.0."

[Conformance Rationale]

- OE is augmented against the security objectives of the operational environment defined in the PP to which this ST conforms.
    - OE. Secure DBMS: OE augmented with conformance to PP selection SFR FAU_STG.1 requirement
    - OE. Time Stamp: OE augmented with conformance to PP selection SFR FPT_STM.1 requirement
    - OE. Secure Channel: OE augmented with conformance to PP selection SFR FPT_TRP.1 requirement

3. Security Objectives

This ST defines the security objectives for the operational environment only. The security objectives for the operational environment are those handled by IT area or non-technical/procedural methods.

3.1. Security Objectives for the Operational Environment

[Table 11] Identification of Security Objectives for the Operational Environment

TOE Security Objective	Description
OE.PHYSIAL_CONTROL	The place where SSO Agent and SSO Server, among the TOE components, are installed and operated shall be equipped with access control and protection facilities so that it is accessible only by an authorized administrator.
OE.TRUSTED_ADMIN	An authorized administrator of the TOE shall not have malicious intentions, shall be properly trained for the TOE management functions and shall accurately fulfill the duties in accordance with the administrator guidance
OE.LOG_BACKUP	An authorized administrator shall check the spare space in the audit data repository on a periodic basis in preparation for audit record loss and carry out audit data backup (external log server, separate storage device, etc.) to prevent audit data loss.
OE.OPERATION_SYSTEM_REINFORCEMENT	An authorized administrator of the TOE shall ensure the reliability and the security of the operating system by taking reinforcement measures for the operation system on which the TOE is installed and operated to address the latest vulnerability.
OE.SECURE_DEVELOPMENT	A 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 specified in the guidance document provided with the TOE.

OE.SECURE_DBMS	Security policies and audit records stored in the TOE are stored in the database. The database shall not be generated, modified or deleted without a request from the TOE.
OE.TIME_STAMP	The TOE shall accurately record security-relevant events by using reliable time stamps provided by the TOE operational environment.
OE.SECURE_CHANNEL	A secure path shall be ensured by the security policy of WAS in case of end user authentication or TOE administrator's UI access and use via a web browser on an authorized user's PC.

4. Extended Components Definition

This ST strictly conforms to the extended components defined in the "National Protection Profile for Single Sign-On V1.0." The following are the extended components defined in the "National Protection Profile for Single Sign-On V1.0."

4.1. FCS, Cryptographic Support

4.1.1. Random Bit Generation

Family Behaviour

This family (FCS_RBG, Random Bit Generation) family defines requirements for the capability that generates random numbers required for TOE cryptographic operation.

Component Levelling

FCS_RBG: Random bit generation	1

FCS_RBG.1 Random bit generation requires the TSF to provide the capability that generates random numbers required for TOE cryptographic operation.

Management: FCS_RBG.1
There are no management activities foreseen.

Audit: FCS_RBG.1
There are no auditable events foreseen.

FCS_RBG.1 **Random bit generation**
Hierarchical to No other components
Dependencies No dependencies

FCS_RBG.1.1 The TSF shall generate random numbers by using the specified random bit generator that meets the following [assignment: *list of* standards].

4.2. FIA, Identification & Authentication

4.2.1. TOE Internal Mutual Authentication

Family Behaviour

This family (FIA_IMA, TOE Internal mutual authentication) defines requirements for providing mutual authentication between TOE components in the process of user identification and authentication.

Component Levelling

FIA_IMA: TOE internal mutual authentication	1

FIA_IMA.1 TOE Internal Mutual Authentication requires that mutual authentication between TOE components is provided in the process of user identification and authentication.

Management: FIA_IMA.1
There are no management activities foreseen.

Audit: FIA_IMA.1
It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: Success and failure of mutual authentication

FIA_IMA.1 **TOE Internal mutual authentication**
Hierarchical to No other components
Dependencies No dependencies

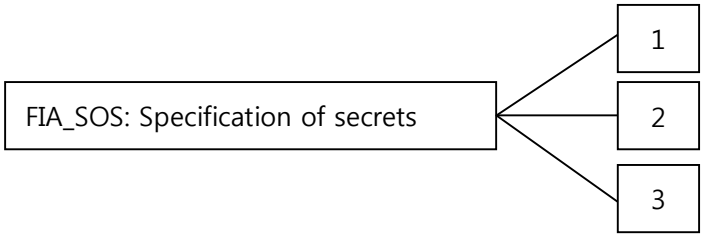
FIA_IMA.1.1 The TSF shall perform mutual authentication between [assignment: *different parts of the TOE*] by [assignment: *authentication protocol*] that meets the following: [assignment: *list of standards*].

4.2.2. Specification of Secrets

Family Behaviour

This family (FIA_SOS, Specification of Secrets) defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

Component Levelling



In CC Part 2, the family of specification of secrets is composed of two components. Since the "National Protection Profile for Single Sign-On V1.0" augmented one extended component as below, the family is composed of three components.
※ Description of two components included in CC Part 2 is left out of this ST.

FIA_SOS.3 Destruction of secrets requires that secrets are destroyed in accordance with the specified destruction method. The specified destruction method may be based on the assigned standards.

Management: FIA_SOS.3
There are no management activities foreseen.

Audit: FIA_SOS.3
It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: Success and failure of an action

FIA_SOS.3 Destruction of secrets
Hierarchical to No other components
Dependencies FIA_SOS.2 Generation of secrets

FIA_SOS.3.1 The TSF shall destroy secrets in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

4.3. FMT, Security Management

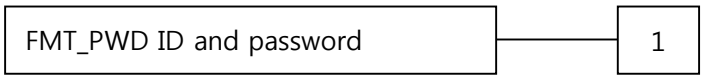
4.3.1. ID and Password

Family Behaviour

This family (FMT_PWD, ID and password) defines requirements for functions to control the

management of ID and password that an authorized user uses in the TOE and to set or modify ID and/or password.

Component Levelling



FMT_PWD.1 Management of ID and password requires that the TSF provides the ID and password management function.

Management: FMT_PWD.1
The following management functions could be considered in FMT.

a) Management of ID and password configuration rules

Audit: FMT_PWD.1
It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All changes of the password

FMT_PWD.1 Management of ID and password

Hierarchical to	No other components
Dependencies	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized roles*] as follows:
1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized roles*].
1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the function for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the*

first time].

4.4. FPT, Protection of the TSF

4.4.1. Protection of Stored TSF Data

Family Behaviour

This family (FPT_PST, Protection of Stored TSF data) defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Component Levelling

FPT_PST Protection of stored TSF data	1

FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.

Management: FPT_PST.1
There are no management activities foreseen.

Audit: FPT_PST.1
FAU There are no auditable events foreseen.

FPT_PST.1	**Basic protection of stored TSF data**	
	Hierarchical to	No other components
	Dependencies	No dependencies

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

4.5. FTA, TOE Access

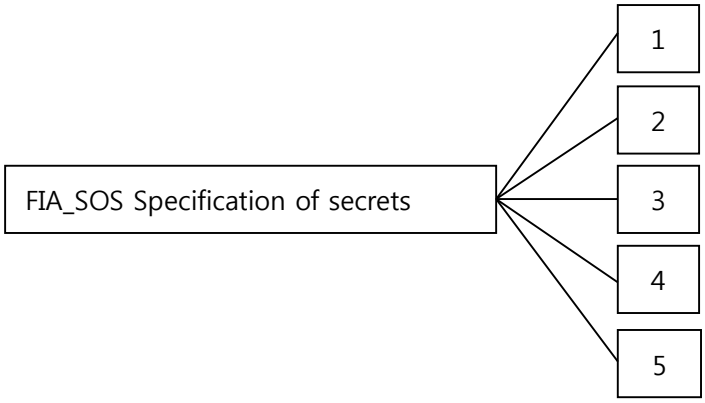
4.5.1. Session Locking and Termination

Family Behaviour

This family (FTA_SSL, Session Locking and termination) defines requirement for the TSF to

provide the capability for TSF-initiated and user-initiated locking, unlocking and termination of sessions.

Component Levelling



In CC Part 2, the family of session locking and termination is composed of four components. Since the "National Protection Profile for Single Sign-On V1.0" augmented one extended component as below, the family is composed of five components.
※ Description of four components included in CC Part 2 is left out of this ST.

FTA_SSL.5 The management of TSF-initiated sessions provides requirements that the TSF locks or terminates the session after a specified time period of user inactivity.

Management: FTA_SSL.5
The following actions could be considered for the management functions in FMT:
a) Specification of the time period of user inactivity that results in session locking or termination for each user
b) Specification of the default user inactivity period that results in session locking or termination

Audit: FTA_SSL.5
It is recommended that the following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Minimal: Locking or termination of interactive sessions

FTA_SSL.5	**Management of TSF-initiated sessions**
Hierarchical to	No other components
Dependencies	FIA_UAU.1 Authentication or No dependencies

FTA_SSL.5.1 TSF shall [selection:

- *lock the session and/or re-authenticate the user before unlocking the session,*
- *terminate*] an interactive session after a [assignment: *time period of user inactivity*].

5. Security Requirements

The security requirements describe security functional requirements and assurance requirements that must be satisfied by the TOE that claims conformance to this ST.

5.1. Security Functional Requirements

All subjects, objects, operations, security attributes and external entities used in the security requirements in this ST are defined as follows:

a) External entity

- Mail Server: Mail Server is used to perform the function to send an appropriate notification to an authorized administrator regarding detection of access by end users, details of access request and so on.

Security requirements in this ST consist of functional components described in Common Criteria (CC V3.1) Part 2. Security functional components are summarized as follows:

[Table 12] Summary of Security Functional Components

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (authentication token)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (authentication token)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(Extended)	Random bit generation
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(Extended)	TOE internal mutual authentication

(FIA)	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	Generation of secrets
	FIA_SOS.3(Extended)	Destruction of secrets
	FIA_UAU.1	Timing of authentication (end user)
	FIA_UAU.2	User authentication before any action (administrator)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification (user)
	FIA_UID.2	User identification before any action (administrator)
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(Extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(Extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF self test
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(Extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

5.1.1. Security Audit (FAU)

FAU_ARP.1 **Security alarms**

Hierarchical to : No other components

Dependencies : FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [actions against security violations in [Table 13]] upon detection of a potential security violation.

[Table 13] Actions against Security Violations

Security Violation	Action
Accumulation of authentication failures specified in FIA_UAU.1	· Limitation on login attempts for a specified period of time (default: 10 minutes) for end users
Accumulation of authentication failures specified in	· Limitation on login attempts for a

FIA_UAU.2	specified period of time (default: 10 minutes) for the administrator · Sending a warning email to the administrator
Integrity violation event and failure of self test that requires validation specified in FPT_TST.1	· Sending a warning email to the administrator
Audit trail exceeding certain pre-defined limits specified in FAU_STG.3	· Sending a warning email to the administrator
Predicted audit data loss specified in FAU_STG.4	· Sending a warning email to the administrator · Ignoring an audited event

FAU_GEN.1 Audit data generation

Hierarchical to : No other components

Dependencies : FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Refer to "auditable event" in [Table 14] Auditable Event]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success of failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [refer to "Additional Audit Record" in [Table 14] Auditable Event, *N/A*]

[Table 14] Auditable Event

Security Functional Component	Auditable Event	Additional Audit Record
FAU_ARP.1	Actions taken due to potential security violations	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms, Automated responses performed by the tool	
FAU_STG.3	Actions taken due to exceeding of a threshold	
FAU_STG.4	Actions taken due to the audit storage failure	

FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity (applied only to distribution of key related to encryption/decryption of TSF data)	
FCS_CKM.4	Success and failure of the activity (applied only to distribution of key related to encryption/decryption of TSF data)	
FCS_COP.1	Success and failure of cryptographic operation, and the type of cryptographic operation (applied only to items related to issuance, storage, verification and deletion of authentication token)	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	
FIA_SOS.2	Rejection by the TSF of any tested secret	
FIA_SOS.3(Extended)	Success and failure of the activity (applied only to destruction of SSO authentication token)	
FIA_UAU.1	All use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UID.1	All use of the administrator identification mechanism, including the administrator identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified values of TSF data
FMT_PWD.1(Extended)	All changes of the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the user group of rules divided	
FPT_TST.1	Execution of the TSF self tests and the results of the tests	Modified TSF data or executable code in case of integrity violation
FTA_MCS.2	Denial of a new session based on the limitation	

	of multiple concurrent sessions	
FTA_SSL.5	Locking or termination of interactive session	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism All attempts at establishment of a user session	

FAU_SAA.1 Potential violation analysis

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [Authentication failure audit event among auditable events in FIA_UAU.2, Failure of self test of approved cryptographic module and integrity violation event among auditable events in FPT_TST.1, Audit storage capacity exceeding among auditable events in FAU_STG.3, Full audit storage in FAU_STG.4] known to indicate a potential security violation;

b) [Any other audit event rules including potential violation]

[

- FIA_UAU.1: Five times of duplicated authentication failure among audit events of authentication failure of end user
- FIA_UAU.2: Five times of duplicated authentication failure among audit events of authentication failure of administrator
- FAU_STG.3: Audit trail exceeding 90 percent of the threshold

]

FAU_SAR.1 Audit review

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide the [authorized administrator] with the capability to read [all the audit data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to : No other components

Dependencies : FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [the following methods of selection and/or ordering] of audit data based on [the following criteria with logical relations].

[

- Criteria with logical relations: [Table 15] Audit Data Type and Selection Criteria
- Methods of selection and/or ordering: Ordering in the descending order based on the time of audit data log generation

]

[Table 15] Audit Data Type and Selection Criteria

Audit Data Type	Selection Criteria	Allowable Ability
Administrator activity log	Date and time of event (start date – end date)	Search, sort (according to the time of occurrence)
	User ID	
	Type	
	Status	
System audit log	Date and time of event (start date – end date)	Search, sort (according to the time of occurrence)
	Keyword	
Administrator login log	Status	Search, sort (according to the time of occurrence)
	Admin ID	
	Date and time of event (start date – end date)	
Nexess log	Date and time of event (start date – end date)	Search, sort (according to the time of occurrence)
Abnormal access audit log	Date and time of event (start date – end date)	Search, sort (according to the time of occurrence)

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to : No other components

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [notice to the authorized administrator, [N/A]] if the audit trail exceeds [the percentage of the spare space against the total capacity of the

audit record storage (default value 90%, the range of values that the authorized administrator is able to set 1% - 90%)].

FAU_STG.4 Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *ignore audited events* and [notify the authorized administrator via email] if the audit trail is full.

5.1.2. Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic key generation (authentication token)

Hierarchical to : No other components

Dependencies : [FCS_CKM.2 Cryptographic key distribution

FCS_COP.1(1) Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_RBG.1 Random bit generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["algorithm" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Sizeand specified "cryptographic key sizes" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Sizethat meet the following ["list of standards" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Size].

[Table 16] Authentication Token Cryptographic Key Algorithm and Key Size

List of Standards	Encryption Method	Algorithm	Cryptographic Security	Cryptographic Key Size	Usage
TTAK.KO-12.0190	Symmetric Key Encryption	SEED(CBC)	128	128	Generation and verification of authentication token
ISO/IEC 9797-2	Message Authentic	HMAC-SHA-256	128	128	Integrity verification of authentication token

	ation Code				

FCS_CKM.1(2) Cryptographic key generation (TSF data encryption)

Hierarchical to : No other components

Dependencies : [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1(2) Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FCS_RBG.1 Random bit generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ["algorithm" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size] and specified cryptographic key sizes ["cryptographic key size" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size] that meet the following ["list of standards" in in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size].

[Table 17] TSF Data Cryptographic Key Algorithm and Key Size

List of Standards	Encryption Method	Algorithm	Cryptographic Key Size	TOE Component	Key Type and Description	Generation Method
TTAK.KO-12.0190	Symmetric Key Encryption	SEED (CBC)	128	Nexess Policy Server Nexess Login Server Nexess AdminTool Nexess Client	Master Key: Used when storing security policy encryption	Using a random bit generator
TTAS.KO-12.0004/R1	Symmetric Key Encryption	SEED (CBC)	128	Nexess Policy Server Nexess Login Server Nexess AdminTool Nexess Client	For encryption when storing Master Key	In-house implementation (combination of system information and TOE executable code hash

						value)
ISO/IEC 10118-3	Hash	SHA-256	N/A	Nexess Policy Server Nexess Login Server Nexess AdminTool Nexess Client	User password hash, TSF and TSF data integrity monitoring, etc.	N/A
TTAS.KO-12.0004/R1	Symmetric Key Encryption	SEED (CBC)	128	Communication between TOE components	Session Key: Used for encryption between TOE components	Using a random bit generator
ISO/IEC 18033-2	Public Key Encryption	RSAES	2048	Communication between TOE components	For Session Key encryption	Using RSA key generation algorithm

Application notes: Master Key and key for encryption when storing Master Key (KEK) are generated upon the initial installation of the TOE

FCS_CKM.2 Cryptographic key distribution

Hierarchical to : No other components

Dependencies : **FCS_CKM.1(1) Cryptographic key generation**
FCS_CKM.1(2) Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ["distribution method" in [Table 18] Cryptographic Key Distribution Method] that meets the following ["list of standards" in in [Table 18] Cryptographic Key Distribution Method].

[Table 18] Cryptographic Key Distribution Method

List of Standards	Origin	Destination	Distribution Target	Distribution Method
N/A (In-house	Nexess Policy	Nexess Login Server	Authentication token	Distributed through cryptographic

implementation)	Server	Nexess Agent	cryptographic key Authentication token integrity verification key	communication between TOE components
ISO/IEC 11770-3	Nexess Policy Server	Nexess Login Server Nexess AdminTool Nexess Client Nexess Agent	Session key for cryptographic communication between TOE components	"Asymmetric key-based key exchange protocol" by using validated cryptographic verification module

FCS_CKM.4 Cryptographic key destruction

Hierarchical to : No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation
FCS_CKM.1(2) Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ["cryptographic key destruction method in [Table 19] Cryptographic Key Destruction Method per Storage] that meets the following [list of standards in Cryptographic Key Destruction Method per Storage].

[Table 19] Cryptographic Key Destruction Method per Storage

List of Standards	Destruction Target	Cryptographic Key Storage Area	Destruction Method	Timing of Destruction
N/A (In-house implementation)	Authentication token cryptographic key Authentication token integrity verification key	Memory	Parameter initialization: initialization by nullifying major parameters	At the time of process shutdown or new key distribution
N/A	Master key,	Memory	Parameter	After

(In-house implementation)	KEK		initialization: initialization by nullifying major parameters	encryption/decryption is completed
N/A (In-house implementation)	Session key	Memory	Parameter initialization: initialization by nullifying major parameters	After encryption/decryption is completed

FCS_COP.1(1) Cryptographic operation (authentication token)

Hierarchical to : No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform ["encryption method" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Sizein accordance with a specified cryptographic algorithm ["algorithm" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Sizeand cryptographic key sizes ["cryptographic key size" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Size that meet the following: ["list of standards" in [Table 16] Authentication Token Cryptographic Key Algorithm and Key Size.

FCS_COP.1(2) Cryptographic operation (TSF data encryption)

Hierarchical to : No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(2) Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform ["encryption method" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size] in accordance with a specified cryptographic algorithm ["algorithm" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size] and cryptographic key sizes ["cryptographic key size" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size] that meet the

following: ["list of standards" in [Table 17] TSF Data Cryptographic Key Algorithm and Key Size].

FCS_RBG.1 Random bit generation (extended)

Hierarchical to : No other components

Dependencies : No dependencies

FCS_RBG.1.1 The TSF shall generate random numbers necessary for generating cryptographic keys by using a specified random bit generator that meets the following [[Table 20] List of Random Bit Generators].

[Table 20] List of Random Bit Generators

Random Bit Generator	Default	Base Function	Method
HASH-DRBG-SHA256	O	HASH function-based	HASH function

5.1.3. Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components

Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [1 – 5 (default value 5)]* unsuccessful authentication attempts occur related to [administrator, end user authentication attempt].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [the following list of actions

[

- Inactivation of identification and authentication function configurable by the authorized administrator (default value 10 minutes, to be set by the administrator within the range or 5 – 20 minutes)
- Sending a warning mail in case of the administrator

]

FIA_IMA.1 TOE internal mutual authentication (extended)

Hierarchical to : No other components

Dependencies : No dependencies

FIA_IMA.1.1 The TSF shall perform mutual authentication through ["asymmetric key-based

key exchange protocol" using the validated cryptographic module] that meets [N/A] between [[Table 21] Mutual Authentication Components].

[Table 21] Mutual Authentication Components

Validated Cryptographic Module	TOE Component	
[Refer to technologies in [Table 7] Validated Cryptographic Module and Cryptographic Algorithm Identification of TOE Component]	Nexess Policy Server	Nexess AdminTool
	Nexess Policy Server	Nexess Login Server
	Nexess Policy Server	Nexess Agent
	Nexess Policy Server	Nexess Client

FIA_SOS.1 Verification of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following defined quality metric].

[

a) Allowable characters

- English capital/small letter (52 letters: a ~ z, A ~ Z)
- Number (10 letters: 0 ~9)
- Special character that can be input by using a keyboard (25 letters: ~,`,!,@,#,$,%,^,&,*,(,),-,_,=,+,₩,|,[,{,],},:,,,?)

b) Min/Max length

- 9 ~ 16 digits

c) Combination rules

- Minimum size rule combination of number or special character
- Minimum size rule combination of number
- Minimum size rule combination of special character

d) Change interval (the period during which the password is used)

- 0~90 days (default value 30 days, the interval is defined by the authorized administrator)

]

FIA_SOS.2 Generation of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.2.1 The TSF shall provide a mechanism to generate **authentication tokens** that meet [the following defined quality metric].

[

a) Mechanism to generate authentication tokens

- Using authentication data encryption

- Refer to [Table 16] Authentication Token Cryptographic Key Algorithm and Key Size

- Authentication data components

  - User ID, user IP, authentication time (time stamp), authentication level, integrity value

- Integrity of authentication data

- Refer to [Table 16] Authentication Token Cryptographic Key Algorithm and Key Size

- Subject of authentication data generation

  - Nexess Login Server

]

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated **authentication tokens** for [the following TSF functions].

[

- FIA_UAU.1 User authentication
- FIA_UID.1 User identification

]

FIA_SOS.3 Destruction of secrets (extended)

Hierarchical to : No other components

Dependencies : FIA_SOS.2 Generation of secrets

FIA_SOS.3.1 The TSF shall destroy **authentication tokens** in accordance with a specified **authentication token** destruction method [[Table 22] Secret Destruction Method] that meets the following [[Table 22] Secret Destruction Method].

[Table 22] Secret Destruction Method

List of Standards	Target	Destruction Method	Timing of Destruction
TTAS.KO-12.0004/R1	Authentication token data	Parameter initialization: initialization by nullifying major parameters	At the time of process shutdown or log-out function call

ISO/IEC 9797-2		Parameter initialization: initialization by nullifying major parameters	

FIA_UAU.1 Timing of authentication (end user)

Hierarchical to : No other components

Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [the following list of TSF mediated actions] on behalf of the **end user** to be performed before the **end user** is authenticated.

[

- Communication check
- Initialization

]

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action (administrator)

Hierarchical to : FIA_UAU.1 Timing of authentication

Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require the **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the **administrator.**

FIA_ UAU.4 Single-use authentication mechanisms

Hierarchical to : No other components

Dependencies : No dependencies

FIA_ UAU.4.1 The TSF shall prevent reuse of authentication data related to [the following identified authentication mechanism(s)].

[

- Single-use authentication mechanism for administrator
  - o The TOE authenticates the administrator through password-based cryptographic authentication.
  - o The TOE stores in DB and checks the timing of authentication and the number of failed attempts upon every administrator

authentication.

o The TOE examines duplicated authentication requests by storing authentication data in the memory upon every administrator authentication.

o The TOE shall prevent the reuse of authentication data by storing in the memory and examining unique session ID at the time of password-based cryptographic authentication.

- Single-use authentication mechanism for user

  o The TOE authenticates the user through password-based authentication.

  o Authentication data generated in accordance with FIA_SOS.2 Generation of secrets are stored in the form of web browser cookie and Nexess Client memory. Time stamps and random cryptographic keys are used in order to prevent them from being stolen and reused. Also, separate HMAC verification is carried out to maintain the integrity.

]

FIA_ UAU.7 Protected authentication feedback

Hierarchical to : No other components

Dependencies : FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [the following list of feedback] to the user while the authentication is in progress.

[

- Passwords being entered are masked (password masking with *) to prevent them from being disclosed on the screen.
- In case of failure of identification and authentication, feedbacks on the reason for the failure are not provided.

]

FIA_UID.1 Timing of identification (end user)

Hierarchical to : No other components

Dependencies : No dependencies

FIA_UID.1.1 The TSF shall allow [the following list of actions] on behalf of the **end user** to be performed before the **end user** is identified.

[

- Communication check
- Initialization

]

FIA_ UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action
Hierarchical to : No other components
Dependencies : No dependencies

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of the **administrator**.

5.1.4. Security Management (FMT)

FMT_MOF.1 Management of security functions behaviour
Hierarchical to : No other components
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to conduct ***management actions*** of the functions in [[Table 23] List of Security Functions Behaviour of Administrator] to [the authorized administrator].

[Table 23] List of Security Functions Behaviour of Administrator

Administrator Type	Classification	Security Function	Ability			
			Determine the behavior	disable	enable	Modify the behavior
Top administrator	User management	User management	O	O	O	O
		Administrator level management	O	O	O	O
	SYSTEM	System status monitoring	O	O	O	O
		Business system management	O	O	O	O
		XML configuration	O	O	O	O

	Audit log	Administrator behavior history view	O	-	-	-
		System audit log	O	-	-	-
		Administrator login log	O	-	-	-
		Nexess log	O	-	-	-
		Abnormal access audit log	O	-	-	-
General administrator	User management	User management	O	-	-	-
	SYSTEM	Business system management	O	-	-	-

(※ Legend: - not supported, ○ supported)

FMT_MTD.1 Management of TSF data

Hierarchical to : No other components

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to ***manage*** [[Table 24] List of TSF Data and Management Ability] to [the authorized administrator].

[Table 24] List of TSF Data and Management Ability

Administrator Type	TSF Data	Ability			
		query	modify	delete	generate
Top Administrator	User management	○	○	○	○
	Administrator level management	○	○	○	○
	System status monitoring	○	-	-	-
	Business system management	○	○	○	○
	XML configuration	○	○	○	○
	Administrator behavior history view	○	-	-	-
	System audit log	○	-	-	-
	Administrator login log	○	-	-	-

	Nexess log	○	-	-	-
	Abnormal access audit log	○	-	-	-
General administrator	User management	○	-	-	-
	Business system management	○	-	-	-

(※ Legend: - not supported, ○ supported)

FMT_PWD.1 Management of ID and password (extended)

Hierarchical to : No other components

Dependencies : FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [user management of Nexess Policy Server] to [the authorized administrator].

[

1. [Password combination rules]

- Allowable characters
  - o 52 English letters (small or capital letter)
  - o 10 numbers (0-9)
  - o 25 special characters (~,`,!,@,#,$,%,^,&,*,(,),-,_,=,+,₩,|,[,{,],},:,,,?)
- Min/Max size
  - o 9 ~ 16 digits
- Combination rules
  - o Minimum size rule combination of number or special character
  - o Minimum size rule combination of number
  - o Minimum size rule combination of special character
- Change interval (the period during which the password is used)
  - o 0~90 days (default value 30 days, the interval is defined by the authorized administrator)

]

FMT_PWD.1.2 The TSF shall restrict the ability to manage ID of [N/A] to [the authorized administrator].

FMT_PWD.1.3 The TSF shall provide the capability for *changing the password when the authorized administrator accesses for the for the first time*.

FMT_SMF.1 Specification of management functions

Hierarchical to : No other components

Dependencies : No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [list of management functions to be provided by the TSF].

[

- Management functions of the TSF: Management functions specified in FMT_MOF.1
- Management of TSF data: Management functions specified in FMT_MTD.1
- Management of ID and password: Management functions specified in FMT_PWD.1

]

FMT_SMR.1 Security roles

Hierarchical to : No other components

Dependencies : FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [[Table 25] User Classification and Roles].

[Table 25] User Classification and Roles

User Classification	Level	Security Policy	Audit Data	Remarks
Security administrator	Top administrator	Query, generate, modify, delete	Query	
	General administrator	Query		

FMT_SMR.1.2 The TSF shall be able to associate users with **roles defined in FMT_SMR.1.1.**

5.1.5. Protection of the TSF (FPT)

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to : No other components

Dependencies : No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE **through the encryption and message integrity verification.**

FPT_PST.1 Basic protection of stored TSF data (extended)

Hierarchical to : No other components
Dependencies : No dependencies

FPT_PST.1.1 The TSF shall protect [the following TSF data] stored in the containers controlled by the TSF from unauthorized *disclosure, modification.*

[

- User account information (administrator, end user)
- DB access account information
- Cryptographic key (Master Key, authentication token cryptographic key, authentication token integrity verification key, etc.)
- Key security parameters (random number value, etc.)
- TOE set value (security policy, configuration parameter)]

FPT_TST.1 TSF testing

Hierarchical to : No other components
Dependencies : No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of [[Table 26] Items Subject to TSF Self Test]

[Table 26] Items Subject to TSF Self Test

Classification	Item	Content (Role)
Nexess Policy Server	Cryptographic module	Self test
	Process	Determine whether it was started normally at the time of start-up and generate audit log
Nexess Login Server Nexess AdminTool	Cryptographic module	Self test
	Process	Confirm normal operation on a periodic basis and send the status to Policy Server
Nexess Agent	Cryptographic module	Self test
Nexess Client	Cryptographic module	Self test
	Process	Confirm normal operation on a periodic basis and send the status to Policy Server

[Table 27] Items Subject to TOE Integrity Test

Classification	Item	Content (Role)
Nexess Policy Server	Configuration file	TOE configuration file
	Stored TSF executable code	Policy server demon process
Nexess Login Server	Configuration file	TOE configuration file
	Stored TSF executable code	Server process
Nexess Client	Configuration file	TOE configuration file
	Stored TSF executable code	Client process
Nexess AdminTool	Configuration file	TOE configuration file
	Stored TSF executable code	Server process

FPT_TST.1.2 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of ["item" configuration file in [Table 27] Items Subject to TOE Integrity Test].

FPT_TST.1.3 The TSF shall provide **the authorized administrator** with the capability to verify the integrity of ["item" stored TSF executable code in [Table 27] Items Subject to TOE Integrity Test].

5.1.6. TOE Access (FTA)

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions
Hierarchical to : FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies : FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [limitation on the maximum number of concurrent sessions in case of management access sessions by the administrator to one, prohibition of concurrent establishment of management access session and local access session that belong to the same user].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] session per user administrator.

FTA_SSL.5 Management of TSF-initiated sessions (extended)

Hierarchical to : No other components
Dependencies : FIA_UAU.1 Timing of authentication

FTA_SSL.5.1 The TSF shall *terminate* an interactive session after [10 minutes of user inactivity, 50 minutes of no access by an end user to the business system].
Application notes: User means top administrator, general administrator and end user.

FTA_TSE.1 TOE session establishment
Hierarchical to : No other components
Dependencies : No dependencies

FTA_TSE.1.1 The TSF shall be able to **deny the administrator's management access session establishment** based on [access IP, *whether or not management access session of the same account is activated*].
Application notes: The number of accessible IP provided by the TOE is set as two by default.

5.2. Security Assurance Requirements

Security assurance requirements of this ST are composed of assurance components in Common Criteria (CC V3.1) Part 3 and the evaluation assurance level is EAL1+(ATE_FUN.1). The table below summarizes assurance components.

[Table 28] Assurance Component Summary

Assurance Class	Assurance Component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE configuration management coverage
Tests	ATE_FUN.1	Functional testing

	ATE_IND.1	Independent testing: conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.2.1. Security Target Evaluation

ASE_INT.1 ST introduction

Dependencies : No dependencies

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies : ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies : No dependencies

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements

ASE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies : No dependencies

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.1 Stated security requirements

Dependencies : ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements

ASE_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies : ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.2. Development

ADV_FSP.1 Basic functional specification

Dependencies : No dependencies

Developer action elements

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.3. Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies : ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies : No dependencies

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.4. Life-cycle Support

ALC_CMC.1 Labelling of the TOE

Dependencies : ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies : No dependencies

Developer action elements

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C The configuration list shall include the followings: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5. Tests

ATE_FUN.1 Functional testing

Dependencies : ATE_COV.1 Evidence of coverage

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent testing: sample

Dependencies : ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements
ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements
ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements
ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6. Vulnerability Assessment

AVA_VAN.1 Vulnerability survey

Dependencies : ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements
AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements
AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements
AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and preparation of evidence.
AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks

performed by an attacker processing Basic attack potential.

5.3. Security Requirements Rationale

Security requirements rationale demonstrates that the SFRs described are suitable to satisfy the security objectives and consequently, appropriate to address the security problem.

5.3.1. Dependency of the SFRs of the TOE

The SFRs used in this ST satisfy the dependencies as indicated in the table below, and there is no component that does not satisfy the dependency.

The table below shows dependencies of functional components.

[Table 29] Dependencies of the SFRs of the TOE

No.	SFR	Dependencies	Reference No.
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.3	FAU_STG.1	Rationale (2)
7	FAU_STG.4	FAU_STG.1	Rationale (2)
8	FCS_CKM.1(1)	FCS_CKM.2, FCS_COP.1(1)	10, 12
		FCS_CKM.4	11
9	FCS_CKM.1(2)	FCS_CKM.2, FCS_COP.1(2)	10, 13
		FCS_CKM.4	11
10	FCS_CKM.2	FCS_CKM.1	10
		FCS_CKM.4	11
11	FCS_CKM.4	FCS_CKM.1	10
12	FCS_COP.1(1)	FCS_CKM.1	10
		FCS_CKM.4	11
13	FCS_COP.1(2)	FCS_CKM.1	10
		FCS_CKM.4	11
14	FCS_RBG.1	-	-
15	FIA_AFL.1	FIA_UAU.1	20
16	FIA_IMA.1	-	-
17	FIA_SOS.1	-	-

18	FIA_SOS.2	-	-
19	FIA_SOS.3	FIA_SOS.2	18
20	FIA_UAU.1	FIA_UID.1	24
21	FIA_UAU.2		
22	FIA_UAU.4	-	-
23	FIA_UAU.7	FIA_UAU.1	20
24	FIA_UID.1	-	-
25	FIA_UID.2		
26	FMT_MOF.1	FMT_SMF.1	29
		FMT_SMR.1	30
27	FMT_MTD.1	FMT_SMF.1	29
		FMT_SMR.1	30
28	FMT_PWD.1	FMT_SMF.1	20
		FMT_SMR.1	30
29	FMT_SMF.1	-	-
30	FMT_SMR.1	FIA_UID.1	24
31	FPT_ITT.1	-	-
32	FPT_PST.1	-	-
33	FPT_TST.1	-	-
34	FTA_MCS.2	FIA_UID.1	24
35	FTA_SSL.5	FIA_UAU.1	20
36	FTA_TSE.1	-	-

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1. However, reliable time stamps provided by the security objective OE.Time Stamp for the operational environment of this ST are used, thereby satisfying the dependency.

Rationale (2): FAU_STG.3 and FAU_STG.4 have a dependency on FAU_STG.1. However, it is protected from unauthorized deletion or modification in accordance with the security objective OE.SECURE_DBMS for the operational environment of this ST, thereby satisfying the dependency.

5.3.2. Dependency of SARs of the TOE

The dependency of each assurance package provided in Common Criteria for Information Technology Security Evaluation is already satisfied. Thus, the rationale is omitted herein.
The augmented SAR ATE_FUN.1 has a dependency on ATE_COV.1. ATE_COV.1has been augmented to ensure that the developer performs tests on test items correctly and documents them in the documentation. However, ATE_COV.1 is not included in this ST since it

is deemed not necessarily required to include ATE_COV.1 that presents the consistency between test items and TSFI.

6. TOE Summary Specification

This chapter provides brief and clear description of how the SFRs are implemented in the TOE.

The following table is the list of the security functions specified in the TOE Summary Specification.

[Table 30] List of TOE Security Functions

Security Functional Class	Security Functional Component	
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
암호지원 (FCS)	FCS_CKM.1(1)	Cryptographic key generation (authentication token)
	FCS_CKM.1(2)	Cryptographic key generation (TSF data encryption)
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (authentication token)
	FCS_COP.1(2)	Cryptographic operation (TSF data encryption)
	FCS_RBG.1(extended)	Random bit generation
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_IMA.1(extended)	TOE internal mutual authentication
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	Generation of secrets
	FIA_SOS.3(extended)	Destruction of secrets
	FIA_UAU.1	Timing of authentication (end user)
	FIA_UAU.2	User authentication before any action (administrator)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification (user)
	FIA_UID.2	User identification before any action (administrator)
Security	FMT_MOF.1	Management of security functions behaviour

Management (FMT)	FMT_MTD.1	Management of TSF data
	FMT_PWD.1(extended)	Management of ID and password
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1(extended)	Basic protection of stored TSF data
	FPT_TST.1	TSF self test
TOE Access (FTA)	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.5(extended)	Management of TSF-initiated sessions
	FTA_TSE.1	TOE session establishment

6.1. Security Audit (FAU)

Security Audit function of the TOE consists of audit data generation and collection, audit data view and review, potential violation analysis and management of audit storage.

6.1.1. Audit Data Generation and Collection

The following audit data are generated in the TOE, which are collected and stored by Nexess Policy Server (satisfying FAU_GEN.1).

- Security log generated by the security management function
- Security log generated by the cryptographic operation function
- Security log such as actions against potential security violation, identification and authentication, TSF self tests, session termination, etc.
- When audit data are generated for any change of TSF data value, modified TSF data value is included

Each security log includes the following items to compose audit data:

- Time of audit occurrence
- Audit message, etc.

SFR to be satisfied: FAU_GEN.1

6.1.2. Potential Violation Analysis and Action

The TSF performs the following actions in case potential security violation is detected, based on audit records generated (refer to 6.1.1).

[Table 31] Actions against Security Violations

Security Violation	Action
Accumulation of authentication failures specified in FIA_UAU.1	· Limitation on login attempts for a specified period of time (default: 10 minutes) for all end users
Accumulation of authentication failures specified in FIA_UAU.2	· Limitation on login attempts for a specified period of time (default: 10 minutes) for all authorized administrators · Sending a warning email to the administrator
Integrity violation event and failure of self test that requires validation specified in FPT_TST.1	· Sending a warning email to the administrator
Audit trail exceeding certain pre-defined limits specified in FAU_STG.3	· Sending a warning email to the administrator
Predicted audit data loss specified in FAU_STG.4	· Sending a warning email to the administrator · Ignoring an audited event

SFR to be satisfied: FAU_ARP.1, FAU_SAA.1

6.1.3. Management of Audit Storage

The TOE shall take the following actions if the audit data exceeds the storage limit (satisfying FAU_STG.3).

a) In case the threshold pre-defined by the administrator is reached (default value: 90 percent), the administrator is notified via email.

b) In case the audit trail is full (default value: 99 percent), an audited event is ignored in the audit data storage and the administrator is notified via email.

The percentage of the threshold means what percentage of the total capacity of HDD using log DB is in use. For example, if the threshold of 100 GB HDD is set as 90 percent, it means that 90 GB is in use and 10 GB is available for further use.

SFR to be satisfied: FAU_STG.3, FAU_STG.4

6.1.4. Audit Data View and Review

Audit data generated are stored in the audit storage (refer to 6.1.1), and the administrator

views and reviews stored audit data through the screen interface (GUI) provided by INISAFE AdminTool. (FAU_SAR.1) (FAU_SAR.1)

- Administrator behavior history view
- System audit log
- Nexess log
- Administrator login log
- Abnormal access audit log

The TOE can search audit logs based on the following items and provides the capability to sort the retrieved audit data based on time. (FAU_SAR.3)

- Administrator behavior history log
  - Date and time of event (start date – end date), user ID, type, status
- System audit log
  - Date and time of event (start date – end date), keyword
- Nexess log
  - Date and time of event (start date – end date)
- Administrator login log
  - Status, administrator ID, date and time of event (start date – end date)
- Abnormal access audit log
  - Date and time of event (start date – end date)

The TSF provides the GUI function that enables the authorized administrator to read audit records after accessing INISAFE AdminTool. For each type of audit data, when entering "selection criteria" value in [Table 32] Audit Data Type and Selection Criteria, the search result that has a combination with AND operation can be displayed.

SFR to be satisfied: FAU_SAR.1, FAU_SAR.3

6.2. Cryptographic Support (FCS)

Cryptographic Support function of the TOE consists of the establishment of security policies by the authorized administrator, and generation, distribution and destruction of cryptographic keys through a secure random bit generator in accordance with the security policies. Based on such cryptographic keys, an authentication token that serves as user authentication data in SSO is stored in the memory of Nexess Client and Nexess Login Server. Then, the authentication token is destroyed in the memory at the time of logout.

6.2.1. Cryptographic Key Generation/Operation and Random Number Generation

(Authentication Token, TSF Data)

The TOE provides cryptographic key algorithm and key size, and cryptographic operation method for authentication token as shown in [Table 32] below.
The TOE provides cryptographic key algorithm and key size, and cryptographic operation method for TSF data as shown in [Table 33] below.
(satisfying FCS_CKM.1, FCS_COP.1, FCS_RBG.1(extended)

[Table 33] Cryptographic Key Algorithm and Key Size, Cryptographic Operation for Authentication Token

List of Standards	Cryptographic Key Size	Operation Method	Usage
TTAK.KO-12.0190	128	SEED(CBC)	Authentication token generation and verification
ISO/IEC 9797-2	128	HMAC-SHA-2	Authentication token integrity verification
ISO/IEC 10118-3	-	SHA-256	One-way use password
TTAK.KO-12.0190	-	HASH-DRBG-SHA256	Random number to generate cryptographic key

[Table 34] Cryptographic Key Algorithm and Key Size, Cryptographic Operation for TSF Data

Algorithm	Cryptographic Key Size	Operation Method	Usage
TTAK.KO-12.0190	128	SEED(CBC)	TSF data encryption/decryption Encryption/decryption of Master Key at the time of storage Communication between TOE components
ISO/IEC 18033-2	2048	RASES	Communication between TOE components
TTAK.KO-12.0190	-	HASH-DRBG-SHA256	Session key generation between TOE components
ISO/IEC 10118-3	-	SHA-256	TSF data integrity verification User password hash

SFR to be satisfied: FCS_ COP.1(1), FCS_ COP.1(2), FCS_CKM.1(1), FCS_CKM.1(2), FCS_RBG.1(extended)

[Table 35] Validated Cryptographic Module

Cryptographic Module	Algorithm	Validation Date	Validation No.
INISAFE Crypto for Java 4.1	SEED, HMAC, SHA256, HASH-DRBG-SHA224/256/384/512	De. 16, 2014	CM-97-2019.12
INISAFE Crypto for C 5.2.0	SEED, HASH-DRBG-SHA224/256/384/512	Apr. 25, 2014	CM-89-2019.4

6.2.2. Cryptographic Key Distribution (Authentication Token, TSF Data)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method that meets the "list of standards" in the following [Table 36] Cryptographic Key Distribution Method.

[Table 36] Cryptographic Key Distribution Method

List of Standards	Origin	Destination	Distribution Target	Distribution Method
N/A (In-house implementation)	Nexess Policy Server	Nexess Login Server Nexess Agent	Authentication token cryptographic key Authentication token integrity verification key	When a user logs in and when an authentication token is generated, after a cryptographic key is generated, it is distributed through cryptographic communication between TOE components
ISO/IEC 18033-2	Nexess Policy Server	Nexess Login Server Nexess AdminTool Nexess Client Nexess Agent	Session key for cryptographic communication between TOE components	Transfer by encrypting with a public key of the counterpart

SFR to be satisfied: FCS_CKM.2

6.2.3. Cryptographic Key Destruction

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following "list of standards" in [Table 37] .

[Table 37] Cryptographic Key Destruction Method per Storage

List of Standards	Destruction Target	Cryptographic Key Storage Area	Destruction Method	Timing of Destruction
N/A (In-house implementation)	Authentication token cryptographic key	Memory	Parameter initialization: initialization by nullifying major parameters	At the time of process shutdown or new key distribution
N/A (In-house implementation)	Master key, KEK	Memory	Parameter initialization: initialization by nullifying major parameters	After encryption/decryption is completed
N/A (In-house implementation)	Session key	Memory	Parameter initialization: initialization by nullifying major parameters	After encryption/decryption is completed

SFR to be satisfied: FCS_CKM.4

6.3. Identification and Authentication (FIA)

The security function of Identification and Authentication of the TOE consists of administrator identification and authentication, end user identification and authentication, TOE internal mutual authentication, generation, verification and destruction of authentication tokens and so forth for the purpose of performing security management through SSO.

6.3.1. TOE Internal Mutual Authentication

Key management for encryption between components is performed by means of private key/public key RSA cryptographic method using a KCMVP-validated cryptographic module, and encryption of communication between TOE modules and mutual authentication are performed.

All TOE components use the same private certificate for cryptographic communication (public key length 2,048 bits).

[Table 38] Algorithm Used in TOE Internal Mutual Authentication

Type	Item	Description
Mutual authentication	Private key/public key RSA	Asymmetric cryptographic method that makes a key promise (algorithm, encoding rule, etc.) between the Server and the Client and then encrypts the data
Session Key	Generation / Hash Algorithm	SEED / SHA-256 HASH-DRBG-SHA256
Data exchange	Cryptographic algorithm	SEED 128 CBC

SFR to be satisfied: FIA_IAM.1(extended)

6.3.2. End User Identification and Authentication

The following actions are allowed for end users before they are authenticated through Nexess Client (satisfying FIA_UAU.1):

- Communication check
- Initialization

If end user ID/password is successfully identified and authenticated through Nexess Policy Server and Nexess Login Server, an authentication token necessary for SSO is issued.

Identification and authentication information provided through the screen GUI for end user identification and authentication is as follows (satisfying FIA_UAU.1, FIA_UID.1):

- End user ID
- End user password

In case of unsuccessful authentication attempts for a defined number of times (five times by default), such ID is locked to prevent repetitive attempts for the identification and authentication process (satisfying FIA_AFL.1).

The TOE provides a mechanism to verify that end user passwords meet the following defined quality metric upon password registration or change (FIA_SOS.1).

- a) Allowable characters
  - English capital/small letter (52 letters: a ~ z, A ~ Z),
  - Number (10 letters: 0 ~9)
  - Special character that can be input by using a keyboard (25 letters: ~,`,!,@,#,$,%,^,&,*,(,),-,_,=,+,₩,|,[,{,],},:,,,,?)
- Min/Max length
  - 9 ~ 16 digits
- Combination rules
  - Minimum size rule combination of number or special character
  - Minimum size rule combination of number
  - Minimum size rule combination of special character
- Change interval (the period during which the password is used)
  - 0~90 days (default value 30 days, the interval is defined by the authorized administrator)

The TOE prevents the reuse of authentication data as follows (FIA_UAU.4):

- End users are authenticated through password-based authentication.
- Authentication data generated are stored in the form of web browser cookie and Nexess Client memory. Time stamps and random cryptographic keys are used in order to prevent them from being stolen and reused. Also, separate HMAC verification is carried out to maintain the integrity.

Passwords being entered are masked (password masking with *) to prevent them from being disclosed on the screen. In case of failure of identification and authentication, feedbacks on the reason for the failure are not provided (satisfying FIA_UAU.7).

SFR to be satisfied: FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.7, FIA_UID.1

6.3.3. Generation/Verification/Destruction of End User SSO Authentication

An end user requests login by using ID/password. Nexess Policy Server and Nexess Login Server interoperate with the storage of end user information to verify login. If the login is valid, Nexess Login Server issues an authentication token and sends it to the web browser and Nexess Client, thereby controlling the access by verifying the authentication token when the user requests access to another business system. The authentication token is automatically deleted in the memory upon logout.

For TOE internal mutual authentication, the TOE provides the confidentiality and the integrity by means of private key/public key cryptographic method using the KCMVP-validated cryptographic module.

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following "list of standards" in [Table 39] .

[Table 39] Cryptographic Key Destruction Method per Storage

List of Standards	Destruction Target	Cryptographic Key Storage Area	Destruction Method	Timing of Destruction
N/A (In-house implementation)	Authentication token cryptographic key	Memory	Parameter initialization: initialization by nullifying major parameters	At the time of process shutdown or new key distribution
N/A (In-house implementation)	Master key, KEK	Memory	Parameter initialization: initialization by nullifying major parameters	After encryption/decryption is completed
N/A (In-house implementation)	Session key	Memory	Parameter initialization: initialization by nullifying major parameters	After encryption/decryption is completed

SFR to be satisfied: FIA_SOS.1, FIA_SOS.2, FIA_SOS.3(extended), FIA_IMA.1(extended)

6.3.4. Administrator Identification and Authentication

The administrator can perform security management after undergoing identification and authentication by Nexess AdminTool.
The administrator shall enter the following identification and authentication data through the screen interface (FIA_UID.2, FIA_UAU.2 extended).

- Administrator ID
- Administrator password

In case of unsuccessful authentication attempts for a defined number of times (five times by default), such ID is locked to prevent repetitive attempts for the identification and authentication process (satisfying FIA_AFL.1).

The TOE provides a mechanism to verify that end user passwords meet the following defined quality metric upon password registration or change (FIA_SOS.1).

- a) Allowable characters
  - English capital/small letter (52 letters: a ~ z, A ~ Z),
  - Number (10 letters: 0 ~9)
  - Special character that can be input by using a keyboard (25 letters: ~,`,!,@,#,$,%,^,&,*,(,),-,_,=,+,₩,|,[,{,],},:,„,?)
- Min/Max length
  - 9 ~ 16 digits
- Combination rules
  - Minimum size rule combination of number or special character
  - Minimum size rule combination of number
  - Minimum size rule combination of special character
- Change interval (the period during which the password is used)
  - 0~90 days (default value 30 days, the interval is defined by the authorized administrator)

The TOE prevents the reuse of authentication data as follows (FIA_UAU.4):

- The TOE authenticates the administrator through password-based cryptographic authentication.
- The TOE stores and examines the number of unsuccessful attempts and authentication time in DB upon every authentication.
- The TOE stores authentication data in the memory upon every authentication to examine duplicated authentication requests.

Passwords being entered are masked (password masking with *) to prevent them from being disclosed on the screen. In case of failure of identification and authentication, feedbacks on the reason for the failure are not provided (satisfying FIA_UAU.7).

SFR to be satisfied: FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

6.4. Security Management (FMT)

6.4.1. Management of Security Functions Behaviour

The TOE provides the following function to manage security functions behavior.

[Table 40] List of Security Functions Behaviour of Administrator

Administrator Type	Classification	Security Function	Ability			
			Determine the behavior	disable	enable	Modify the behavior
Top administrator	User management	User management	O	O	O	O
		Administrator level management	O	O	O	O
	SYSTEM	System status monitoring	O	O	O	O
		Business system management	O	O	O	O
		XML configuration	O	O	O	O
	Audit log	Administrator behavior history view	O	-	-	-
		System audit log	O	-	-	-
		Administrator login log	O	-	-	-
		Nexess log	O	-	-	-
		Abnormal access audit log	O	-	-	-
General administrator	User management	User management	O	-	-	-
	SYSTEM	Business system management	O	-	-	-

Administrators are classified into top administrator and general administrator and perform security management behaviours including security policy establishment according to web security management roles.

SFR to be satisfied: FMT_MOF.1, FMT_SMF.1, FMT_SMR.1

6.4.2. Management of TSF Data

All users in the TOE are classified into top administrator, administrator and end user. The ability of the authorized administrator to manage TSF data is described below (FMT_MTD.1).

[Table 41] List of TSF Data and Management Ability

Administrator Type	TSF Data	Ability			
		query	modify	delete	generate
Top Administrator	User management	○	○	○	○
	Administrator level management	○	○	○	○
	System status monitoring	○	-	-	-
	Business system management	○	○	○	○
	XML configuration	○	○	○	○
	Administrator behavior history view	○	-	-	-
	System audit log	○	-	-	-
	Administrator login log	○	-	-	-
	Nexess log	○	-	-	-
	Abnormal access audit log	○	-	-	-
General administrator	User management	○	-	-	-
	Business system management	○	-	-	-

SFR to be satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.4.3. Management of Security Password

The TOE provides the function to register and modify user's authentication data – password. Only the top administrator can register and change password. The administrator can change passwords through the screen interface provided by Nexess AdminTool. Password is encrypted with SHA256 algorithm, including which the security policy is once again encrypted with SEED algorithm and stored. Refer to FIA_SOS.1 for password lengths and combination rules selected when registering or changing password.

Nexess AdminTool provides the function to set up password of the top administrator in the process of the installation.

SFR to be satisfied: FMT_PWD.1(extended)

6.5. Protection of the TSF (FPT)

6.5.1. Basic Protection of Stored TSF Data

The TOE encrypts and stores cryptographic keys (Master Key, etc.), key security parameters, TOE set value (security policy value, configuration value), administrator/user ID and password, DBMS account information and so forth (satisfying FPT_PST.1(extended)).

[Table 42] Protection Method in Storing Cryptographic Key and Key Parameters

Module	Encryption Target	Algorithm and Operation Method	Key Used	Storage Location	Application Method
Nexess Policy Server	Master Key	SEED 128 CBC	Derivation Key	File	Encryption
	Certificate Private Key	SEED 128 CBC	Master Key	File	Encryption
Nexess Login Server	Master Key	SEED 128 CBC	Derivation Key	File	Encryption
	Authentication Token	SEED 128 CBC	Authentication Token Cryptographic Key	Memory	Encryption
	Authentication Token HMAC	HMAC-SHA-2	Authentication Token Integrity Verification Key	Memory	Encryption
	Certificate Private Key	SEED 128 CBC	Master Key	File	Encryption
Nexess Agent	Master Key	SEED 128 CBC	Derivation Key	File	Encryption
	Certificate Private Key	SEED 128 CBC	Master Key	File	Encryption
	Authentication Token	SEED 128 CBC	Authentication Token Cryptographic Key	Memory	Encryption

	Authentication Token HMAC	HMAC-SHA-2	Authentication Token Integrity Verification Key	Memory	Encryption
Nexess Client	Master Key	SEED 128 CBC	Derivation Key	File	Encryption
	Certificate Private Key	SEED 128 CBC	Master Key	File	Encryption
Nexess AdminTool	Master Key	SEED 128 CBC	Derivation Key	File	Encryption
	Certificate Private Key	SEED 128 CBC	Master Key	File	Encryption

[Table 43] List of Security Policy, Account Information Encryption

Classification	Cryptographic Key	Cryptographic Method	Algorithm	Encryption List	Data Storage Location
Nexess Policy Server	Master Key	Symmetric key encryption	SEED (CBC)	All security policy information	File
Nexess Policy Server	Master Key	Symmetric key encryption	SEED (CBC)	DBMS account information encryption	File
Nexess Login Server	-	Secure hash	SHA-2 (256)	Admin and user password	DBMS
Nexess AdminTool	-	Secure hash	SHA-2 (256)	Admin and user password	DBMS

[Table 44] Configuration File Encryption and Integrity Check Algorithm and Key

Classification	Type	Algorithm	List of Standards	Key
Nexess Policy Server	Configuration file encryption	SEED (CBC)	TTAK.KO-12.0190	128 bit key generated by using "random bit generator" in [Table 20] List of Random Bit Generators
	Integrity check	SHA-2	ISO/IEC 9797-2	
Nexess Login Server Nexess AdminTool	Configuration file encryption	SEED (CBC)	TTAK.KO-12.0190	128 bit key generated by using "random bit generator" in [Table 20] List of Random Bit Generators
	Integrity check	SHA-2	ISO/IEC 9797-2	

Nexess Agent	Configuration file encryption	SEED (CBC)	TTAK.KO-12.0190	128 bit key generated by using "random bit generator" in [Table 20] List of Random Bit Generators
	Integrity check	SHA-2	ISO/IEC 9797-2	
Nexess Client	Configuration file encryption	SEED (CBC)	TTAK.KO-12.0190	128 bit key generated by using "random bit generator" in [Table 20] List of Random Bit Generators
	Integrity check	SHA-2	ISO/IEC 9797-2	

A key that encrypts a configuration file is encrypted with a key encryption key and stored in a file. KEK is generated by using a derivation key algorithm, and then the configuration file cryptographic key is encrypted and stored in a file.
Furthermore, configuration files and execution files that do not include TOE configuration values such as IP address, port information, the number of unsuccessful authentication attempts and integrity check interval are not encrypted. A file whose corruption can affect the operation of the TOE is subject to the integrity check.

SFR to be satisfied: FPT_PST.1(extended)

6.5.2. Basic Internal TSF Data Transfer Protection

Cryptographic communication used in data transfer between TOE components is as follows:
A cryptographic algorithm in a KCMVP-validated cryptographic module is used to encrypt the data by generating a new session key for encryption whenever data are transferred. The generated session key is encrypted with the counterpart's public key that is already available in a file and is transferred together. The counterpart verifies the session key by using the private key and decrypts the transferred TSF data. TCP/IP is used by default for the communication protocol. All parameters (key [authentication token verification key, session key], key parameter, plaintext, ciphertext, etc.) are encrypted (satisfying FPT_ITT.1).

Refer to 6.3.1 for detailed mechanisms on cryptographic communication procedures between TOE components.

SFR to be satisfied: FPT_ITT.1

6.5.3. TSF Self Tests and Integrity Tests

The TOE runs a suite of self tests during initial start-up and periodically (default: 10 minutes)

during normal operation to demonstrate the correct operation as specified in [Table 45] Items Subject to TOE Self Test.

The TOE verifies the integrity upon request by the administrator by comparing hash values of TSF executable code and stored configuration file.

[Table 45] Items Subject to TOE Self Test

Classification	Item	Content (Role)
Nexess Policy Server	Cryptographic module	Self test
	Process	Determine whether it was started normally at the time of start-up and generate audit log
Nexess Login Server Nexess AdminTool	Cryptographic module	Self test
	Process	Confirm normal operation on a periodic basis and send the status to Policy Server
Nexess Agent	Cryptographic module	Self test
Nexess Client	Cryptographic module	Self test
	Process	Confirm normal operation on a periodic basis and send the status to Policy Server

[Table 46] Items Subject to TOE Integrity Test

Classification	Item	Content (Role)
Nexess Policy Server	Configuration file	TOE configuration file
	Stored TSF executable code	Policy server demon process
Nexess Login Server	Configuration file	TOE configuration file
	Stored TSF executable code	Server process
Nexess Client	Configuration file	TOE configuration file
	Stored TSF executable code	Client process
Nexess AdminTool	Configuration file	TOE configuration file
	Stored TSF executable code	Server process

SFR to be satisfied: FPT_TST.1

6.6. TOE Access (FTA)

6.6.1. TOE Access

The TOE provides the capability to restrict the administrator's management access sessions based on access IP that belongs to the same TSF administrator. The TOE provides the default value of two for the number of accessible IP.

It enforces the limitation on the maximum number of concurrent sessions of the administrator to one by default and blocks new access in case of concurrent access.

In case there is not interaction for the period of user inactivity (default value: 10 minutes), the TOE checks the period of inactivity, makes a request to WAS, and then terminates the session with the support of WAS. In addition, for end users, an authentication token is destroyed after the defined period of no access to the business system (default value: 50 minutes).

SFR to be satisfied: FTA_MCS.2, FTA_SSL.5(extended), FTA_TSE.1