KECS-CR-24-45

# iSIGN+ v4.0

# Certification Report

Certification No.: KECS-CISS-1323-2024

2024. 08. 12.

IT Security Certification Center

## History of Creation and Revision

| No. | Date | Revised Pages | Description |
|---|---|---|---|
| 00 | 2024.08.12. | - | Certification report for iSIGN+ v4.0<br>- First documentation |

This document is the certification report for iSIGN+ v4.0 of Penta Security Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

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

# Table of Contents

# 1. Executive Summary

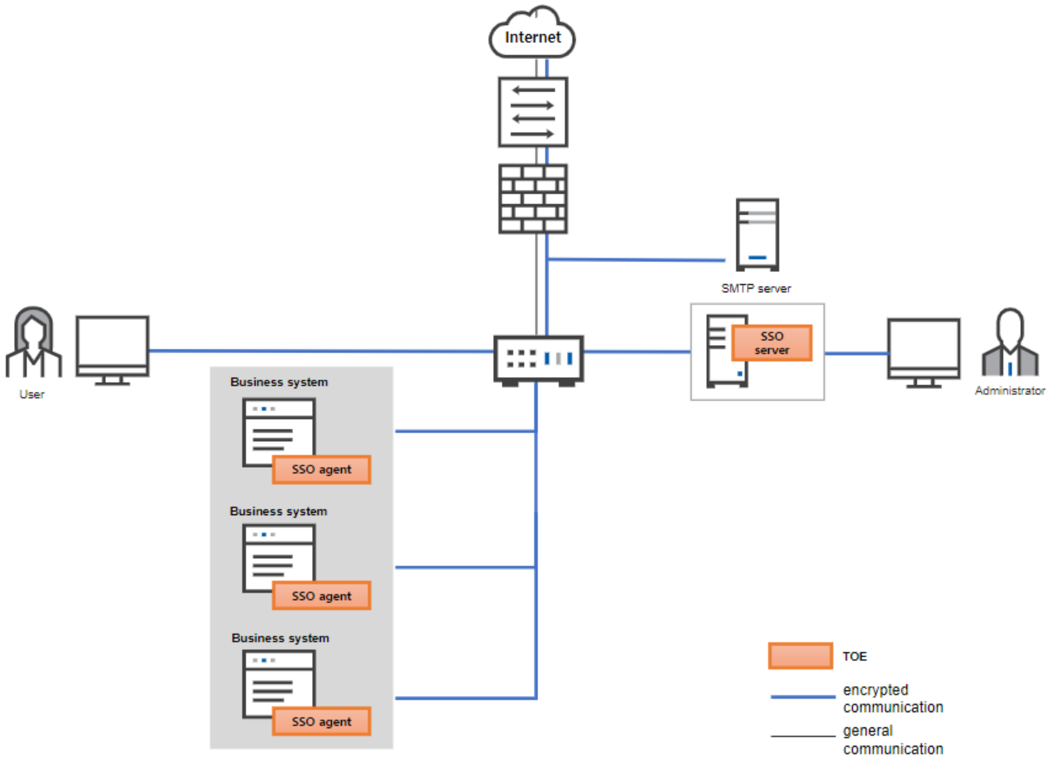
This report describes the evaluation result drawn by the certification body on the iSIGN+ v4.0 eveloped by Penta Security Inc. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter) [1]. It describes the evaluation result and its soundness and conformity. The Target of Evaluation ("TOE" hereinafter) is used to enable the user to access various business systems and use the service through a single user login without additional login action. Also, the TOE shall provide a variety of security features: security audit, Cryptographic support, Identification and authentication including mutual authentication between TOE components, Protection of the TSF, TOE access, Trusted channels and Security management.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on July 19, 2024. This report grounds on the evaluation technical report (ETR) [3] KSEL had submitted and the Security Target (ST) [4].

The ST claims conformance to the Korean National Protection Profile for Single Sign On V3.0 ("PP" hereinafter) [5]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1 augmented by ATE_FUN.1. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and newly defined components in the Extended Component Definition chapter of the PP, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the general TOE operational environment. TOE is composed of the SSO server and SSO agent. The SSO server uses user information stored in the DBMS to provide functions such as direct user login verification, authentication token management, and policy settings. The SSO agent is installed in each business system and requests authentication token verification requests to the SSO server. In addition, the SSO agent can be 'API type' composed of the library file. Authorized administrators may perform security management by accessing the SSO server through web browsers.

The communication section between TOE components performs encrypted communication, and encrypted communication is also performed between the mail server and the SSO server.



**[Figure 1] Operational environment of the TOE**

[Table 1], [Table 2] shows the hardware and software requirements, and operating system to install the TOE.

| Component | | Specification |
|---|---|---|
| H/W | CPU | Intel® Core™ I3-9100 Processor 3.6GHz (4core) or higher |
| | RAM | 16GB or higher |
| | HDD | Space required for TOE installation 1GB or higher |
| | NIC | 100/1000 Mbps x 1EA or higher |
| S/W | OS | Debian GNU/Linux 11(bullseye) (kernel 5.10) 64bits |
| | DBMS | MariaDB v10.5.23 64bits |
| | WAS | Apache Tomcat v10.1.19 64bits |

**[Table 1] Hardware and Software Requirements for SSO server**

| Component | | Specification |
|---|---|---|
| H/W | CPU | Intel® Core™ I3-9100 Processor 3.6GHz (4core) or higher |
| | RAM | 16GB or higher |
| | HDD | Space required for TOE installation 50MB or higher |
| | NIC | 100/1000 Mbps x 1EA or higher |
| S/W | OS | Debian GNU/Linux 11(bullseye) (kernel 5.10) 64bits |
| | WAS | Apache Tomcat v10.1.19 64bits |

**[Table 2] Hardware and Software Requirements for SSO agent**

[Table 3] shows the software requirements for the administrator’s and end user's PC.

| Component | Specification |
|---|---|
| SW | Chrome 125.0.6422.142(official build) (64bits) |

**[Table 3] Software Requirements for administrator’s and end user's PC**

[Table 4] shows the external entities for the operation of the TOE.

| Component | Specification |
|---|---|
| SMTP server | Mail server for sending emails such as administrator notifications when detect security violation |

**[Table 4] external entities for the operation of the TOE**

**Certification Validity**: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

# 2. Identification

The TOE consists of SSO server, SSO agent and related guidance documents.

| | | |
|---|---|---|
| TOE Name | iSIGN+ v4.0 | |
| TOE Version | v4.0-r3 | |
| TOE components | SSO server | SS-ATH v4.0-r3 |
| | SSO agent | SA-WEB v4.0-r3 |
| Guidance documents | iSIGN+ v4.0 Preparative procedures v1.2<br>iSIGN+ v4.0 Operational user guidance v1.2 | |

**[Table 5] TOE identification**

| | |
|---|---|
| Scheme | Korea Evaluation and Certification Guidelines for IT Security (MSIT Notice No.2022-61, October 31, 2022)<br>Korea Evaluation and Certification Regulation for IT Security (May 17, 2021) |
| TOE | iSIGN+ v4.0 |
| Common Criteria | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017 |
| EAL | EAL1+ (ATE_FUN.1) |
| Protection Profile | Korean National Protection Profile for Single Sign On V3.0 |
| Developer | Penta Security Inc. |
| Sponsor | Penta Security Inc. |
| Evaluation Facility | Korea Security Evaluation Laboratory (KSEL) |
| Completion Date of Evaluation | July 19, 2024 |
| Certification Body | IT Security Certification Center |

**[Table 6] Additional identification information**

# 3. Security Policy

The TOE complies security policies pertaining to the following security functional requirenents defined in the ST [4].

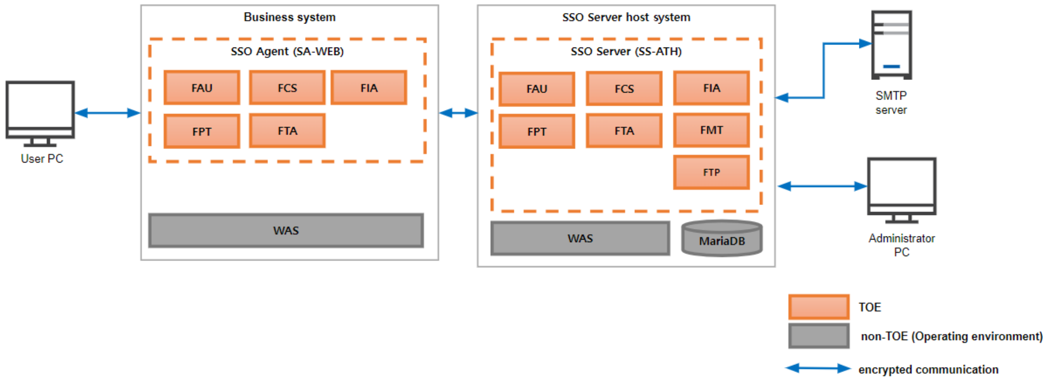
- Security Audit
- Cryptographic Support
- Identification and Authentication
- Protection of the TSF
- TOE Access
- Security Management
- Trusted channels

# 4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST [4]. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 5])

# 5. Architectural Information

As shown in [Figure 2], the TOE provides security functions such as [FAU, FCS, FIA, FPT, FTA, FMT, FTP].



[Figure 2] Logical scope of the TOE

The following security functions are provided by the TOE:

### [SSO server]

- **Security audit**

  Audit data generated from TOE components (SSO server, SSO agent) are stored in the DBMS of the SSO server. Authorized administrators can view all logs after successfully identifying and authenticating to the SSO server and logging into the management tool.

  The SSO server periodically checks the disk usage of audit data and notifies the 0 level administrator by email if it exceeds the disk usage threshold or disk usage limit. If the disk usage limit is exceeded, the audit data is deleted file by file, starting with the oldest audit data.

  If a potential security violation occurs (Audit trail storage threshold/limit exceeding event, administrator or user successive authentication failure event, self-test or integrity verification failure event) during TOE operation, response actions are taken, such as notifying the 0 level administrator by email.

- **Cryptographic support**

The SSO server uses a verified encryption module (CIS-CC V4.0) to generate KEK, DEK, integrity verification key, and token encryption/decryption key. KEK is used to encrypt and decrypt token encryption/decryption key/DEK/integrity verification key, DEK is used to encrypt and decrypt TSF data and mutual authentication data between TOE components, and integrity verification key is used to verify the integrity of TSF execution code and TSF data. The token encryption and decryption key is used to encrypt and decrypt the authentication token. The TOE performs encryption and decryption using the SEED (128 bits, CBC mode) encryption algorithm provided by the verified encryption module (CIS-CC V4.0). In addition, the integrity of the TSF and TSF data is verified using the HMAC SHA256 algorithm, and one-way encryption of administrator and user passwords is performed using the SHA256 algorithm.

All encryption keys created in the TOE are immediately destroyed by being overwritten 5 times (0x00) immediately after use.

- **Identification and authentication**

The SSO server provides an identification and authentication mechanism for administrators based on ID and password. While administrator identification and authentication are in progress, the entered password is changed to masking characters and output. Also, when processing an administrator login failure, detailed information on the reason for the failure is not provided.

When the number of administrator authentication failures reaches the allowable number of failures set by the 0~1 level administrator, the administrator account is locked for the time set by the 0~1 level administrator.

The TOE performs mutual authentication between separate TOE components (SSO server, SSO agent) using its own implemented protocol (request protocol and response protocol).

- **Protection of the TSF**

  TSF data transmitted between separate components of the TOE (SSO server and SSO agent) is safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2).

  TSF data required for the operation of the SSO server is protected from unauthorized exposure and modification by being encrypted with a verified encryption module (CIS-CC V4.0).

  The SSO server performs integrity verification of all TSFs and TSF data on the SSO server at startup and upon request from the 0 level administrator. It also performs self-testing of the authentication token generation and verification process at startup and periodically.

- **TOE access**

  The number of simultaneous sessions between 0~2 level administrators, excluding level 3 administrators, and between the same accounts is limited to a maximum of 1. And the administrator can only connect from the accessible IP set in the management tool. Additionally, the maximum number of simultaneous sessions for the same user that can use business services is limited to 1.

  The session that the administrator manages and connects to the SSO server through the management tool is automatically terminated when the administrator session timeout time set in the management tool by the 0~1 level administrator has elapsed.

- **Security management**

  Authorized administrators can perform security function management and TSF data management through management tools through the TOE identification and authentication process. For 3 level administrators, only the audit log review function can be used among the security management functions provided by the TOE, and other security management functions cannot be used.

- **Trusted channels**

  TSF data transmitted between the SSO server and external mail servers is safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2). In addition, the SSO server forms a communication channel between itself and the mail server based on the mail server information (server address and port, mail user ID/password) set by the 0~1 level administrator in the management tool and identifies the corresponding mail server.

**[SSO agent]**

- **Security audit**

  The SSO agent creates audit records during the operation process and stores them in the DBMS within the SSO server to track responsibility for security-related actions. When the connection between the SSO server and SSO agent is lost, the SSO agent records audit records in a file and transmits the audit record file to the SSO server at the time of connection.

- **Cryptographic support**

  The SSO agent generates encryption keys and performs encryption operations using the encryption algorithm provided by the verified encryption module (CIS-CC V4.0).

  The SSO agent acquires the KEK using the salt.dat file (Includes KEK_salt, encrypted DEK, encrypted integrity verification key) generated by the SSO server and distributed offline and the KEK derived password, and obtains the DEK and integrity verification key by decrypting the DEK and integrity verification key encrypted with the KEK. DEK is used to encrypt and decrypt TSF data and mutual authentication data between TOE components, and the integrity verification key is used to verify the integrity of TSF executable code and TSF data. The TOE performs encryption and decryption using the SEED (128 bits, CBC mode) encryption algorithm provided by the verified encryption module (CIS-CC V4.0), and also verifies the integrity of the TSF and TSF data using the HMAC SHA256 algorithm.

All encryption keys created in the TOE are immediately destroyed by being overwritten 5 times (0x00) immediately after use.

- **Identification and authentication**

  The SSO agent provides an identification and authentication mechanism for users based on ID and password. In addition, users who are successfully identified and authenticated can use the authentication token to access business services assigned to the user by 0~2 level administrators. During user identification and authentication, the entered password is changed to masked characters and output, and when handling user login failure, detailed information on the reason for the failure is not provided.

  When the number of user authentication failures reaches the allowable number of failures set by the 0~1 level administrator, the user account is locked for the time set by the 0~1 level administrator.

- **Protection of the TSF**

  TSF data transmitted between the SSO server and SSO agent, which are separate components of the TOE, are safely protected from exposure and modification through a secure encrypted transmission protocol (TLS V1.2).

The SSO agent's TSF data is encrypted with a verified encryption module (CIS-CC V4.0) and stored in the salt.dat file to protect it from unauthorized exposure and modification. In addition, integrity verification is performed on all TSF executable files and TSF data at startup and periodically (every 6 hours).

- **TOE access**

  Users can access business services only from the accessible IP set by the 0~2 level administrator in the management tool. In addition, users can only access business services that have been mapped to the corresponding user ID by 0~2 level administrators through management tools.

  The session in which the user accesses the business service is automatically terminated when the user session timeout time set by the 0~1 level administrator in the management tool has elapsed.

# 6. Documentation

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

| Identifier | Data |
|---|---|
| iSIGN+ v4.0 Preparative procedures v1.2 | June 25, 2024 |
| iSIGN+ v4.0 Operational user guidance v1.2 | May 30, 2024 |

**[Table 7] Documentation**

# 7. TOE Testing

The developer took a testing approach based on the security services provided by each TOE component based on the operational environment of the TOE. The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1. The evaluator performed all the developer’s tests, and conducted independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST [4]. The evaluator considered the followings when devising a test subset:

- TOE security functionality: The TOE is software used to enable the user to access various business systems and use the service through a single user login without additional login action, and
- Developer's testing evidence: The evaluator analyzed evaluation deliverables for ATE_FUN.1, and ATE_IND.1 to understand behavior of the TOE security functionality and to select the subset of the interfaces to be tested, and
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL1+(ATE_FUN.1), and the evaluator tried to balance time and effort of evaluator's activities between EAL1+ assurance components.

In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [3].

## 8. Evaluated Configuration

The TOE is software consisting of the following components:

- TOE : iSIGN+ v4.0
- TOE Components : SSO server(SS-ATH v4.0-r3), SSO agent(SA-WEB v4.0-r3)

The TOE is identified by TOE name and version number including release number. The TOE identification information is provided via GUI. And the guidance documents listed in this report chapter 6, [Table 7] were evaluated with the TOE.

# 9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL1+(ATE_FUN.1).

## 9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (ST reference, TOE reference, TOE overview and TOE description), and these four descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The ST clearly and unambiguously defines the extended SFR component. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification describes how the TOE meets each SFR, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

## 9.2 Development Evaluation (ADV)

The functional specifications specify the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their purpose, method of use and all parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict PASS is assigned to the assurance class ADV.

## 9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and the interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the

TOE in a secure manner. The guidance documents take into account the various types of users(e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

## 9.4 Life Cycle Support Evaluation (ALC)

The developer has uniquely identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

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

The verdict PASS is assigned to the assurance class ALC.

## 9.5 Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore, the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore, the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

## 9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

## 9.7 Evaluation Result Summary

| Assurance Class | Assurance Component | Evaluator Action Elements | Verdict | | |
|---|---|---|---|---|---|
| | | | Evaluator Action Elements | Assurance Component | Assurance Class |
| ASE | ASE_INT.1 | ASE_INT.1.1E | PASS | PASS | PASS |
| | | ASE_INT.1.2E | PASS | | |
| | ASE_CCL.1 | ASE_CCL.1.1E | PASS | PASS | |
| | ASE_OBJ.1 | ASE_OBJ.1.1E | PASS | PASS | |
| | ASE_ECD.1 | ASE_ECD.1.1E | PASS | PASS | |
| | | ASE_ECD.1.2E | PASS | | |
| | ASE_REQ.1 | ASE_REQ.1.1E | PASS | PASS | |
| | ASE_TSS.1 | ASE_TSS.1.1E | PASS | PASS | |
| | | ASE_TSS.1.2E | PASS | | |
| ALC | ALC_CMS.1 | ALC_CMS.1.1E | PASS | PASS | PASS |
| | ALC_CMC.1 | ALC_CMC.1.1E | PASS | PASS | |
| AGD | AGD_PRE.1 | AGD_PRE.1.1E | PASS | PASS | PASS |
| | | AGD_PRE.1.2E | PASS | | |
| | AGD_OPE.1 | AGD_OPE.1.1E | PASS | PASS | |
| ADV | ADV_FSP.1 | ADV_FSP.1.1E | PASS | PASS | PASS |
| | | ADV_FSP.1.2E | PASS | | |
| ATE | ATE_FUN.1 | ATE_FUN.1.1E | PASS | PASS | PASS |
| | ATE_IND.1 | ATE_IND.1.1E | PASS | PASS | |
| | | ATE_IND.1.2E | PASS | | |
| AVA | AVA_VAN.1 | AVA_VAN.1.1E | PASS | PASS | PASS |
| | | AVA_VAN.1.2E | PASS | | |
| | | AVA_VAN.1.3E | PASS | | |

**[Table 8] Evaluation Result Summary**

# 10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE is implemented to provide a mutual authentication mechanism for TOE components (SSO server, SSO agent) using timestamp information provided in the operating environment before linking between TOE components to perform the SSO function. Therefore, the administrator must set the operating system time to match accurately before operating the SSO server and SSO agent.
- The TOE is implemented to overwrite the oldest audit data when the audit data storage reaches a set limit. Therefore, if the management tool administrator (0 level administrator) receives an email notification due to the audit data storage threshold or limit being exceeded, an audit log backup must be performed immediately to prevent audit data from being lost.
- The authorized administrator must ensure that the password used to generate the key encryption key (KEK) is different from the password used for administrator login, and must not use information that can be easily inferred by an attacker, such as personal information. To ensure the safety of the KEK, it is recommended to set and use the KEK at a level equivalent to the security strength of the administrator's password (set a rule combination of 3 or more of English letters/numbers/special characters and use 9 or more characters).
- The TOE purchaser must use the SSO agent to link the user identification and

authentication functions with the TOE in the TOE operating environment (business system) through additional development or modification. In this case, the TOE operating environment must be developed by complying with the requirements provided by the TOE.

- SSL communication is implemented to perform secure communication between SSO server and mail server to send warning mails for security violation events. Authorized administrators should note that a public certificate must be used as the SSL certificate of the mail server that works with SSO server to send warning mails normally.

# 11. Evaluation Evidence

| Identifier | Issue date |
|---|---|
| iSIGN+ v4.0 Security Target v1.2 | 2024.06.25 |
| iSIGN+ v4.0 Functional Specification v1.2 | 2024.07.02 |
| iSIGN+ v4.0 Preparative procedures v1.2 | 2024.06.25 |
| iSIGN+ v4.0 Operational user guidance v1.2 | 2024.05.30 |
| iSIGN+ v4.0 Configuration Management Documentation v1.1 | 2024.06.18 |
| iSIGN+ v4.0 Test Documentation v1.1 | 2024.07.02 |

**[Table 9] Evaluation Evidence**

# 12. Acronyms and Glossary

| | |
|---|---|
| CC | Common Criteria |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| OR | Observation Report |
| PP | Protection Profile |

|  |  |
|---|---|
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TSF Interface |

|  |  |
|---|---|
| Validated Cryptographic Module | A cryptographic module that is validated and given a validation number by validation authority |
| Management tools | It is a web-based user interface for administrators to perform audit review and SSO server security functions and TSF data management functions, and is composed of multiple web pages. |
| Administrator | An administrator who connects to the SSO server through a management tool and performs management functions, and is classified into 0~3 level administrators depending on authority. |
| Integrity verification key | The key used to create the HMAC value when storing TSF data in DBMS. |
| Decryption | The act that restoring the ciphertext into the plaintext using the decryption key |
| User | Authorized administrator and authorized end-user |
| Encryption | The act that converting the plaintext into the ciphertext using the encryption key |
| Business services ID | This is a unique number assigned when adding a service and is used when setting up the service in the business system |
| Business System | An application server that authorized users access through ‘SSO’ |
| End User | A user who does not have authority to manage |

| | |
|---|---|
| | security functions or manage TSF data through management tools, and uses the TOE's initial login or SSO login function to use the business system |
| Authorized Administrator | Authorized user to securely operate and manage the TOE |
| Token encryption and decryption key | The key used to encrypt and decrypt the authentication token when generating and verifying it |
| Token serial number | As a means of preventing the reuse of authentication tokens, a token serial number is generated for each user session. When an authentication token is created, '1' is initially given, and when the authentication token is reissued (renewed) after requesting authentication token verification, it is incremented by 1 in the authentication server |
| Database Management System (DBMS) | A software system composed to configure and apply the database. TSF data is stored and managed in DBMS |
| DEK | The key that encrypts user information, server and agent information, and SecureData used for mutual authentication |
| KEK | The key that encrypts the DEK, integrity verification key, and token encryption/decryption key |
| Transport Layer Security (TLS) | This is a cryptographic protocol between a SSL-based server and a client and is described in RFC 2246. Used when transmitting TSF data between TOE |
| TSF Data | Data for the operation of the TOE upon which the |

| | |
|---|---|
| | enforcement of the SFR relies. This includes DEK, integrity verification keys, token encryption and decryption keys, and user information |
| 0 level administrator | This refers to the initially created administrator. Level 0 administrators can use all management and inquiry functions |
| 1 level administrator | This is an administrator who is allowed to use service inquiry, management, setting functions, all integrated management functions, and product registration functions. All functions except integrity verification can be used |
| 2 level administrator | This administrator is allowed to view administrator logs and user logs, manage user identity, and manage agents |
| 3 level administrator | Administrator log and user log inquiry TSF function is allowed |

# 13. Bibliography

The evaluation facility has used the following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3] iSIGN+ v4.0, Evaluation Technical Report V2.00, August 5, 2024

[4] iSIGN+ v4.0, Security Target v1.2, June 25, 2024

[5] Korean National Protection Profile for Single Sign On V3.0, October 14, 2022