KECS-CR-19-17

# ISign+ v3.0

# Certification Report

Certification No.: KECS-CISS-0924-2019

2019. 4. 10.

IT Security Certification Center

| History of Creation and Revision | | | |
|---|---|---|---|
| No. | Date | Revised Pages | Description |
| 00 | 2019.04.10. | - | Certification report for ISign+ v3.0<br>- First documentation |

This document is the certification report for ISign+ v3.0 of Penta Security System Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory (KSEL)

# Table of Contents

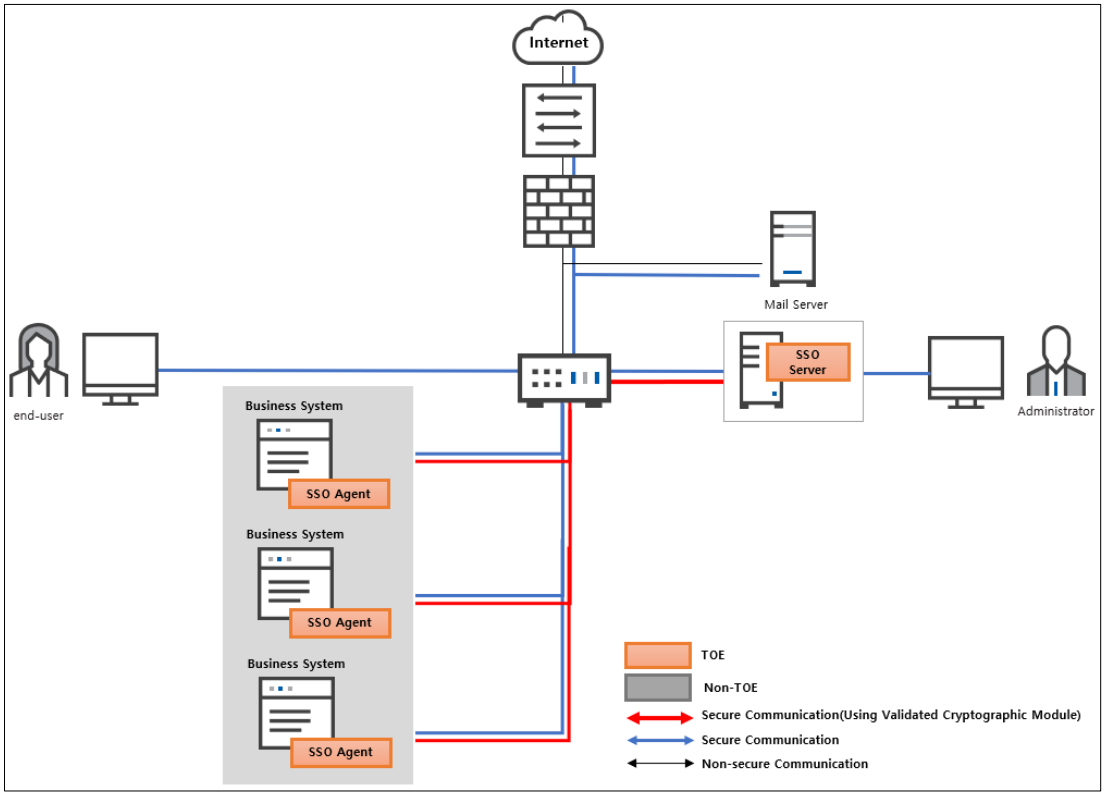
# 1. Executive Summary

This report describes the evaluation result certification body on the results of the ISign+ v3.0 developed by Penta Security System 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, TOE access, TSF protection, and security management function.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on March 6, 2019. 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 PP for Single Sign On V1.0 [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] Operational environment of the TOE

When the end-user or the management console administrator accesses the TOE through web browser, WAS, which is operating environment of SSO agent and SSO server supports secured channel by HTTPS/TLS.

The TOE consists of SSO server and SSO agent. Using user information stored in the DBMS, the SSO server provides various functions such as user login verification, authentication token issuance and management/policy setting. The SSO agent also provides various functions such as request of verifying the authentication token, and is installed and operated on each system. The external IT entity (Mail server to send e-mails, such as management console administrator notification when audit data loss is predicted) is required to operate the TOE.

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

| Component | | Specification |
|---|---|---|
| HW | CPU | Intel Pentium Processor G4600 3M Cache 3.60 GHz or higher |
| | Memory | 8 GB or higher |
| | HDD | 500 MB or higher (Space for TOE installation) |
| | NIC | 100/1000 Mbps x 1EA or higher |
| SW | DBMS | MariaDB v10.2.22 64bits |
| | WAS | Apache Tomcat v8.5.35 (openjdk 1.8.0_202) 64bits |
| OS | | Debian GNU/Linux 8.9(jessie) (kernel 3.16.59-1) 64bits |

[Table 1] Hardware and Software Requirements for SSO Server

| Component | | Specification |
|---|---|---|
| HW | CPU | Intel Pentium Processor G4600 3M Cache 3.60 GHz or higher |
| | Memory | 8 GB or higher |
| | HDD | 10 MB or higher (Space for TOE installation) |
| | NIC | 100/1000 Mbps x 1EA or higher |
| SW | WAS | Apache Tomcat v8.5.35 (openjdk 1.8.0_202) 64bits |
| OS | | Debian GNU/Linux 8.9(jessie) (kernel 3.16.59-1) 64bits |

[Table 2] Hardware and Software Requirements for SSO Agent

[Table 3] shows the hardware and software requirements for the management console administrator and end-user's PC.

| Component | | Specification |
|---|---|---|
| HW | CPU | Intel core i5-4200U 1.60 GHz or higher |
| | Memory | 4 GB or higher |
| | HDD | 100 GB or higher |
| | NIC | 100/1000 Mbps x 1EA or higher |
| SW | | Chrome 71.0.3578.98(official build) (64-bit) |
| OS | | Windows 10 Pro (64-bit) |

[Table 3] HW and SW Requirements for the management console administrator and user's PC

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

# 2. Identification

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

| | | |
|---|---|---|
| TOE Name | ISign+ v3.0 | |
| TOE Version | v3.0.27 | |
| TOE components | SSO Server | SS-ATH v3.0.27 |
| | SSO Agent | SA-WEB v3.0.27 |
| Guidance documents | ISign+ v3.0 Preparative Procedure U-IG : 1.8<br>(UIG_ISign+_v3.0_ Preparative Procedure _v1.8.pdf)<br>ISign+ v3.0 Operation Guide U-OG : 1.5<br>(UOG_ISign+_v3.0_Operation Guide _v1.5.pdf) | |

[Table 4] TOE identification

| | |
|---|---|
| Scheme | Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017)<br>Korea Evaluation and Certification Regulation for IT Security (September 12, 2017) |
| TOE | ISign+ v3.0 |
| 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 V1.0 |
| Developer | Penta Security System Inc. |
| Sponsor | Penta Security System Inc. |
| Evaluation Facility | Korea Security Evaluation Laboratory (KSEL) |
| Completion Date of Evaluation | March 6, 2019 |

| Certification Body | IT Security Certification Center |
|---|---|

[Table 5] 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
- TOE access
- Protection of the TSF
- Security Management

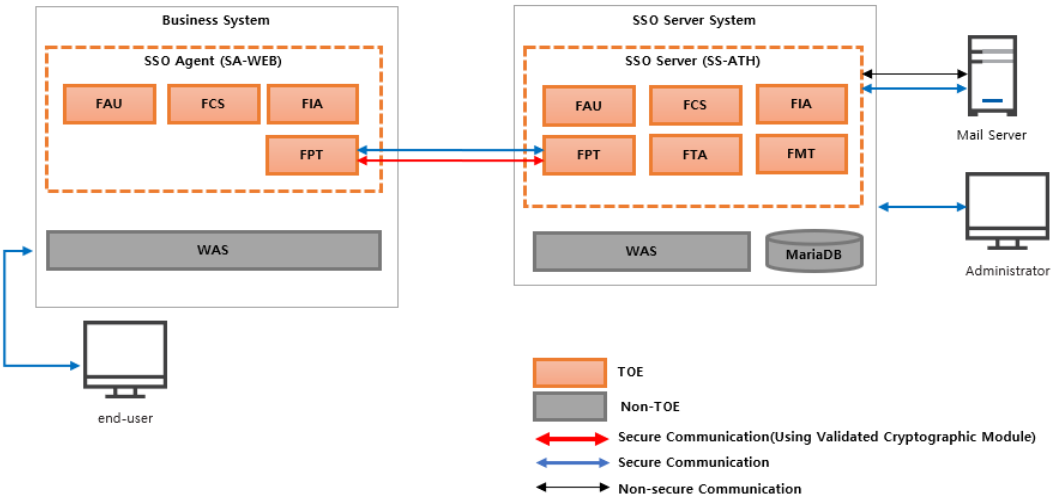
# 4. Assumptions and Clarification of Scope

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 4])

# 5. Architectural Information

TOE consists of the SSO Server and SSO Agent. Cryptographic module(CIS-CC v3.3) validated under the KCMVP is embedded in the TOE components. [Figure 2] shows the logical scope of the TOE.




[Figure 2] Logical scope of the TOE

# 6. Documentation

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

| Identifier | Date |
|---|---|
| ISign+ v3.0 Preparative Procedure U-IG : 1.8<br>(UIG_ISign+_v3.0_ Preparative Procedure _v1.8.pdf) | February 27, 2019 |
| ISign+ v3.0 Operation Guide U-OG : 1.5<br>(UOG_ISign+_v3.0_ Operation Guide _v1.5.pdf) | February 12, 2019 |

[Table 6] 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+ v3.0 (v3.0.27)

- TOE Components : SS-ATH v3.0.27(SSO Server), SA-WEB v3.0.27(SSO Agent)

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

And the guidance documents listed in this report chapter 6, [Table 6] were evaluated with the TOE.

# 9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [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 | | |

| Assurance Class | Assurance Component | Evaluator Action Elements | Verdict | | |
|---|---|---|---|---|---|
| | | | Evaluator Action Elements | Assurance Component | Assurance Class |
| | | AVA_VAN.1.3E | PASS | | |

[Table 7] 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 performs mutual authentication between the TOE components (SSO Server and SSO Agent) using timestamp information provided by the operational environment (OS) prior to interoperating with each other. Thus, administrator should make sure of the reliability of the OS time of the TOE components, and apply proper mutual authentication effective time (default 60 second recommended) to authenticate each other successfully.
- The TOE overwrites the oldest stored audit records if audit storage is full. Thus, 0-level administrator should immediately backup audit data to prevent possible audit data loss if he receives an alarming e-mail from the TOE.
- The TOE sends temporary passwords to a related user via e-mail when adding an administrator, and adding or password initializing end-users. Thus, authorized administrator should be careful temporary passwords were not exposed by applying “SSL enable(default) or TLS enable” in Event Alarm Setting in SMTP Setting (“plain text enable” not recommended).
- The TOE allows an authorized administrator to manage password policies

(length limit, including special/alphabetical/number character, etc.). Weak password policies are vulnerable to brute force attacks and lead to a password exposure, Thus, it is recommended that password policies (including passwords used to derive KEK) containing over 9 characters and special/alphabetical/number characters are applied to ensure the safety of the administrator and end-user passwords.

# 11. Security Target

ISign+ v3.0 Security Target V1.4 [4] is included in this report for reference.

# 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 |
| KCMVP | Korea Cryptographic Module Validation Program |

| | |
|---|---|
| Management console | Application program that provides GUI, CLI, etc. to the administrator and provides system management and configuration |
| Management console administrator | Authorized user to securely operate and manage the TOE. There are 0~3-level administrators based on their access levels. |
| 0-level administrator | Management console administrator created initially when the SSO server installed. Its ID is ‘adm’ which is fixed and not changeable. 0-level admin can operate the TOE. And only the administrator can use the [Integrity Verification] function and reboot the SSO server and the SSO agent. |
| 1-level administrator | Management console administrators who can manage function of SSO server. |
| 2-level administrator | Management console administrators who can view management logs and user logs, manage accounts of users and download the manual. |
| 3-level administrator | Management console administrators can view management logs and user logs, download the manual. |
| end-user | Users of the TOE who want to use the business system, not the administrators of the TOE |

# 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+ v3.0, Evaluation Technical Report V1.00, March 6, 2019

[4] ISign+ v3.0 Security Target D-ST : 1.4, February 22, 2019

[5] Korean National Protection Profile for Single Sign On V1.0, August 18, 2017