KECS-CR-23-38

# TouchEn Wiseaccess v1.4

# Certification Report

Certification No.: KECS-CISS-1244-2023

2023. 6. 2.

IT Security Certification Center

| History of Creation and Revision | | | |
|---|---|---|---|
| No. | Date | Revised Pages | Description |
| 00 | 2023. 6. 2. | - | Certification report for TouchEn Wiseaccess v1.4<br>- First documentation |

This document is the certification report for TouchEn Wiseaccess v1.4 of RaonSecure Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

## Table of Contents

# 1. Executive Summary

This report describes the evaluation results drawn by the evaluation facility on the results of the TouchEn Wiseaccess v1.4 developed by RaonSecure Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation results 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, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.

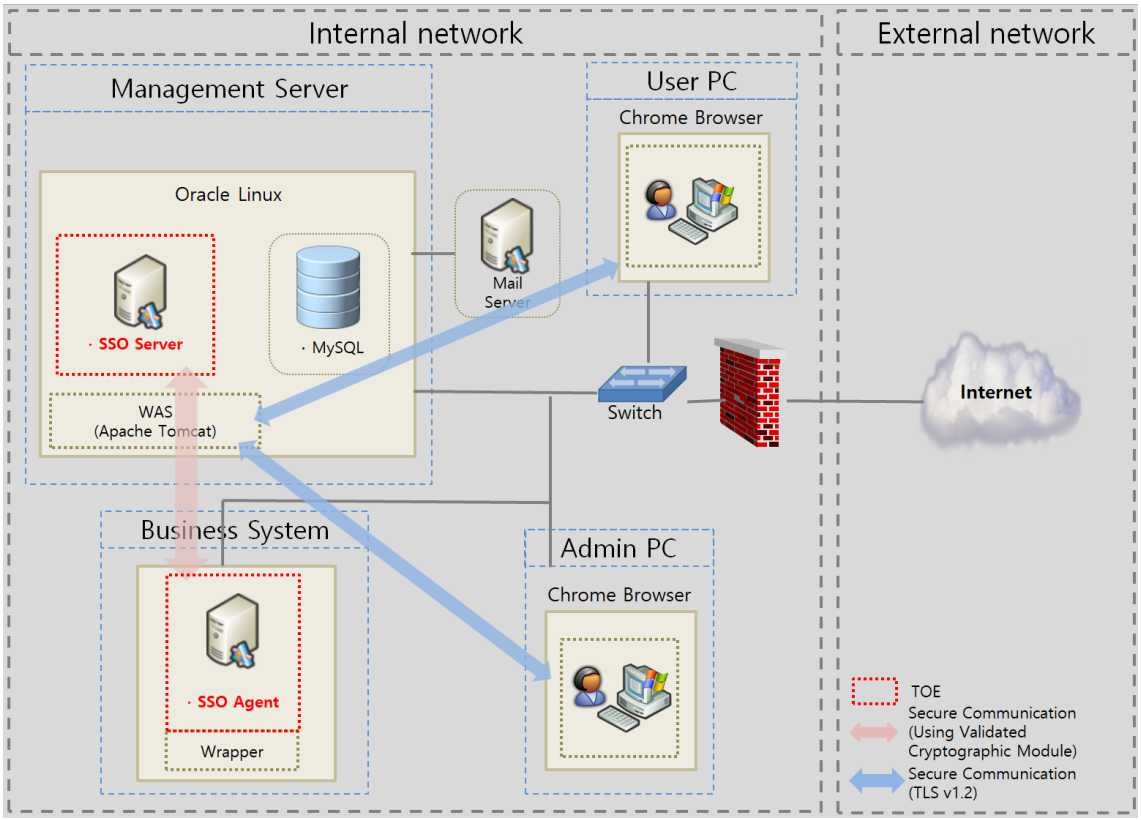
The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on May 31, 2023.

The ST claims conformance to the Korean National Protection Profile for Single Sign On V1.1[3]. 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+. 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 a newly defined component in the Extended Component Definition chapter of the PP, therefor the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

The TOE provides the security audit function that records and manages critical events as audit data when activating the security functionality and management function, function of protecting the data that stored in the TSF controlled repository, and TSF protection function such as TSF self-testing. In addition, the TOE provides authentication failure handling, identification and authentication functions including mutual authentication between the TOE components, cryptographic support function such as cryptographic key management and cryptographic operation for issuing a token, security management function for management of security functions behavior and configuration, and the TOE access function to manage the authorized administrator’s interacting session.

In addition, the token requires confidentiality and integrity protection, and the TOE executable code requires integrity protection.

[Figure 1] shows the operational environment of the TOE.




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

The operational environment of the TOE is composed of the SSO server that is installed in the management server and the SSO Agent that is installed in the business system.

The TOE is provided in software. The SSO Server is installed in the management server as process type and performs security management. The SSO Agent is installed in each business system. It is provided in a combination 'API type' composed of the library file which performs the authentication token issuance and verification functions, 'process type' composed of the executable file.

The SSO Server performs the security management of the TOE via web browser which supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). A Wrapper is used for compatibility with various business systems, out of the TOE scope.

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

| Component | | | Requirement |
|---|---|---|---|
| SSO Server | H/W | CPU | Intel(R) Xeon(R) 2.8 GHz or higher |
| | | RAM | 8 GB or higher |
| | | HDD | Space required for TOE installation is 1 GB or higher |
| | | NIC | 100/1000 Ethernet Port x 1 EA or higher |
| | S/W | OS | Oracle Linux 8.7 (64 bit, Kernel 5.15.0) |
| | | DBMS | MySQL 8.0.33 |
| | | Java | OpenJDK 1.8.0_372 (64 bit) |
| | | WAS | Apache Tomcat 8.5.88 |
| SSO Agent | H/W | CPU | Intel(R) Xeon(R) 2.8 GHz or higher |
| | | RAM | 8 GB or higher |
| | | HDD | Space required for TOE installation is 1 GB or higher |
| | | NIC | 100/1000 Ethernet Port x 1 EA or higher |
| | S/W | OS | Oracle Linux 8.7 (64 bit, Kernel 5.15.0) |
| | | Java | OpenJDK 1.8.0_372 (64 bit) |
| | | WAS | Apache Tomcat 8.5.88 |

**[Table 1] TOE Hardware and Software Specifications**

Administrator uses a PC which can operate web browser to use the security management. Administrator PC minimum requirements are shown in [Table 2].

| Component | | Requirement |
|---|---|---|
| S/W | Web Browser | Chrome 112.0 |

**[Table 2] Administrator PC Requirements**

In addition, external IT entities linked for TOE operation are shown in [Table 3].

| Component | Requirement |
|---|---|
| Mail Server | Sends an e-mail about potential security violations to the authorized administrator on the designated receiving side from the SSO server. |

**[Table 3] External IT entity**

**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 reference is identified as follows.

| | |
|---|---|
| TOE | TouchEn Wiseaccess v1.4 |
| Version | v1.4.4.3 |
| TOE Components | - TouchEn Wiseaccess v1.4 Server v1.4.4.3<br>- TouchEn Wiseaccess v1.4 Agent v1.4.4.3 |
| Manuals | - TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3<br>- TouchEn Wiseaccess v1.4 API Manual v1.4.2<br>- TouchEn Wiseaccess v1.4 Installation Guide v1.4.3 |

**[Table 4] TOE Identification**

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

| | |
|---|---|
| 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) |
| Common Criteria | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017 |
| TOE | TouchEn Wiseaccess v1.4 |
| EAL | EAL1+(ATE_FUN.1) |
| Protection Profile | Korean National Protection Profile for Single Sign On V1.1<br>(December 11, 2019) |
| Developer | RaonSecure Co., Ltd. |
| Sponsor | RaonSecure Co., Ltd. |
| Evaluation Facility | Korea System Assurance (KOSYAS) |
| Completion Date of Evaluation | May 31, 2023 |

**[Table 5] Additional Identification Information**

# 3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

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

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4].

# 4. Assumptions and Clarification of Scope

There are no assumptions in the Security Problem Definition in the ST. 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

## 5.1 Physical Scope of TOE

The physical scope of the TOE consists of the SSO Server, SSO Agent and manuals (Administrator's manual, API manual, Installation guidance). The validated cryptographic module (Key# Crypto V1.5) is embedded in the TOE components.

Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE.

| Category | | Identification | Type |
|---|---|---|---|
| TOE components | SSO Server | TouchEn Wiseaccess v1.4 Server v1.4.4.3 (wiseaccess_server_v1.4.4.3_linux.tar.gz) | Software (Distributed |

| | | | |
|---|---|---|---|
| | SSO Agent | TouchEn Wiseaccess v1.4 Agent v1.4.4.3<br>(wiseaccess_agent_v1.4.4.3_linux.tar.gz) | as a CD) |
| Manuals | | TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3<br>(TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3.pdf) | PDF (Distributed as a CD) |
| | | TouchEn Wiseaccess v1.4 API Manual v1.4.2<br>(TouchEn Wiseaccess v1.4 API Manual v1.4.2.pdf) | |
| | | TouchEn Wiseaccess v1.4 Installation Guide v1.4.3<br>(TouchEn Wiseaccess v1.4 Installation Guide v1.4.3.pdf) | |

**[Table 6] Physical Scope of the TOE**

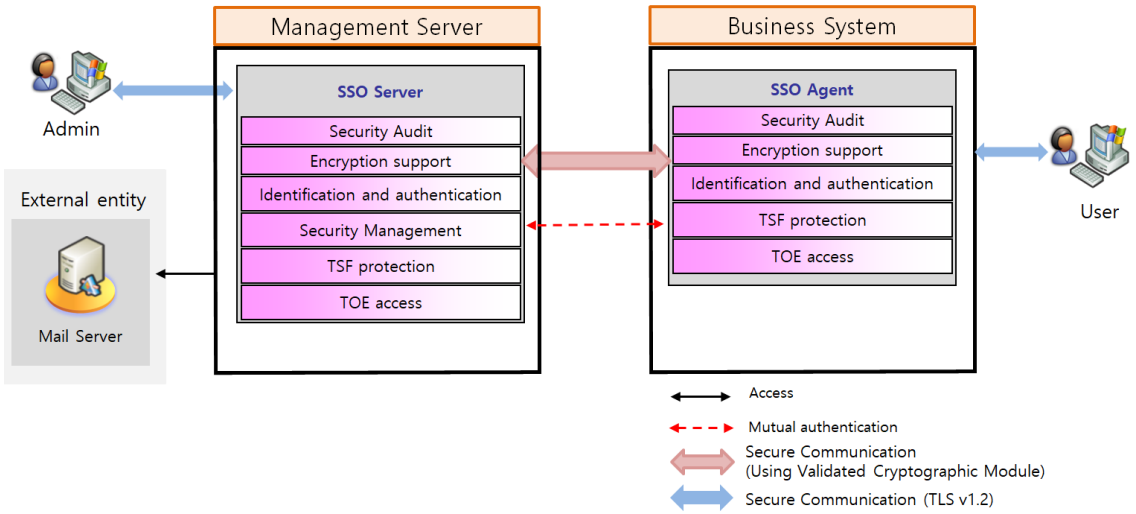
The validated cryptographic module included in the TOE is as follows.

| Classification | Description |
|---|---|
| Cryptographic Module | Key# Crypto V1.5 |
| Validation No. | CM-220-2027.11 |
| Developer | RaonSecure Co., Ltd. |
| Validation Date | 2022. 11. 2. |
| Expiration Date | 2027. 11. 2. |

**[Table 7] Validated Cryptographic Module**

## 5.2 Logical Scope of TOE

The logical scope of the TOE is shown in [Figure 2].




**[Figure 2] Logical Scope of the TOE**

### ▣ Security Audit

<SSO Server>

SSO Server manages the TSF data from browser and generates the audit data on security management. Generate the audit data about management and security setting, information change of the TSF data, identification and authentication, integrity test, start/termination of the audit function and security violation.

The TOE corresponds to security violations and mutual authentication between the SSO Server and SSO Agent. Generate the audit data about cryptographic key management, integrity test and start/termination of the audit function accordingly.

The audit data includes log generation time, identity of the subject, result of the event (success or failure), type of the event and additional audit data.

The audit data is stored in the DBMS. The audit data is provided in a manner suitable for the authorized administrator. Protect the data from unauthorized users to delete.

Only the top-level administrator can search the audit data.

SSO Server shall periodically check audit data storage according to the setting and send a warning email to the administrator when the audit data storage exceeds the threshold. Delete the past records in the DBMS if the past records exceed the deletion threshold.

In addition, perform corresponding actions (send a warning email to the authorized administrator) on security violations (self-test failure of the validated cryptographic module ‘Key# Crypto V1.5’, exceed the audit storage, self-verification and integrity test failure of the SSO Server and the SSO Agent, the audit storage failure, exceeding the number of authentication failures (administrator/end-user)).

<SSO Agent>

SSO Agent generates the audit data about the mutual authentication between the SSO Agent and the SSO Server, authentication token generation/operation/destruction using the cryptographic key, cryptographic key management, integrity test and start/termination of the audit function.

The audit data includes log generation time, subject's identity, event result (success or failure), items about event type and additional audit data.

**▣ Cryptographic support**

<SSO Server>

SSO Server generates random numbers with the RBG for mutual authentication and verifies signature with the digital signature algorithm. After completing mutual authentication, distribute cryptographic key to the SSO Agent. Use Key# Crypto V1.5, a validated cryptographic module. Do not save the encryption key but destory it.

<SSO Agent>

SSO Agent generates random bits with the RBG for mutual authentication with the SSO Server. During mutual authentication, user the digital signature algorithm to perform signature verification. After mutual authentication, use the symmetric algorithm and the MAC algorithm to generate and manage the authentication token. Use the validated cryptographic module, Key# Crypto V1.5, as a cryptographic algorithm. Do not save the encryption key but destory it.

**▣ Identification and authentication**

<SSO Server>
Identify the administrator with ID when attempting identification and authentication, and perform administrator authentication before all the actions. Present the password with '•' to prevent the password from being exposed by providing the information of authentication failure reason.
SSO Server provides the function to prevent reuse of authentication information related to the administrator.
Set administrator's password according to the password rule. If identification and authentication succeeds, the administrator maintains the security management authority.
If the number of authentication attempts via the SSO Server exceeds the allowed number of authentication failures (5 times), lock the account for 10 minutes as the administrator sets.
Perform mutual authentication via implemented protocol for safe communication among TOE components.

<SSO Agent>
SSO Agent identifies the end-user with ID when the end-user initially attempts to identify

and authenticate. Perform the end-user authentication before all the actions. Present the password as '•' to prevent the password from being exposed by providing the information of authentication failure.

After completing the initial identification and authentication of end user, issue an authentication token depending on the implementation and performs identification and authentication with the authentication token. Onetime Token prevents the authentication from being reused. Do not save the authentication token but destroy it.

If the end-user exceeds the allowed number of authentication failures (5 times), lock the end-user's account for the set time interval of user lock.

**▣ Security Management**

<SSO Server>
Conduct security management via SSO Server.
Set security policy for single authentication with organization/service.
Forced to change the password when the authorized administrator accesses for the first time to the security management interface.
There is only top-level administrator who can set and perform all the policy of security management functions.

**▣ Protection of the TSF**

<SSO Server>
SSO Server shall protect the TSF data stored within containers controlled by the TSF and transferred between the TOE components. Run TSF testing to check major security function process. SSO Server shall run self-test for major processes and ensure the integrity of the TOE configuration files and major process periodically during initial start-up and operation. If integrity is compromised, send a warming email to the administrator.
SSO Server safely store and manage the authentication information of end user and administrator in the DBMS.

<SSO Agent>
When transmitting data between separate parts of the TOE, protects the data from disclosure and modification using the secure channel. Check integrity periodically.
SSO Agent shall protect the TSF data stored within containers controlled by the TSF and transferred between the TOE components. Run TSF testing to check major security function process. The TOE shall run self-test for major processes and ensure the integrity of the TOE configuration files and major process periodically during initial start-up and operation. If integrity is compromised, send a warming email to the administrator.
The authentication token is temporarily saved in the user's PC memory and destructed immediately right after the use.

**▣ TOE access**

<SSO Server>
For the time interval of SSO Server inactivity, the administrator performs the automated termination of sessions function. In order to reuse, reauthentication is required.
In addition, limit the maximum number of session connection for the administrator session of security management to 1 to avoid duplication log-in. After the authorized administrator logs in, another administrator PC performs a log-in with the same account, the previous connection will be terminated.
Able to set the allowed IP addresses for administrator to 2. Output 'Access Denied Error!' when accessing from an IP not in the allowed list.

<SSO Agent>
After the end-user's identification and authentication, terminates the session when the idle time of authentication token exceeds. Re-authenticate the user and perform identification and authentication.

# 6. Documentation

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

| Identification | Date |
|---|---|
| TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3<br>(TouchEn Wiseaccess v1.4 Administrator's Manual v1.4.3.pdf) | May 8, 2023 |
| TouchEn Wiseaccess v1.4 API Manual v1.4.2<br>(TouchEn Wiseaccess v1.4 API Manual v1.4.2.pdf) | April 24, 2023 |
| TouchEn Wiseaccess v1.4 Installation Guide v1.4.3<br>(TouchEn Wiseaccess v1.4 Installation Guide v1.4.3.pdf) | May 8, 2023 |

**[Table 8] Documentation**

# 7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [5], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.
These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [6].

# 8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: TouchEn Wiseaccess v1.4
Version: v1.4.4.3
- TouchEn Wiseaccess v1.4 Server v1.4.4.3
- TouchEn Wiseaccess v1.4 Agent v1.4.4.3

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 were evaluated with the TOE

# 9. Results of the Evaluation

The evaluation facility wrote the evaluation results in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation results were based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation (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 (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to 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 Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

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

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

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

The verdict **PASS** is assigned to the assurance class ASE.

## 9.2 Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS

is assigned to ADV_FSP.1.

The verdict **PASS** is assigned to the assurance class ADV.

## 9.3 Guidance Documents Evaluation (AGD)

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

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

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

The verdict **PASS** is assigned to the assurance class AGD.

## 9.4 Life Cycle Support Evaluation (ALC)

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

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

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

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE 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 Results 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 | |

| Assurance Class | Assurance Component | Evaluator Action Elements | Verdict | | |
|---|---|---|---|---|---|
| | | | Evaluator Action Elements | Assurance Component | Assurance Class |
| | ASE_TSS.1 | ASE_TSS.1.1E | PASS | PASS | |
| | | ASE_TSS.1.2E | PASS | | |
| ADV | ADV_FSP.1 | ADV_FSP.1.1E | PASS | PASS | PASS |
| | | ADV_FSP.1.2E | 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 | |
| ALC | ALC_CMC.1 | ALC_CMC.1.1E | PASS | PASS | PASS |
| | ALC_CMS.1 | ALC_CMS.1.1E | PASS | 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 9] Evaluation Results 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 Server must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.

- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.

- The administrator should periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prevent audit data loss.

- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

# 11. Security Target

TouchEn Wiseaccess v1.4 Security Target v1.4.4 [4] is included in this report for reference.

# 12. Acronyms and Glossary

## (1) Acronyms

**CC** Common Criteria

**CEM** Common Methodology for Information Technology Security Evaluation

**EAL** Evaluation Assurance Level

**ETR** Evaluation Technical Report

**SAR** Security Assurance Requirement

**SFR** Security Functional Requirement

**ST** Security Target

**TOE** Target of Evaluation

**TSF** TOE Security Functionality

**TSFI** TSF Interface

## (2) Glossary

**Application Programming Interface (API)**

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

**Authenticated Data**

Information used to verify a user's claimed identity

**Authenticated token**

Authentication data that authorized end-users use to access the business system

**Authorized Administrator**

Authorized user to securely operate and manage the TOE

**Authorized User**

The TOE user who may, in accordance with the SFRs, perform an operation

**Business System**

An application server that authorized end-users access through ‘SSO’

**Decryption**

The act that restoring the ciphertext into the plaintext using the decryption key

**Encryption**

The act that converting the plaintext into the ciphertext using the cryptographic key

**end-user**

Users of the TOE who want to use the business system, not the administrators of the TOE

**External Entity**

An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE

**Top Administrator**

The authorized administrator who has the highest authority to perform all security management functions in the security management interface

**Validated Cryptographic Module**

A cryptographic module that is validated and given a validation number by validation

authority

**Wrapper**

Interfaces for interconnection between the TOE and various types of business systems or authentication systems

# 13. Bibliography

The 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] Korean National Protection Profile for Single Sign On V1.1, December 11, 2019

[4] TouchEn Wiseaccess v1.4 Security Target v1.4.4, May 31, 2023

[5] TouchEn Wiseaccess v1.4 Independent Testing Report(ATE_IND.1) V2.00, May 31, 2023

[6] TouchEn Wiseaccess v1.4 Penetration Testing Report(AVA_VAN.1) V2.00, May 31, 2023