KECS-CR-26-08

V-FRONT v8

Certification Report

Certification No.: KECS-CISS-1390-2026

2026. 2. 25.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2026.2.25.	-	Certification report for V-FRONT v8 - First documentation

This document is the certification report for V-FRONT v8 of AirCUVE 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 result drawn by the evaluation facility on the results of the V-FRONT v8 developed by AirCUVE Co,. LTD. 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, 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 January 26, 2026. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [7] and the Security Target (ST) [4].

The ST claims conformance to the Korean National Protection Profile for Single Sign On V3.1[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 is an ‘integrated authentication’ solution which allows an end-user to access to various business systems with a single log-in.

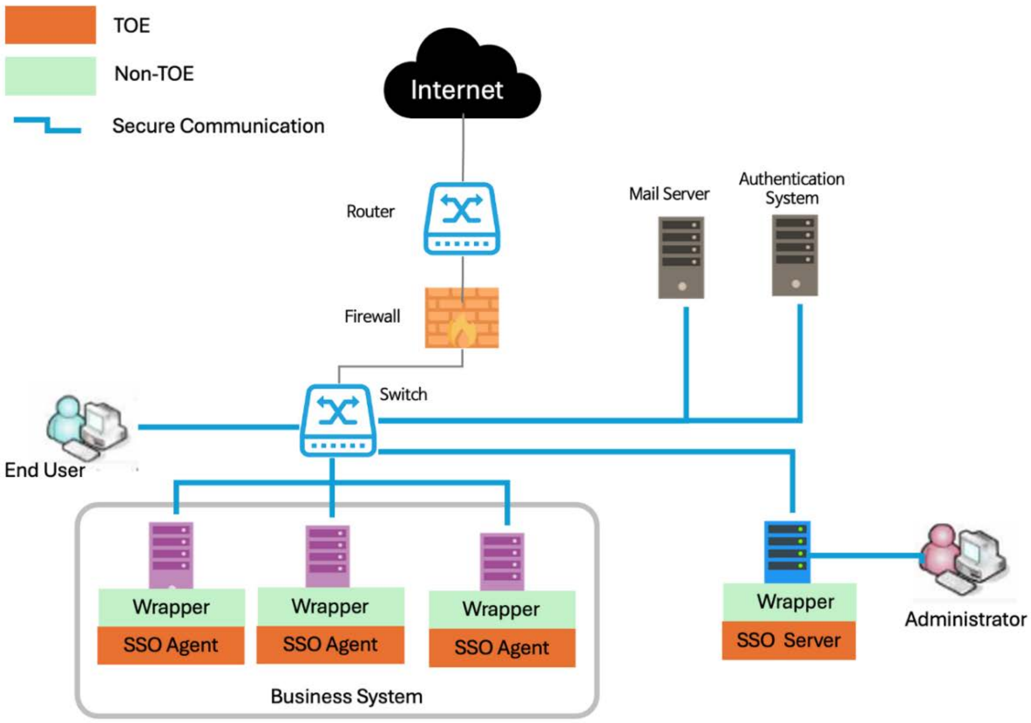
The TOE provides the end user login function using an ID/PW-based authentication method in conjunction with an external authentication system, issues an authentication token during end user login, and verifies the issued authentication token when accessing another business system after user login.

For administrators, an authentication function based on ID and password is provided. Additionally, an OTP-based authentication function is provided after ID/PW-based authentication. For end users, an external authentication system provides the authentication function at the initial authentication phase of Single Sign-On, so it is not included in the TOE.

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 file and configuration file 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 mounted on Web Application Server and operates as a web application. The SSO Agent is installed in each business system web application server in the form of process type. Wrapper is used for compatibility with various business systems and Wrapper is excluded from the scope of the TOE.

The SSO Server performs the security management of the TOE via web browser which supports the confidentiality and integrity of data transmitted for communication between the web browser of the Administrator PC and the web server, which is the operating environment of the management server, must be guaranteed. The SSO server and PostgreSQL, a relational database management system, are interlinked for the purpose of the management of authentication and policy information. External IT entities necessary for the operation of the TOE are email server to notify the authorized administrator in case of audit data loss and to send OTP number for additional authentication, and the authentication system for the end user identification and authentication.

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

Component			Requirement
SSO Server	HW	CPU	Intel CPU : Intel Xeon 3.4Ghz, 4 Core or higher
		RAM	8GB or higher
		HDD	Space required for installation of TOE 100GB or higher
		NIC	10/100/1000Mbps Ethernet Port 1EA or higher
	SW	OS	Ubuntu 22.04 LTS kernel 5.15.0-164-generic (64 bit)
		DBMS	PostgreSQL 17.7
		WAS	Apache Tomcat 10.1.50
SSO Agent	HW	CPU	Intel CPU : Intel Xeon 3.4Ghz, 4 Core or higher
		RAM	8GB or higher
		HDD	Space required for installation of TOE 10GB or higher
		NIC	10/100/1000Mbps Ethernet Port 1EA or higher
	SW	OS	Ubuntu 22.04 LTS kernel 5.15.0-164-generic (64 bit)
		WAS	Apache Tomcat 10.1.50

[Table 1] TOE Hardware and Software specifications

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

Classification		Minimum Requirement
SW	Web Browser	Chrome 143.0

[Table 2] Administrator PC Requrements.

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

Component	Requirement
Authentication System	Perform end user identification and authentication
Mail Server	Send OTP for additional administrator authentication
	Send administrator alert massages

[Table 3] External 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	V-FRONT v8
Version	8.1.1.3
TOE Components	V-FRONT v8 Server 8.1.1.2 V-FRONT v8 Agent 8.1.1.2
Manuals	V-FRONT v8 Operational User Guidance 1.9

[Table 4] TOE identification

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

Scheme	Korea IT Security Evaluation and Certification Guideline (Ministry of Science and ICT Guidance No. 2022-61, October 31, 2022) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	V-FRONT v8
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-07-002 Version 1.1, July 2024
Common Evaluation Methodology	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1 Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-07-002 Version 1.1, July 2024
EAL	EAL1+(ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Single Sign On V3.1
Developer	AirCUVE Co., LTD.
Sponsor	AirCUVE Co., LTD
Evaluation Facility	Korea System Assurance, Inc. (KOSYAS)
Completion Date of Evaluation	January 26, 2026

[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

It is assumed that the following conditions exist in the TOE operational environment.

A.PHYSICAL_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 only authorized administrator can access.

A.TRUSTED_ADMIN
The authorized administrator of the TOE is non-malicious, has been appropriately trained for the TOE management functions, and accurately fulfills their duties in accordance with administrator guidelines.

A.OPERATION_SYSTEM_REINFORCEMENT
The reliability and security of the operating system shall be ensured by reinforcing the latest vulnerabilities in the operating system on which the TOE is installed and operated.

A.SECURE_DEVELOPMENT
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.

A.AUTHENTICATION_SYSTEM_SECURITY
If TOE receives the support of the external authentication system (RADIUS, TACACS, Kerberos, or other authentication server within the organization) regarding the initial end

user identification and authentication function, the external authentication system shall support the function of storing and managing the authentication information of the authorized end user safely.

A.SECURED_ADMIN_ACCESS
The WEB Server of the TOE operating environment and the WEB Browser of the administrator PC must communicate using a secure path.

A.SECURE_CHANNEL
The TOE must communicate with trusted external IT entities using a secure TLS-based channel.

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

1. Physical Scope of TOE

The physical scope of the TOE consists of the SSO Server, the SSO Agent, an operational user guidance. Verified Cryptographic Module (MPowerCrypto V3.0) is embedded in the TOE components.

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

Category		Identification	Type
TOE		V-FRONT v8	-
TOE Detailed Version		8.1.1.3	-
TOE components	SSO Server	V-FRONT v8 Server 8.1.1.2 (V-FRONTv8_Server_setup-8.1.1.2.x86_64.bin)	Software file (Distributed as a CD)

	SSO Agent	V-FRONT v8 Agent 8.1.1.2 (V-FRONTv8_Agent_setup-8.1.1.2.x86_64.bin)	PDF file (Distributed as a CD)
Documents		V-FRONT v8 Operational User Guidance 1.9 (CCV8-OPE-1.9_EAL1+.pdf)	

[Table 4] Physical scope of the TOE

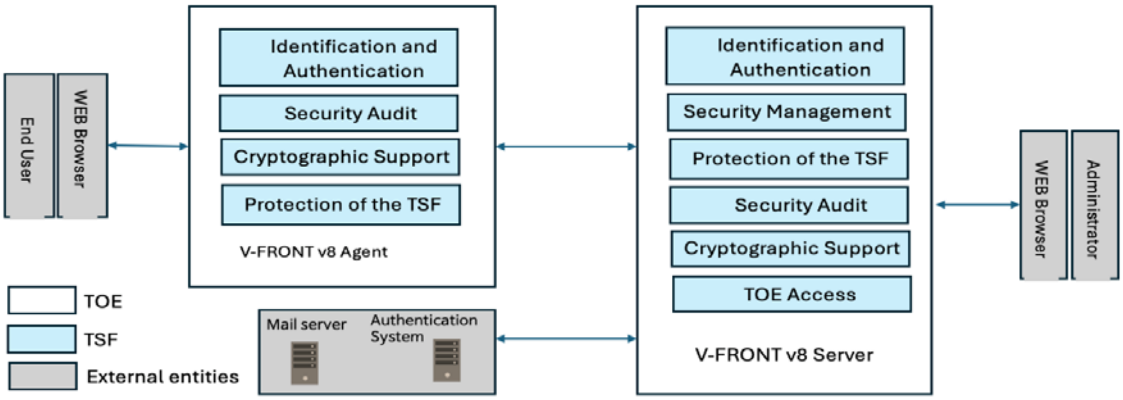
Validated cryptographic modules included the TOE are as follows in [Table 6].

category	content
Cryptographic Module Name	MPowerCrypto V3.0
Verification number	CM-249-2029.6
Verification Grade	VSL1
Developer	UBIMINFO. Co., LTD.
Verification date	June 17, 2024

[Table 5] General Verification Cryptographic Module

2. Logical Scope of TOE

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



[Figure 2] TOE Logical scope

▣ Security Audit

The TOE creates audit records using trusted time information for major audit events and stores them in the DBMS, but does not store information such as authentication passwords or encryption keys.

Provides the ability to detect potential breaches in security-related incidents, and an authorized administrator performs a search function by searching and sorting the operation logs and user authentication logs through the log management environment of the SSO server according to selected search conditions.

When the audit records size reaches the defined capacity (80%), an administrator is notified, and when the capacity is full (90%), some of the older audit records (10%) are deleted to prevent failure in saving new audit records.

▣ Cryptographic support

The encryption key generated by TOE is derived based on a random number generated by a random bit generation algorithm using the validated cryptographic module, and encryption keys that have been used are safely destroyed.

TOE uses the validated cryptographic module to perform cryptographic key management and cryptographic operations to ensure secure operation and integrated authentication.

Additionally, TOE supports encryption related to the storage of important data, issuance, storage, verification, and disposal of authentication tokens, and support encrypted communication (TLSv1.3), and performs encryption key management and encryption operations at this time.

▣ Identification and authentication

End users access the business system through a web browser installed on their PCs, and the business system transmits the ID/PW received from the user to the SSO server through the connected SSO agent (V-FRONT v8 Agent), and the SSO server confirms authentication by an external authentication system. At this time, the transmission connection between the SSO server and the SSO agent performs mutual authentication based on custom protocol.

If the end user authentication is successful, the SSO agent generates an authentication token and sends it to the business system, which then stores this token in the user's browser as a cookie. This authentication token contains an authentication session ID and timestamp to prevent reuse.

Afterwards, when the user accesses another business system, the previously issued token is transmitted, and this business system verifies the validity of the token through the connected SSO agent and SSO server, performs Single Sign-On processing.

If token verification is successful, the business system verifies the user based on the token information and allows access to the service according to the business system permissions. If authentication fails, no reason for failure is provided.

The administrator manages the SSO server by accessing the Admin Portal of the SSO server (V-FRONT v8 Server) with WEB browser.

For administrator authentication, identification and authentication are performed based on ID/Password, and additional identification and authentication are performed based on OTP authentication. Authentication data used for authentication will be rejected when reused, and the password information used during authentication is masked (marked with ●) to prevent exposure, and the reason for failure is not provided.

When the number of failed user authentication attempts reaches the number of failed login attempts set by the authorized administrator (default 5, configurable from 1 to 5), the SSO server locks the account for 10 minutes and then automatically unlocks the account.

When using Password for administrator identification and authentication, The SSO Server checks for compliance with password security regulations.

The authentication token generated upon successful authentication of an end user is generated in a form that can ensure sufficient security through a secure algorithm and is destroyed in an irreversible manner (overwriting three times with a value of 0 in the memory area) after transmitting the generated authentication token or verifying the authentication token.

▣ Security Management

The SSO server (V-FRONT v8 Server) provides policy settings and permission management for service access by administrators and SSO agents (V-FRONT v8 Agent) by allowing access only to authorized administrators through the login function.

The management function supports the ability to add/modify/delete/query security information for administrator identification and authentication.

Security information is maintained through administrator account information, agent information, agent policy information, logs, and system management (authentication system, mail system connection settings, etc.) functions.

Administrators are classified into read-only and read/write administrators based on their administrative privileges. Read-only administrators can only query data, while read/write administrators can perform add/modify/delete functions in addition to query functions.

The SSO server registers the IP address of the PC for management access and blocks access from unregistered IP addresses.

When installing the SSO server, set the administrator password and the account, and ensure that the password complies with password-related security regulations.

The Service Agent Information Management function manages the settings for trust-based connections with the SSO agent installed on the Single Sign-On target service.

The Policy Information Management manages the security functions to add, query, modify, and delete security policies for administrators of the SSO server.

The Report Management provides administrators with audit logs for security audits.

▣ Protection of the TSF

The SSO server and SSO agent use a shared secret key to ensure confidentiality and integrity of internally transmitting TSF data such as general user authentication request information, agent status information, agent configuration management information, and authentication token verification-related information through mutual connection. Furthermore, TSF data is encrypted using DEK when stored or is securely managed in the DBMS. The TOE maintains a secure state in the event of a failure in the random number generator noise source integrity test of the cryptographic module used.

The SSO server and SSO agent each generate a KEK using the PBKDF2 method using the password entered during installation to protect the encryption key (DEK) for encrypting important stored data such as the administrator password and product settings.

The SSO server performs a self-test to ensure the normal operation of the single sign-on feature and the process status upon startup and at the administrator's request, and the SSO agent performs a self-test upon startup and periodically to check the integrity of the relevant executable file and setting values. If an error occurs, SSO Server and SSO Agent perform response actions. Authorized administrators can review the verification details and results by viewing the logs on the management screen.

When the SSO server and SSO agent are started, normal operation and integrity are checked, and if an abnormality is found, the reason for the failure can be checked on the screen.

▣ **TOE access**

The SSO server provides a feature to terminate an authorized administrator session after a specified period of inactivity (10 minutes). Furthermore, to prevent duplicate access to the product using the same user account and permissions, it provides a feature to terminate the first session in the event of a duplicate access. Any administrator accessing the SSO server will have their access sessions restricted based on the set allowed IPs.

6. Documentation

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

Identification	Date
V-FRONT v8 Operational User Guidance 1.9 (CCV8-OPE-1.9_EAL1+.pdf)	January 05, 2026

[Table 6] 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: V-FRONT v8 (8.1.1.3)

- V-FRONT v8 Server 8.1.1.2
- V-FRONT v8 Agent 8.1.1.2

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)).

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 Problem Definition clearly defines the security problems that the TOE and operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.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.

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.

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.

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.

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.

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.

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_SPD.1	ASE_SPD.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		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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 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 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 prvent

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**

V-FRONT v8 Security Target 1.9 [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

Authentication Data
Information used to verify a user's claimed identity

Authentication 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.

Monitoring administrator

As An authorized user who operates and manages the TOE securely, Only the audit log can be viewed among the security management functions

Super Administrator

As an authorized user who operates and manages the TOE securely, it can perform all security management functions

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 following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1

Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-002 Version 1.1, July 2024

[2] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1

Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2024-07-002 Version 1.1, July 2024

[3] Korean National Protection Profile for Single Sign On V3.1, June 27, 2025

[4] V-FRONT v8 Security Target 1.9, January 05, 2026

[5] V-FRONT v8 Independent Testing Report(ATE_IND.1) V1.00, January 23, 2026

[6] V-FRONT v8 Penetration Testing Report (AVA_VAN.1) V1.00, January 23, 2026

[7] V-FRONT v8 Evaluation Technical Report V2.00 Febrary 23, 2026