KECS-CR-24-51

Echelon V4.5

Certification Report

Certification No.: KECS-CISS-1329-2024

2024. 9. 27.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.09.27.	-	Certification report for Echelon V4.5 - First documentation

This document is the certification report for Echelon V4.5 of UbimInfo Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the certification body on the results of the EAL1+ evaluation of Echelon V4.5(“TOE” hereinafter) 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 TOE provides column-level encryption/decryption functions through a plug-in type to protect user data, and the operating environment for operating the TOE is shown in [Figure 1]. The TOE consists of Management tool, Manager, and Agent and the functions provided by each component are as follows.

The Management tool installed on the authorized administrator PC is an administrator access tool that provides the ability for administrators (security manager) to perform security management.

The Manager installed on the management server performs core functions such as security management, encryption key management, audit history management and notification services.

The Agent installed on the database server performs encryption/decryption of user data according to the security policy received from the manager.

An application server and an external entity (NTP server, mail server, etc.) are required for TOE operation. The NTP server is used to reliable time information for the audit data generated by the manager, and the mail server sends emails to the authorized administrator regarding security alert events.

TOE components (Management tool, Manager, Agent) provide encrypted communication based on standard protocols. The contents of the KCMVP (Korea Cryptographic Module Validation Program) cryptographic module, installed in each TOE component and performing encryption/decryption, are as shown in [Table 1].

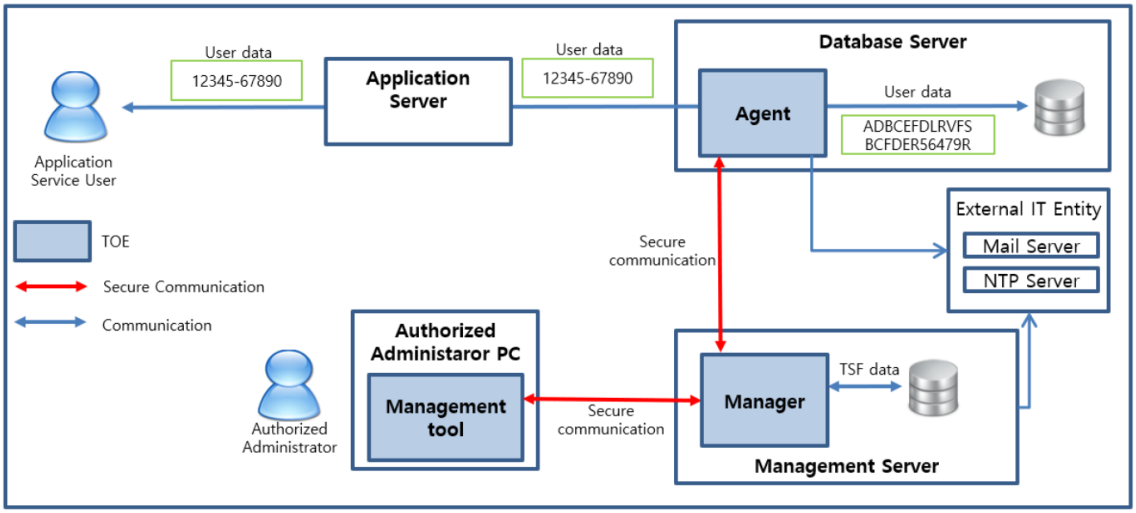
Classification	Contents
cryptographic module name	MPowerCrypto V3.0
Verification number	CM-249-2029.6
verification level	VSL1
developer	UbimInfo Co.,Ltd.
verification date	2024-06-17
expiration date	2029-06-17

[Table 1] KCMVP cryptographic module information

The TOE is used to encrypt the user data according to the security policy set by the authorized administrator to prevent the unauthorized disclosure of the confidential information. In order that the authorized administrator can operate the TOE securely in the operational environment of the organization, the TOE provides various security features such as the security audit function that records and manages major auditable events; cryptographic support function such as cryptographic key management and cryptographic operation; user data protection function that encrypts the user data and protects the residual information; identification and authentication function such as verifying the identity of the authorized administrator, authentication failure handling, and mutual authentication among the TOE components; security management function for security functions and TSF data; TSF protection functions including protecting the TSF data transmitted among the TOE components, protecting the TSF data stored in the storage that is controlled by the TSF, and TSF self-test; and TOE access function to manage the access session of the authorized administrator. The DEK (Data Encryption Key) used to encrypt/decrypt the user data is protected by encryption with the KEK (Key Encryption Key).

The evaluation of the TOE was carried out by the Telecommunications Technology Association (TTA) and completed on September 25, 2024. This report is based on the evaluation technical report (ETR)[6] submitted by TTA and the Security Target (ST) [7][8]. The ST claims strict conformance to the Korean National Protection Profile for Data Encryption V3.0 [3]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3. 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 operational environment of the TOE is shown in [Figure 1] TOE Operational Environment. The operational environment of the TOE includes plug-in type defined in the PP [3].



[Figure 1] Operational environment 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 reference is identified as follows.

TOE	Echelon V4.5
Version	V4.5
Build version	4.5.0.0.2
TOE Components	- Echelon V4.5-AdministratorV1.02 - Echelon V4.5-ManagerV1.02 - Echelon V4.5-AgentV1.02
Guidance Documents	- Echelon V4.5-PRE.1-r1.2.pdf - Echelon V4.5-OPE.1-r1.2.pdf - Echelon V4.5-OPE.2-r1.2.pdf

[Table 2] TOE identification

[Table 3] summarizes additional identification information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Scheme for IT Security (May 17, 2021)[4]
TOE	Echelon V4.5
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+ (augmented by ATE_FUN.1)
Developer	UbimInfo Co., Ltd.
Sponsor	UbimInfo Co., Ltd.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	September 25, 2024
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE provides following security features. For more details refer to the ST [7][8].

TSF	Explanation
Security Audit	The TOE generates audit records of security relevant events such as the start-up/shutdown of the audit functions, integrity violation, self-test failures, and stores them in the DBMS.
Cryptographic Support	The TOE performs cryptographic operation such as encryption/decryption, and cryptographic key management such as key generation/distribution/destruction.
User data protection	The TOE provides encryption / decryption function for each column of Database to protect user data.
Identification and	The TOE provides identification and authentication functions for the administrator based on ID/PW and mutual authentication between

TSF	Explanation
Authentication	TOE components.
Security Management	Only the authorized administrator who can access the management interface provided by TOE can performs security management of the TOE.
Protection of the TSF	The TOE provides secure communications to protect confidentiality and integrity of the transmitted data between TOE components. The TOE protects stored TSF data through encryption and performs self-test of TSF.
TOE Access	When an authorized administrator connects, the TOE verifies whether the IP address is allowed and terminates the session if the inactivity period exceeds a certain time.

[Table 4] Security features

4. Assumptions and Clarification of Scope

There are no explicit Assumptions in the Security Problem Definition in the Low Assurance ST. The followings are procedural method supported from operational environment in order to provide the TOE security functionality accurately.

- The place where the TOE components are installed and operated shall be equipped with access control and protection facilities so that only authorized administrator can access.
- The authorized administrator of the TOE shall be non-malicious users, have appropriately trained for the TOE management functions and accurately fulfill the duties in accordance with administrator guidances.
- 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.
- The authorized administrator of the TOE shall periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup (external log server or separate storage device, etc.) to prevent audit data loss.
- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement on the latest

vulnerabilities of the operating system in which the TOE is installed and operated.

- The TOE shall accurately record security-related events using the reliable timestamp provided by the TOE operating environment.
- The DBMS that interacts with the TOE stores the audit records, so the stored audit records shall be protected from unauthorized deletion and modification.
- Since the mail server linked with the TOE sends a security warning email to the security manager, the channel between the TOE and the mail server shall be safely protected with encrypted communication.

5. Architectural Information

The TOE package consists of a CD 1EA and documents (product license certificate, technical support agreement) and is provided by direct delivery method. The CD consists of TOE installation files (Management tool, Manager, Agent), manuals, and required software. The TOE installation files are provided in the form of software, and preparative procedures necessary for installation, Operation Guide(administrator manual and user operation manual) necessary for operation are provided as PDF files. In addition, essential software (JRE, Eclipse, MPowerPlus) required for TOE installation is included, which is excluded from the scope of the TOE.

The physical scope of the TOE is Management tool, Manager, Agent, Guidance Documents. The major security functions of the TOE and logical scope of the TOE are shown in chapter 3, [Table 4].

For the detailed description, refer to the ST [7][8].

6. Documentation

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

Identifier	Release	Date
Echelon V4.5-PRE.1-r1.2.pdf	V1.2	Sep. 8, 2024
Echelon V4.5-OPE.1-r1.2.pdf	V1.2	Sep. 8, 2024
Echelon V4.5-OPE.2-r1.2.pdf	V1.2	Sep. 8, 2024

[Table 5] 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. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- 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 developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.
The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

8. Evaluated Configuration

The TOE is software consisting of the following components:
TOE: Echelon V4.5(build version 4.5.0.0.2)

- Echelon V4.5-AdministratorV1.02
- Echelon V4.5-ManagerV1.02
- Echelon V4.5-AgentV1.02

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, [Table 5] were evaluated with the TOE

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [6] 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.

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 PP and requirement 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 meets 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 for use as the basis for the TOE evaluation.
The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The Configuration Management Capabilities clearly identifies the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.
The Configuration Management Scope 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.

9.3 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(including warnings) for the secure use of the TOE, addresses secure procedures for all modes of operation except for misleading and unreasonable guidance. 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 Development Evaluation (ADV)

The functional specifications specifies 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.

9.5 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 TSF, 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	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	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 6] 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 authorized administrator should install and operate the TOE and DBMS in a physically secure environment accessible only by the authorized administrator, and should not allow remote management from the outside.
- The authorized administrator is innocuous, properly trained in TOE management functions, and shall perform their duties accurately in accordance with manager guidelines.
- Developers who link the encryption function to the application or DBMS should ensure that the security functions of the TOE are applied safely in accordance with the requirements of the manual.
- The TOE shall accurately record security-related events using reliable timestamps provided by the TOE operating environment.
- It is necessary to maintain the reliability and safety of the operating system by performing reinforcement work on the latest vulnerabilities of the operating system installed and operated by the TOE.
- The authorized administrator shall periodically check the free space of the audit data storage in preparation for the loss of the audit records and perform the backup of the audit records so that the audit records are not deleted.
- Since the mail server linked to the TOE sends security warning mail to the authorized administrator, the channel between them shall be secured by encrypted communication.
- Since DBMS that interact with TOE stores audit records, they shall be protected from unauthorized modification and deletion of the stored audit records.
- During product operation, the authorized administrator must maintain a secure state by periodically changing passwords.
- The authorized administrator must set only the necessary policies and delete unused ones to prevent potential vulnerabilities.

11. Security Target

The Echelon V4.5 Security Target V1.2, September 8, 2024 [7] is included in this report by reference. For the purpose of publication, it is provided as sanitised version [8] according to the CCRA supporting document ST sanitising for publication [9].

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
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

13. Bibliography

The evaluation facility has used 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 Database Encryption V3.0, KECS-PP-1232-2023, April 27, 2023

[4] Korea Evaluation and Certification Guidelines for IT Security, October 31, 2022

[5] Korea Evaluation and Certification Scheme for IT Security, May 17, 2021

[6] TTA-CCE-23-006 Echelon V4.5 Evaluation Technical Report V1.1, September 25, 2024

[7] Echelon V4.5 Security Target V1.2, September 8, 2024
[8] Echelon V4.5 Security Target Lite r1.0, September 8, 2024
[9] ST sanitising for publication, CCDB-2006-04-004, April 2006