KECS-CR-23-12

Echelon V3.5

Certification Report

Certification No.: KECS-CISS-1218-2023

2023. 3. 17.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.03.17.	-	Certification report for Echelon V3.5 - First documentation

This document is the certification report for Echelon V3.5 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 certification result drawn by the certification body on the results of the EAL1+ evaluation of Echelon V3.5(“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.

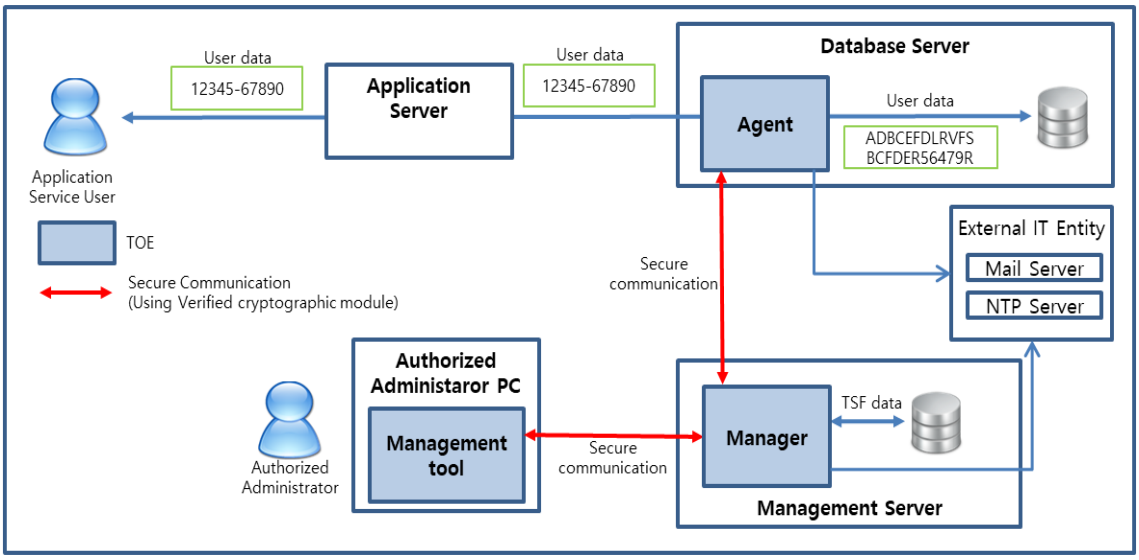
The TOE is database encryption software to prevent the unauthorized disclosure of confidential information by encrypting the database.

The TOE consists of management tool, manager, and agent. The management tool is an administrator access tool that provides the ability for administrators (security manager) to perform security management and encryption key management (encryption key generation/destruction/inquiry function), and to view audit history.
The manager installed on the Echelon 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 encrypts and decrypts user data according to the security policy sent from the manager. The TOE includes cryptographic module (MPowerCrypto V2.5) validated under the Korea Cryptographic Module Validation Program (KCMVP).

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on March 17, 2023. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6].

The ST claims strict conformance to the Korean National Protection Profile for Data Encryption V1.1 [7]. 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.

[Figure 1] shows the operational environment of the TOE, which is the plug-in type as defined in the PP[7].



[Figure 1] Operational environment of the TOE

[Table 1] shows minimum hardware and software requirements necessary for installation and operation of the TOE.

Category		Contents
Management tool	CPU	Intel Core i3 @ 3.40GHz or higher
	RAM	8 GB or higher
	HDD	1 GB or higher space for installation of TOE
	NIC	Ethernet 10/100/1000 Mbps x 1 Port or more
	OS	Windows 10 Pro(64bit)
	Required S/W	Eclipse RCP 4.19.0 JRE 11.0.16
Manager	CPU	Intel Core i3 @ 3.40GHz or higher
	RAM	8 GB or higher
	HDD	1 GB or higher space for installation of TOE
	NIC	Ethernet 10/100/1000 Mbps x 1 Port or more
	OS	Ubuntu 18.04.6 (64bit) (Kernel:4.15.0-204)
	Required S/W	PostgreSQL 14.7 MPowerPlus 1.3.1 JRE 11.0.16
Agent	CPU	Intel Core i3 @ 3.40GHz or higher

	RAM	8 GB or higher
	HDD	1GB or higher space for installation of TOE
	NIC	Ethernet 10/100/1000 Mbps x 1 Port or more
	OS	Oracle linux 8.7 (64bit) (Kernel:4.18.0-425)
	Required S/W	Oracle 19.3.0.0.0 MPowerPlus 1.3.1 JRE 11.0.16

[Table 1] Hardware and software requirements for 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 is software consisting of the following software components and related guidance documents.

TOE	Echelon V3.5	
Version	V3.5	
Detail version	3.5.0.0.3	
TOE Components	Management tool	Echelon V3.5-AdministratorV1.04 - Echelon V3.5@AdministratorV1.04.msi
	Manager	Echelon V3.5-ManagerV1.04 - Echelon V3.5@ManagerV1.04.jar
	Agent	Echelon V3.5-AgentV1.04 - Echelon V3.5@AgentV1.04.jar
Guidance Document	- Echelon V3.5-PRE.1-r1.1.pdf - Echelon V3.5-OPE.1-r1.1.pdf - Echelon V3.5-OPE.2-r1.0.pdf	

[Table 2] TOE identification

Note that the TOE is delivered contained in a CD-ROM.

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022)[3] Korea Evaluation and Certification Scheme for IT Security (May 17, 2021)[4]
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
Protection Profile	Korean National Protection Profile for Database Encryption V1.1, KECS-PP-0820a-2017, 11 December 2019
Developer	UbimInfo Co., Ltd.

Sponsor	UbimInfo Co., Ltd.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date of Evaluation	March 17, 2023
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The ST [6] for the TOE claims strict conformance to Korean National Protection Profile for Database Encryption V1.1 [7], and complies security policies defined in the PP [7] by security requirements. The TOE provides security features defined in the PP [7] as follows:

- Security audit: The TOE generates audit records of security relevant events including the start-up/shutdown of the audit functions, integrity violation and self-test failures, and stores them in the DBMS.
- Cryptographic support: The TOE performs cryptographic operation such as encryption/decryption and hash, and cryptographic key management such as key generation/distribution/destruction using cryptographic module (MPowerCrypto V2.5) validated under the KCMVP.
- User data protection: The TOE provides encryption and decryption for the user data in a column of a database.
- Identification and authentication: The TOE identifies and authenticates the administrators(Security Manager) based on ID/PW. The TOE also mutually authenticates TOE components when they communicate each other.
- Security management: Security management of the TOE is restricted to only the authorized administrator who can access the management interface provided by TOE.
- Protection of the TSF: The TOE provides secure communications between TOE components to protect the transmitted data. The TOE encrypts the stored TSF data to protect them from unauthorized exposure and modification. The TOE performs self-tests on the TOE components, which includes the self-test on the validated cryptographic module.

- TOE access: The TOE manages authorized administrators' sessions based on access IP addresses. The TOE terminates the sessions after predefined time interval of inactivity.

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.
- Since the DBMS interacting with the TOE stores the audit records, it must be protected from unauthorized deletion and modification of the stored audit records.

5. Architectural Information

The physical scope of TOE is Management tool, Manager, and Agent, and those are inside CD. The major security policy of the TOE and logical scope of the TOE are shown in [Figure 1] and chapter 3. For the detailed description, refer to the ST [6].

6. Documentation

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

Identifier	Release	Date
Echelon V3.5-PRE.1-r1.1.pdf	V1.1	Jan. 8, 2023
Echelon V3.5-OPE.1-r1.1.pdf	V1.1	Feb. 8, 2023
Echelon V3.5-OPE.2-r1.0.pdf	V1.0	Dec. 3, 2022

[Table 4] 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.: 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 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 [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:
TOE: Echelon V3.5(version 3.5.0.0.3)

- Echelon V3.5-AdministratorV1.04
- Echelon V3.5-ManagerV1.04
- Echelon V3.5-AgentV1.04

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 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [5] 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 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 Life Cycle Support Evaluation (ALC)

The developer has uniquely 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.

9.3 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 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.

9.5 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_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.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		
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 5] 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 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.
- Developers who link the encryption function to DBMS should ensure that the security functions of the TOE are applied safely in accordance with the requirements of the manual.
- When operating the product, the administrator's password should be changed periodically.
- 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.
- After installing the product, the administrator must register the administrator's e-mail address on the product so that warning mail can be sent normally in the event of a potential security violation, and ensure that the e-mail address is correctly registered and functional.
- The policy manager should manage the PC so that only the authorized policy manager can access the system to prevent modification and deletion of the audit log from unauthorized users.

11. Security Target

The Echelon V3.5 Security Target V1.2, February 1, 2023 [6] is included in this report by reference.

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

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
Self-test	Pre-operational or conditional test executed by the cryptographic module
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority

13. Bibliography

The certification body 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
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

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

[3] Korea Evaluation and Certification Guidelines for IT Security (24 August 2017)

[4] Korea Evaluation and Certification Scheme for IT Security (17 May 2021)

[5] TTA-CCE-21-010 Echelon V3.5 Evaluation Technical Report V1.3, March 17, 2023

[6] Echelon V3.5 Security Target V1.2, February 1, 2023

[7] Korean National Protection Profile for Database Encryption V1.1 (KECS-PP-0820a-2017, 11 December 2019)