KECS-CR-20-17

Petra Cipher V3.2

Certification Report

Certification No.: KECS-CISS-1003-2020

2020. 4. 2.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2020.04.02.	-	Certification report for Petra Cipher V3.2 - First documentation

This document is the certification report for Petra Cipher V3.2 of SINSIWAY 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 Petra Cipher V3.2 developed by SINSIWAY 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.

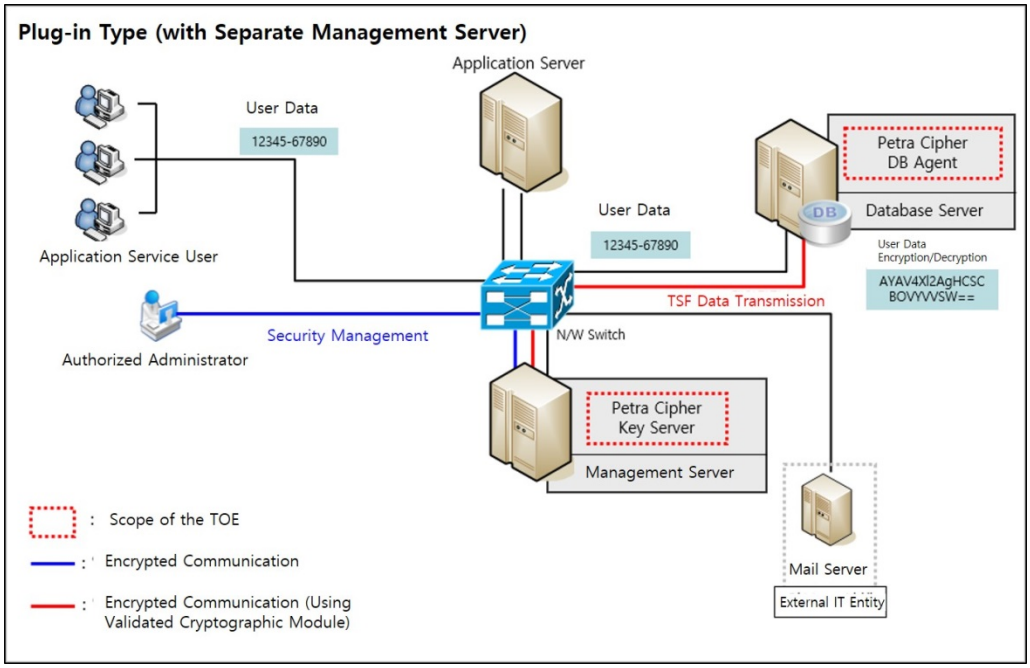
The Target of Evaluation (“TOE” hereinafter) is database encryption software to prevent unauthorized exposure of the information from DBMS. Also, the TOE shall provide a variety of security features: security audit, cryptographic operation using cryptographic module, the user identification and authentication 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 March 11, 2020.

The ST claims conformance to the Korean National Protection Profile for Database Encrytion 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 is comprised of the Petra Cipher Key Server, Petra Cipher DB Agent and Petra Cipher API Agent and can be installed 'Plug-in' and 'API' type. [Figure 1], [Figuer 2] shows the operational environment of the TOE.

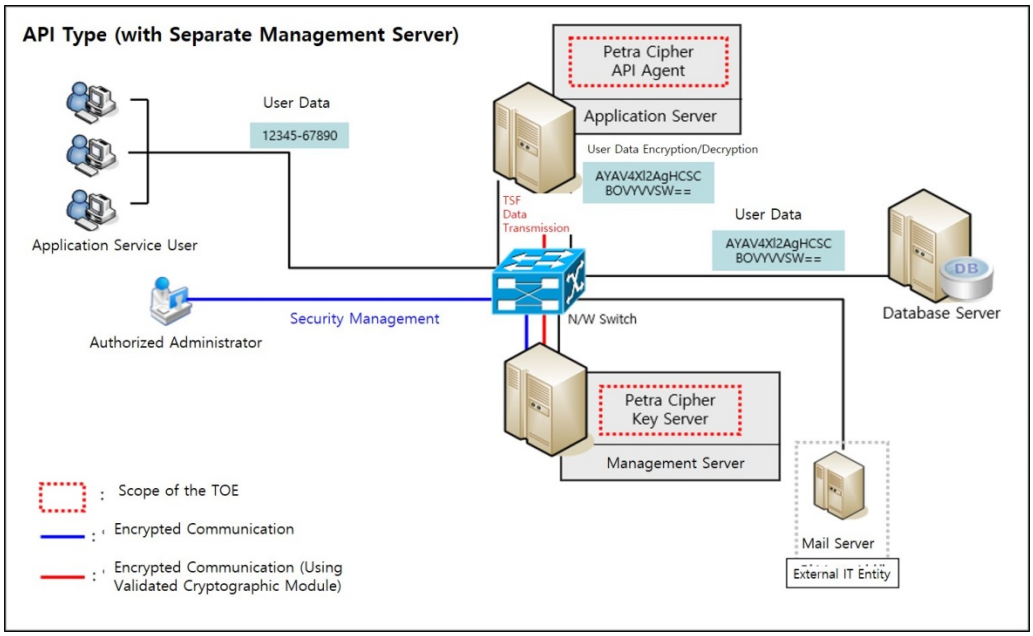
[Figure 1] shows a typical operational environment of the plug-in type. The plug-in operational environment is composed of the Management Server and DB Agent. First, the Management Server manages the information on policies established by the authorized administrator and manages the keys and the audit records. It also encrypts the information on a distributed key and loads it on the shared memory. Second, the DB Agent is installed inside the Database Server where the DB under the protection is located, and encrypts the user data received from the Application Server before they are stored in the DB. In addition, it decrypts the encrypted user data to be transmitted from the Database Server to the Application Server.



[Figure 1] Plug-in type operational environment of the TOE
(Agent, management server separate type)

The application service user requests the encryption or decryption of the user data through the Application Server in accordance with the scope of the encryption as required by the security policy. The requested data are encrypted by the DB Agent and stored in the DB. The authorized administrator accesses the Management Server to perform the security management of the encrypted data stored in the DB.

[Figure 2] shows the API type operational environment. The API type consists of the API Agent and the Management Server. The API Agent is installed and operated outside the DB under the protection, and performs the encryption and decryption of the important data in accordance with the policy established by the administrator. The authorized administrator can access the Management Server and perform the security management. The TOE components may be subject to change depending on the roles including the encryption and decryption of the important information, security management and cryptographic key management.



[Figure 2] API-type operational environment of the TOE
(API module, management server separate type)

The application service user performs the encryption and decryption of the user data through the API Agent on the Application Server in accordance with the scope of the encryption as required by the security policy. The authorized administrator accesses the Management Server to perform the security management of the encrypted data stored in the DB.

The cryptographic algorithm subject to the validation in the validated cryptographic module is used for the communication between the TOE components for the purpose of secure communication. In case the administrator accesses the Management Server through a web browser, a secure path (TLS V1.2) is generated to carry out the communication.

As other external entities necessary for the operation of the TOE, there is email server to send alerts by email to the authorized administrator.

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

Component			Requirement
Petra Cipher Key Server	HW	CPU	Intel(R) Core (TM) i5-4250U CPU @ 1.30GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE 5 GB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	CentOS 6.10 (Kernel 2.6.32) 64 bit
		etc	apache tomcat 8.5.51 openJDK 13.0.2
Petra Cipher DB Agent	HW	CPU	Intel(R) Core (TM) i5-4250U CPU @ 1.30GHz or higher
		Memory	4 GB or higher

		HDD	Space required for installation of TOE 1 GB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	CentOS 6.10 (Kernel 2.6.32) 64 bit
		DBMS	Oracle 11g: 11.2.0.1.0 (DB to be Protected)
Petra Cipher API Agent	HW	CPU	Intel(R) Core (TM) i5-4250U CPU @ 1.30GHz or higher
		Memory	4 GB or higher
		HDD	Space required for installation of TOE 1 GB or higher
		NIC	100/1000 Mbps Ethernet Port 1 unit or higher
	SW	OS	CentOS 6.10 (Kernel 2.6.32) 64 bit
		etc	openJDK 13.0.2

[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]

Component		Requirement
HW	CPU	Intel(R) Core(TM) i5-4250U CPU @ 1.30GHz or higher
	Memory	4 GB or higher

	HDD	50 GB or higher
	NIC	100/1000 Ethernet Port 1 unit or more
SW	OS	Windows 10 Pro 64 bit
	Web Browser	Chrome 80

[Table 2] Administrator PC Requirements

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		Petra Cipher V3.2
Version		r234
TOE Components	**Petra Cipher Key Server**	Petra Cipher Key Server r234
	Petra Cipher DB Agent	Petra Cipher DB Agent r234
	Petra Cipher API Agent	Petra Cipher API Agent r234
Manuals		Petra Cipher V3.2-OPE(Operational Guidance)-V1.2 Petra Cipher V3.2-PRE(Preparative Procedure)-V1.2 Petra Cipher V3.2-API(Developer Guide)-V1.0

[Table 3] TOE identification

[Table 4] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (September 12, 2017)
TOE	Petra Cipher V3.2
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	Korean National Protection Profile for Database Encryption V1.1
Developer	SINSYWAY Co., LTD.
Sponsor	SINSYWAY Co., LTD.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	March 11, 2020

[Table 4] Additional identification information

3. Security Policy

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

- Security Audit
- Cryptographic Support
- User data protection
- Identification and Authentication
- Security Management
- Prtoection 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 3])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the Petra Cipher Key Server, Petra Cipher DB Agent, Petra Cipher API Agent and manuals(preparative procedure, operation guide, developer guide). Verified Cryptographic Module(KLIB V2.2) is embedded in the TOE components. Hardware, operating system, DBMS, WAS, JDK which are operating environments of the TOE are excluded from the physical scope of the TOE.

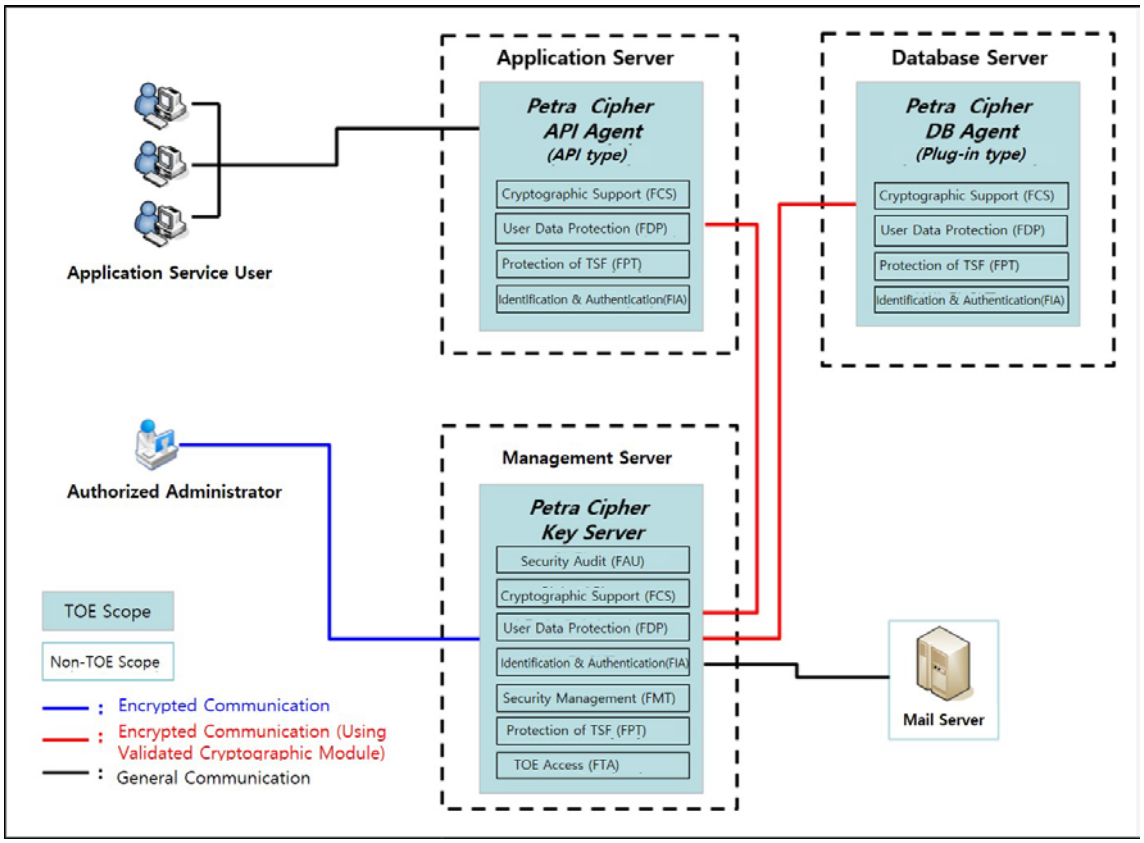
Category		Identification	Type
TOE component	Petra Cipher Key Server	Petra Cipher Key Server r234 (installer-Petra_Cipher_V3.2-r234-linux-64bit.tar.gz)	Software (Distributed as a CD)
	Petra Cipher DB Agent	Petra Cipher DB Agent r234 (dbagent-Petra_Cipher_V3.2-r234-linux-64bit.tar.gz)	
	Petra Cipher API Agent	Petra Cipher API Agent r234 (apiagent-Petra_Cipher_V3.2-r234-linux-64bit.tar.gz)	
Manual		Petra Cipher V3.2-OPE(Operational Guidance)-V1.2 (Petra Cipher V3.2-OPE(Operational Guideline)-V1.2.pdf)	PDF Document (Distributed as a CD)
		Petra Cipher V3.2-PRE(Preparative Procedure)-V1.2 (Petra Cipher V3.2-PRE(Preparative Procedure)-	

	V1.2.pdf)	
	Petra Cipher V3.2-API(Developer Guide)-V1.0 (Petra Cipher V3.2-API(Developer Guide)-V1.0.pdf)	

[Table 5] Physical scope of TOE

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 3] TOE Logical scope

▣ Security Audit (FAU)

Audit data of the TOE stores, as data, the date and time of an event, the type of an event, subject identity, an outcome and content of an event and so forth, which are stored and managed on the Management Server. Only the authorized administrator can view the generated audit data on the Management Server via a web browser. An alarm email is sent in case of any access by an unauthorized user.

Furthermore, results of self-tests carried out in each component of the TOE are stored

and managed on the Management Server. If a self-test fails, an alarm is sent to an email set by the authorized administrator.

In case the audit data storage reaches the initial threshold established by the administrator when audit data are stored on the Management Server, an alarm is sent to the administrator email. If it reaches the threshold for audit data overwriting, an alarm is sent to the administrator email and the oldest audit data are overwritten to trail the latest audit data. The audit records stored in the audit trail are protected by preventing an unauthorized deletion of the stored audit data.

▣ Cryptographic support (FCS)

The TOE generates and destroys all cryptographic keys used for the operation of the product in a secure manner through the validated cryptographic module whose safety and suitability for the implementation have been confirmed by the cryptographic module validation scheme, and performs cryptographic operations in accordance with the cryptographic policy that defines the cryptographic algorithm. In addition, it generates and exchanges cryptographic keys through the validated cryptographic module for secure communication between the TOE components that are physically separated.

The TOE is generate the cryptographic key is generated, a cryptographic key is generated using a random bit through a random bit generator (HASH_DRBG 256) of the validated cryptographic module, and to encrypt user data of the DBMS to be protected is encrypted, a symmetric key encryption algorithm (ARIA-CBC/OFB/CFB 128 bit, ARIA-CBC/OFB 192 bit, ARIA-CBC/OFB 256 bit, SEED-CBC/OFB/CFB 128 bit) and hash algorithm(SHA-256/384/512). In addition, a symmetric key encryption algorittm (ARIA-CBC 128 bit, SEED-CBC 128 bit), digital signature algorittm (RSA-PSS 2048 bit), hash algorithm (SHA-256) and MAC algorithm(HMAC-SHA 256, 1024 bit) are used for protction of TSF data.

Cryptograchic key distribution between the TOE components is safely distributed through public key encryption method (RSAES 2048 bit), and the cryptographic key is overwritten with "0x00" for destruction.

▣ User data protection (FDP)

When user data are stored or modified in the DB within the scope of the encryption, the

TOE encrypts/decrypts the user data by using the validated cryptographic module KLIB V2.2 according to the user data encryption/decryption policies established by the authorized administrator.

In case of the plug-in type, Petra Cipher DB Agent performs the user data encryption/decryption at the column level. In case of the API type, Petra Cipher API Agent installed on the Application Server encrypts/decrypts user data.

The TOE generates different encryption values for the same user data each time it performs the encryption.

When the encryption/decryption is complete, the TOE carries out the initialization so that the previous original user data value cannot be recovered. A policy is in place to keep an unauthorized user from decrypting the information that has been encrypted and stored (in case of data generated with a SHA algorithm, however, the algorithm itself does not support the decryption).

▣ Identification and authentication (FIA)

The TOE provides the identification and authentication function for an administrator in charge of the security management. Upon the initial login after the product is installed, the administrator shall change the ID and password. When data are entered to identify and authenticate the administrator, the password entered is masked with "●" to protect the authentication feedback.

In addition, in case of failed authentication, feedback on the reason for failure is not provided. If authentication attempts fail consecutively (five times), the account is locked (for five minutes).

The TOE also prevents the reuse of authentication data of the administrator logging in to the TOE.

The TOE performs mutual authentication through the protocol developed by SINSIWAY Co., Ltd. for the purpose of the secure communication among the TOE components.

▣ Security Management (FMT)

The TOE has only one administrator account, changing the ID and password when the authorized administrator accesses for the first time.

The TOE provides the function of security policy management to monitor access to the DB and to respond to violations, and the function of security management to manage user data encryption/decryption, administrator information, and configuration. The authorized administrator performs the security management through the security management interface.

▣ Protection of the TSF (FPT)

Ensuring confidentiality and integrity of TSF data transmitted between physically separated TOE components through encrypted communication, and to maintain the secure state of the TOE and to ensure that the security functions operate normally, at startup and during regular operation. Perform self tests to check the status of the process and perform integrity checks on TSF data and TSF executable code that are subject to integrity checks.

The TOE performs self-test at initial start-up, and the self-test is automatically performed at each TOE periodically (1 minute). In addition, an authorized administrator accesses the security management screen through a web browser and provides a function for performing a self test manually.

▣ TOE access (FTA)

The TOE restricts the administrator's management access sessions whose access is allowed to perform the security management function to one. If a session of the administrator who has logged in to the Management Server already exists, no further access by the authorized administrator is allowed.

If the authorized administrator logs in to the Management Server via a web browser and then remains inactive for a specified period of time (default value: 10 minutes), the session that accessed the Management Server is terminated.

Furthermore, the number of authorized administrator IPs is limited to two, and one administrator IP allowed for access is designated in advance in the process of the initial installation of the Management Server.

6. Documentation

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

Identification	Date
Petra Cipher V3.2-PRE(Preparative Procedure)-V1.2 (Petra Cipher V3.2-PRE(Preparative Procedure)-V1.2.pdf)	February 12, 2020
Petra Cipher V3.2-OPE(Operational Guidance)-V1.2 (Petra Cipher V3.2-OPE(Operational Guideline)-V1.2.pdf)	February 12, 2020
Petra Cipher V3.2-API(Developer Guide)-V1.0 (Petra Cipher V3.2-API(Developer Guide)-V1.0.pdf)	November 26, 2019

[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. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules 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: Petra Cipher V3.2 (r234)
- Petra Cipher Key Server r234
- Petra Cipher DB Agent r234
- Petra Cipher API Agent r234

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 result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation. (EAL1+).

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.

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 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.

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		
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 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 checks 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

Petra Cipher V3.2-ASE(Security Target)-V1.4 [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 Server
The application server defined in this PP refers to the server that installs and operates the application, which is developed to provide a certain application service by the organization that operates the TOE. The pertinent application reads the user data from the DB, which is located in the database server, by the request of the application service user, or sends the user data to be stored in the DB to the database server.

Column
A set of data values of a particular simple type, one for each row of the table in a relational database

Database
A set of data that is compiled according to a certain structure in order to receive, save, and provide data in response to the demand of multiple users to support multiple application duties at the same time. The database related to encryption by column, which is required by this PP, refers to the relational database.

Database Server
The database server defined in this PP refer to the server in which the DBMS managing the protected DB is installed in the organization that operates the TOE

DBMS (Database Management System)
A software system composed to configure and apply the database. The DBMS related to encryption by column, which is required by this PP, refers to the database management system based on the relational database model.

Data Encryption Key (DEK)
Key that encrypts and decrypts the data

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

Encryption

The act that converts the plaintext into the ciphertext using the encryption key

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Management access

The access to the TOE by using the HTTPS, SSH, TLS, etc to manage the TOE by administrator, remotely

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic

and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Secret Key

A cryptographic key which is used in an symmetric cryptographic algorithm and is uniquely associated with one or several entity, not to be disclosed

Master Key

It refers to the Key Encryption Key (KEK) used in Petra Cipher V3.2.

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 V1.1, December 11, 2019

[4] Petra Cipher V3.2-ASE(Security Target)-V1.4, March 24, 2020

[5] Petra Cipher V3.2 Independent Testing Report(ATE_IND.1) V1.00, March 10, 2020

[6] Petra Cipher V3.2 Penetration Testing Report (AVA_VAN.1) V1.00, February 14, 2020