KECS-CR-24-15

Document SAFER Blue 3
Certification Report

Certification No.: KECS-CISS-1293-2024

2024. 2. 26.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.02.26.	-	Certification report for Document SAFER Blue 3 - First documentation

This document is the certification report for Document SAFER Blue 3 of

MarkAny Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Contents

1. Executive Summary

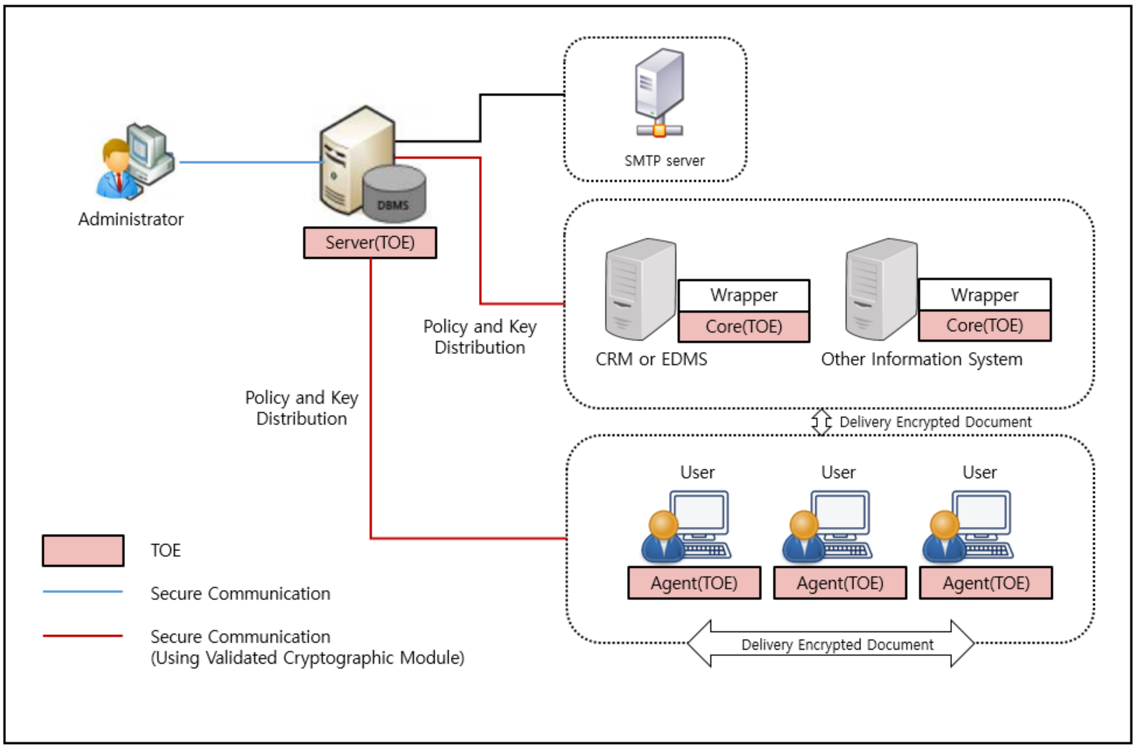
This report describes the certification result drawn by the certification body on the results of the EAL1+ evaluation of the Document SAFER Blue 3 (“TOE” hereinafter) with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (hereinafter referred to as “TOE”) is Electronic Document Encryption designed to protect important documents managed by the organization based on the encryption/decryption. Also, the TOE provides 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 February 20, 2024. This report grounds on the Evaluation Technical Report[7] had submitted and the Security Target(ST)[4].

The ST claims conformance to the Korean National Protection Profile for Electronic Document Encryption 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+. 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. The TOE is composed of the Document SAFER Blue 3 Server(“Server(TOE)” hereinafter) which manages the security policy and cryptographic key, the Document SAFER Blue 3 Agent(“Agent”(TOE) hereinafter) that performs Electronic Document encryption/decryption installed in the user PC, and the Document SAFER Blue 3 Core(“Core”(TOE) hereinafter) that performs Electronic Document encryption installed in the information system in the form of API module. A wrapper is used for compatibility between the Core and various information systems, but it is outside of the TOE scope.



[Figure 1] Operational Environment of the TOE

The requirements for hardware, software and operating system to install the TOE are shown in **오류! 참조 원본을 찾을 수 없습니다.**].

Component		Requirement	
Server	HW	CPU: Intel(R) 2.45 GHz or higher RAM: 8 GB or higher HDD: 1 TB or higher for the installation of TOE NIC: 100/1000 Ethernet Card 1 Port or higher	
	OS	Windows Server 2022 Standard (64 bit)	Ubuntu 22.04 (5.15.0-53-generic) 64 bit
	SW	OpenJDK 1.8.0_392 Apache Tomcat 9.0.85 Oracle 19c (19.3.0.0.0)	OpenJDK 1.8.0_392 Apache Tomcat 9.0.85 Mariadb 11.0.4
Agent	HW	CPU: Intel Core 2.50 GHz or higher RAM: 4 GB or higher HDD: 500 GB or higher for the installation of TOE NIC: 100/1000 Ethernet Card 1 Port or higher	

	OS	Windows 10 pro (64 bit) Windows 11 pro (64 bit)
Core	HW	CPU: Intel(R) 2 GHz or higher RAM: 8 GB or higher HDD: 500 GB or higher for the installation of TOE NIC: 100/1000 Ethernet Card 1 Port or higher
	OS	Ubuntu 22.04 (5.15.0-53-generic) 64 bit
	SW	OpenJDK 1.8.0_392

[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 **오류! 참조 원본을 찾을 수 없습니다.**]

Component	Requirement
S/W	Chrome 120.0.6099.217

[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 is reference is identified as follows.

TOE	Document SAFER Blue 3	
Version	3.0.02	
TOE Components	Server	− Document SAFER Blue 3 Server 3.0.02 (Document_SAFER_Blue_3_Server_3.0.02.sh) (Document_SAFER_Blue_3_Server_3.0.02.exe)
	Agent	− Document SAFER Blue 3 Agent 3.0.02 (Document_SAFER_Blue_3_Agent_3.0.02.exe)
	Core	− Document SAFER Blue 3 Core 3.0.02 (Document_SAFER_Blue_3_Core_3.0.02.sh)
Guidance Document	Document SAFER Blue 3 Operation Guide V1.02 (Document SAFER Blue 3 Operation Guide V1.02.pdf)	
	Document SAFER Blue 3 Preparative Procedure V1.02 (Document SAFER Blue 3 Preparative Procedure V1.02.pdf)	

[Table 3] TOE identification

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

[Table 4] summarizes additional 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 Regulation for IT Security (May 17, 2021)
TOE	Document SAFER Blue 3
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 Electronic Document Encryption V1.1

Developer	MarkAny Inc.
Sponsor	MarkAny Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	February 20, 2024
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The ST [4] for the TOE claims strict conformance to Korean National Protection Profile for Database Encryption V1.1 [3], and complies security policies defined in the PP [3] by security requirements. The TOE provides security features defined in the PP [3] as follows:

- 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 hash, and cryptographic key management such as key generation/distribution/destruction using cryptographic module (MACRYPTO V3.00) validated under the KCMVP.
- User data protection: The TOE provides user' documents by making them Secured Documents by means of encrypting them and controlling access to them in accordance to the access control policy per user set by the administrator.
- Identification and authentication: The TOE identifies and authenticates the administrators and document users based on ID/PW.
- Security management: The TOE provides functions such as TOE security function management, security attribute management and TSF data management to the authorized administrator.
- 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' access to itself by termination interactive sessions after defined time interval of inactivity.

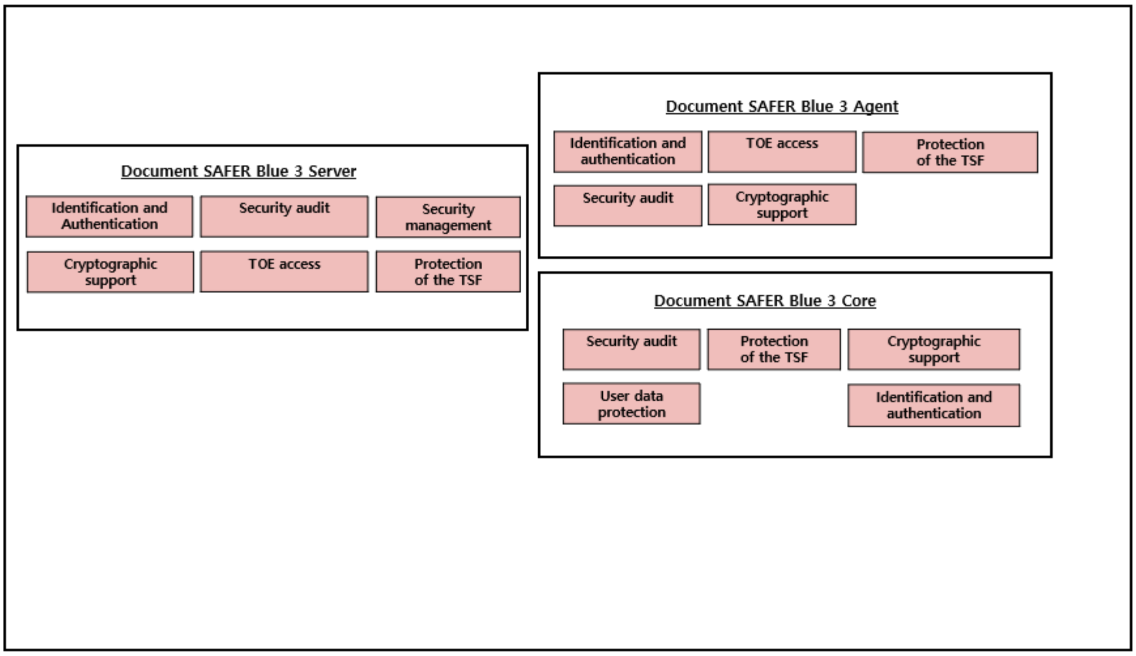
4. Assumptions and Clarification of Scope

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 guidance.
- 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.

5. Architectural Information

The physical scope of the TOE consists of the Server(TOE), Agent(TOE), Core(TOE), and guidance documents. The following security functions are provided by the TOE logical scope and boundary of TOE is shown in [Figure 2].



[Figure 3] TOE Logical Scope

The TOE is composed of the Server(TOE), Agent(TOE), Core(TOE and should be installed and operated inside the internal network of the protected organization.
The Server(TOE) manages policy and security data for document encryption/decryption and provides the function to apply to the Agent(TOE). The Agent(TOE) controls the permissions of secured documents according to the policy and performs document encryption/decryption. The Core(TOE) interacts with information system and encryption/decryption document according to the policy. The TOE also includes the MACRYPTO V3.00 validated by KCMVP(Korea Cryptographic Module Validation Program) to perform Electronic Document encryption/decryption.

6. Documentation

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

Identification	Date
Document SAFER Blue 3 Operation Guide V1.02	January 15, 2024

(Document SAFER Blue 3 Operation Guide V1.02.pdf)	
Document SAFER Blue 3 Preparative Procedure V1.02 (Document SAFER Blue 3 Preparative Procedure V1.02.pdf)	January 15, 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.: 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 [7].

8. Evaluated Configuration

The TOE is software consisting of the following components:
TOE: Document SAFER Blue 3 (3.0.02)

- Document SAFER Blue 3 Server 3.0.02
- Document SAFER Blue 3 Agent 3.0.02
- Document SAFER Blue 3 Core 3.0.02

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 [7] 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+).
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 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.

9.5 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.

9.6 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	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
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		
	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 periodically check the free space of the audit data storage in preparation for the loss of the audit records, and perform backups of the audit records so that the audit records are not exhausted.
- The Server(TOE) must be installed and operated in a physically secure environment that is accessible only to authorized administrators and should not allow remote administration from outside.
- If a cryptographic key is lost due to administrator's wrong cryptographic key

management, document users may not be able to decrypt the encrypted file stored on the user's PC, so administrator has to be careful with cryptographic key management.

- If the TOE is operated in a ‘Information system encryption’ type defined in the PP [3], it is recommended that those who are good at using the API.

11. Security Target

Document SAFER Blue 3 Security Target V1.02 [4] is included in this report for 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
Authorized Document User	The TOE user who may, in accordance with the SFRs, perform an operation.
Authorized Administrator	Authorized user to securely operate and manage the TOE
Data Encryption Key (DEK)	Key that encrypts the data
External Entity	An entity (person or IT object) that interact (or can interact) with the TOE from outside the TOE.

Key Encryption Key (KEK)	Key that encrypts another cryptographic key.
Validated Cryptographic Module	A cryptographic module that is validated and given a validation number by validation authority
Wrapper	Interface to connect the TOE with various types of information system

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

[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 Electronic Document Encryption V1.1, December 11, 2019

[4] Document SAFER Blue 3 Security Target V1.02, January 15, 2024

[5] Document SAFER Blue 3 Independent Testing Report(ATE_IND.1) V1.00, February 20, 2024

[6] Document SAFER Blue 3 Penetration Testing Report (AVA_VAN.1) V1.00, February 19, 2024

[7] Document SAFER Blue 3 Evaluation Technical Report Lite V1.00, February 20,2024