FilingBox MEGA2 v2
Certification Report

Certification No.: KECS-CISS-1298-2024

2024. 3. 28.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.03.28.	-	Certification report for FilingBox MEGA2 v2 - First documentation

This document is the certification report for FilingBox MEGA2 v2 of Namusoft Co., Ltd.

<u>The Certification Body</u>

<u>IT Security Certification Center</u>

<u>The Evaluation Facility</u>

<u>Korea System Assurance (KOSYAS)</u>

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the evaluation of FilingBox MEGA2 v2 of Namusoft 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) is an information security software that allows only authorized applications to access files within the storage protected by the TOE. The TOE is provided as software and provides the following security features: security audit, cryptographic operations using OpenSSL, user data protection, identification and authentication, security management, TSF protection function, and TOE access.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on 26 March 2024. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [5] and the Security Target (ST) [6].

The ST has no conformance claim to the protection profile (PP). 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 (EAL) 1. 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 newly defined components in the Extended Component Definition chapter of 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 consists of the following software components: FilingBox MEGA2 v2 Server, FilingBox MEGA2 v2 Windows Client, and FilingBox MEGA2 v2 Linux Client. The component FilingBox MEGA2 v2 Server provides security management features for administrators (the super and general administrators) through web UI. The components FilingBox MEGA2 v2 Windows Client and FilingBox MEGA2 v2 Linux Client provide device administrators to configure the security attributes of the objects (application softwares) to access to the files in the storage protected by the TOE.
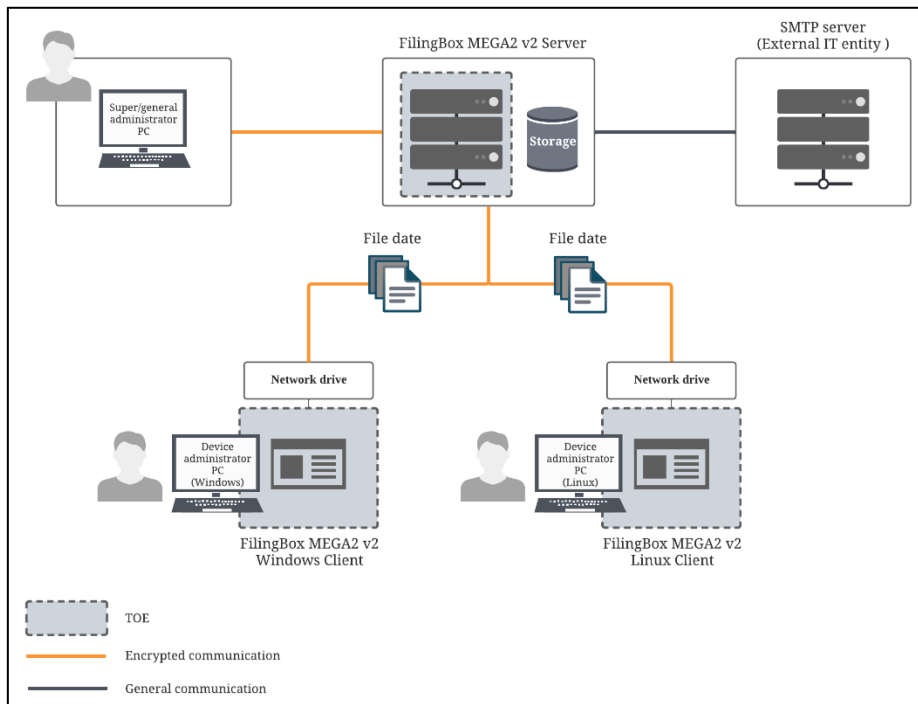
[Figure 1] Operational environment of the TOE

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

Category		Contents
FilingBox MEGA2 v2 Server	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or above
	RAM	16 GB or higher
	SSD	At least 10 GB of space required for the TOE installation
	NIC	100/1000 Mbps X 1 Port or more
	OS	Rocky Linux 8.8 64-bit (Kernel 4.18.0-477.10.1)
	S/W	MariaDB 10.11.5 Tomcat 9.0.85 OpenJDK 1.8.0_382 NGINX 1.24.0
FilingBox MEGA2 v2 Windows Client	CPU	Intel(R) Core(TM) i5-7600 CPU @ 3.5 GHz or above
	RAM	8 GB or higher
	SSD	At least 10 GB of space required for the TOE installation
	NIC	100/1000 Mbps X 1 Port or more
	OS	Windows Server 2016 64-bit Version 1607, OS Build 14393.693

FilingBox MEGA2 v2 Linux Client	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or above
	RAM	16 GB or higher
	SSD	At least 10 GB of space required for the TOE installation
	NIC	100/1000 Mbps X 1 Port or more
	OS	Rocky Linux 8.8 64-bit (Kernel 4.18.0-477.10.1)

[Table 1] Hardware and software requirements for the TOE

A PC with the following requirement is needed for authorized administrators (super/general administrators) to access the component FilingBox MEGA2 v2 Server for security management.

Category	Contents
SW (Web Browser)	Chrome V 120.0 (64 bit)

[Table 2] The minimum requirements for the administrator's PC

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	FilingBox MEGA2 v2	
Version	v2.6.0	
TOE Components	FilingBox MEGA2 v2 Server	FilingBox MEGA2 v2 Server v2.2.0 (FilingBox MEGA2_v2_Server_v2.2.0.tgz)
	FilingBox MEGA2 v2 Windows Client	FilingBox MEGA2 v2 Windows Client v2.2.0 (FilingBox MEGA2_v2_Windows_Client_v2.2.0.exe)
	FilingBox MEGA2 v2 Linux Client	FilingBox MEGA2 v2 Linux Client v2.2.0 (FilingBox MEGA2_v2_Linux_Client_v2.2.0.tgz)
Guidance	FilingBox MEGA2 v2 Server User Manual v1.3	

Document	FilingBox MEGA2 v2 Client User Manual v1.3
	FilingBox MEGA2 v2 Server Installation Manual v1.4
	FilingBox MEGA2 v2 Client Installation Manual v1.4

[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 Scheme for IT Security (May 17, 2021)
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
Protection Profile	ST does not claim conformance to PP
Developer	Namusoft Co., Ltd.
Sponsor	Namusoft Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	March 26, 2024
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [6] by security requirements. Thus, the TOE provides the following security features: security audit, cryptographic operations using OpenSSL, user data protection, identification and authentication, security management, TSF protection function, and TOE access. The details of SFRs

can be found in the ST [6].

4. Assumptions and Clarification of Scope

There is no explicit Security Problem Definition chapter, therefore no Assumptions section in the low assurance ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target.

5. Architectural Information

The TOE is software consisting of the following components:
- FilingBox MEGA2 v2 Server
- FilingBox MEGA2 v2 Windows Client
- FilingBox MEGA2 v2 Linux Client
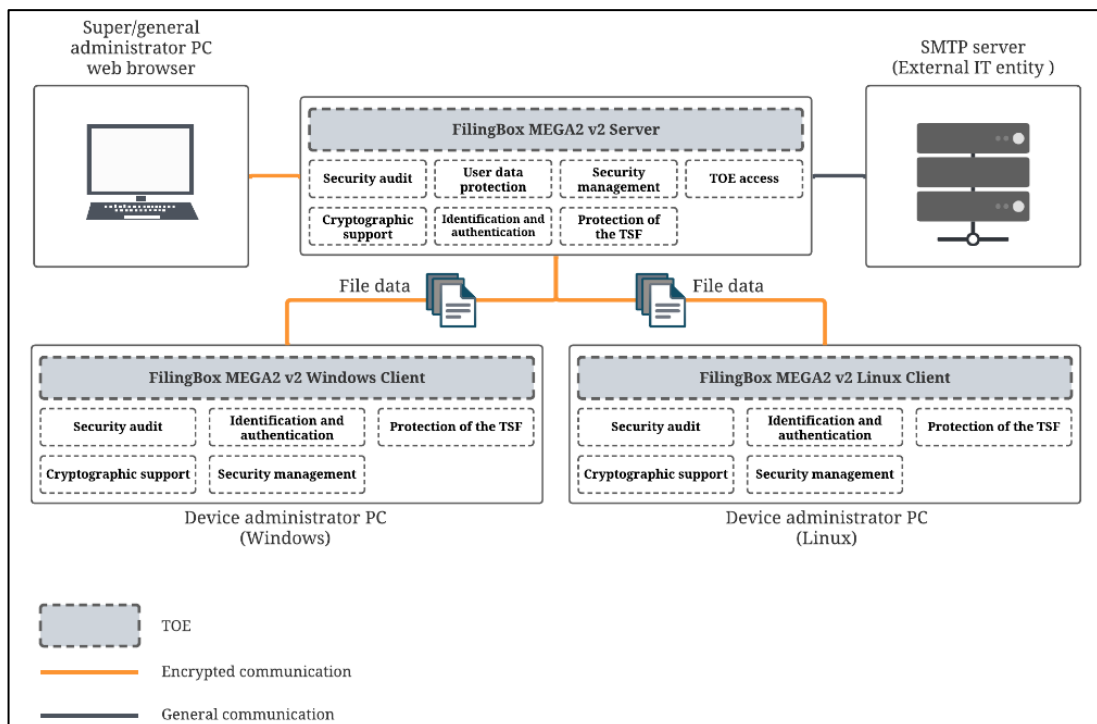
[Figure 2] Architectural Information of the TOE

6. Documentation

The following documentations are evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
FilingBox MEGA2 v2 Server User Manual v1.3	v1.3	February 26, 2024
FilingBox MEGA2 v2 Client User Manual v1.3	v1.3	February 26, 2024
FilingBox MEGA2 v2 Server Installation Manual v1.4	v1.4	February 26, 2024
FilingBox MEGA2 v2 Client Installation Manual v1.4	v1.4	February 26, 2024

[Table 5] Documentation

7. TOE Testing

The evaluator installed and prepared the TOE in accordance to the preparative procedures, then conducted independent testing based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. 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's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is FilingBox MEGA2 v2 (version number v2.6.0). See table 3 for detailed information on the TOE components.

The TOE is installed from the CD-ROM distributed by Namusoft Co., Ltd. After installing the TOE, the administrator can check the TOE version from the product. 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 [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 of EAL1.

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 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 it is 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 list includes the TOE and the evaluation evidence required by the SARs in the ST. Therefore, the verdict PASS is assigned to ALC_CMS.1.

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 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 developer has provided a high-level description of at least 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)

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 penetration testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE, 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

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		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_IND.1	ATE_IND.1.1E	PASS	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 TOE shall be located in a physically secure environment to which only the authorized administrator is allowed to access. The TOE shall not allow remote management.
- The authorized administrator of the TOE shall preserve a secure state of the TOE by various methods such as keeping the OS and the DBMS up to date with the latest patch, eliminating unnecessary services, and changing the default ID and password.
- The authorized administrator shall periodically checks 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.

11. Security Target

FilingBox MEGA2 v2 Security Target v1.5 [6] is included in this report for reference.

12. Acronyms and Glossary

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
Authorized Administrator	Authorized user to securely operate and manage the TOE

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 (31 October 2022)

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

[5]   FilingBox MEGA2 v2 Evaluation Technical Report V3.00, 26 March 2024

[6]   FilingBox MEGA2 v2 Security Target v1.5, 21 March 2024