KECS-CR-22-32

LG App Monitoring Security Solution V1.0 for webOS TV

Certification Report

Certification No.: KECS-CISS-1174-2022

2022. 06. 23

IT Security Certification Center

History of Creation and Revision

No.	Date	Revised Pages	Description
00	2022.06.23	-	Certification report for LG App Monitoring Security Solution V1.0 for webOS TV - First documentation

This document is the certification report for ‘LG App Monitoring Security Solution V1.0 for webOS TV’ by LG ELECTRONICS Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory (KSEL)

Table of Contents

1. Executive Summary

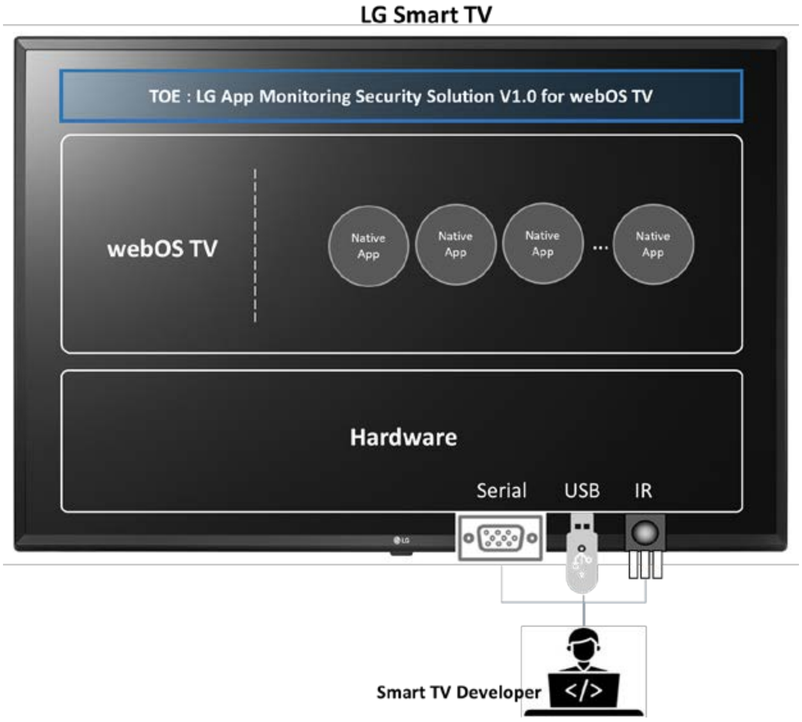
This report describes the result of the EAL2 evaluation of “LG App Monitoring Security Solution V1.0 for webOS TV” from LG ELECTRONICS Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on June 22, 2022. This report grounds on the evaluation technical report (“ETR” hereinafter)[3] and the Security Target (“ST” hereinafter)[4]. 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 EAL2. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 conformant.

LG App Monitoring Security Solution V1.0 for webOS TV (hereinafter “TOE”) is a Smart TV Security Solution that provides security functions in the form of software by being embedded on “LG Smart TV based on webOS” (hereinafter “Smart TV”). The TOE is used to make a blocking request to webOS when an unauthorized Native Apps are executed to prevent operating Smart TV from performing unintended services offered by Native Apps. Unintended service is a service not provided by authorized Native App included in webOS TV. Whitelist used to verify unauthorized Native App is created by Smart TV Developer. The TOE user is a Smart TV Developer. Smart TV Developer uses TOE in the webOS TV development stage. The scenarios in which the TOE is used are as follows. First, the Smart TV Developer physically includes ‘AppMonitoringService-1.0.WO4S21.r01’ of the TOE in the webOS TV so that the webOS TV provides the Native App tamper detection function. In addition, the Smart TV Developer creates the Native App tamper detection rule using ‘makeWhitelistRule-1.0.WO4S21.r01’ of the TOE.

The TOE provides major security features for the secure operation of Smart TV with Native App Integrity monitoring by comparing the hash value of Native App's ELF, Executable or text file with the Whitelist Rule. Whitelist Rule contain the hash values of Native Apps that are the list of Native Apps installed on Smart TV that are allowed to execute.

The TOE operational environment is illustrated as the following figure.



[Figure 1] Operational environment for Smart TV Developer of the TOE

The TOE is a Smart TV Security Solution that provides security functions in the form of software by being embedded on Smart TV. The TOE operates on the Smart TV which is developed based on webOS 6.0 and shall be installed and executed in the Smart TV. The TOE requests the webOS(LSM) to allow Native Apps that are not tampered(ELF, Executable or text file hash value of Native App is not tampered) and requests the webOS(LSM) to deny Native Apps that are tampered(ELF, Executable or text file hash value of Native App is tampered). The subject that actually allows and blocks execution of Native App is webOS(LSM).

In order for the Smart TV Developer to operate the TOE, the Serial(RS-232), USB and IR Receiver must be supported in the TOE operating environment. Smart TV Developer can execute commands for the TOE and Native Apps installation, create the Whitelist Rule file, and review the TOE reference information. The Smart TV Developer saves the distributed the TOE installation file and Native App installation file (including binaries) to the USB in order to install it on the Smart TV and delivers it to the Smart TV. The Smart TV Developer can power on/off the Smart TV through the IR Receiver and start or stop the webOS including systemd in which the TOE execution daemon is registered.

The TOE is a security solution that is in the form of software running in LG Smart TV and has the hardware and the software requirements as in the following [Table 1] and [Table 2]. [Table 1] and [Table 2] show the TOE Operational Environments not included in the TOE scope.

Category		Minimum Specifications
H/W	CPU	ARM architecture (Cortex A53 Quad) or higher
	DDR Memory	2.0 GB or higher
	Flash Memory	15 MB or higher (Capacity required for TOE installation)
	USB	USB 2.0 X 1
	Serial	RS-232C X 1
	IR Receiver	IR Receiver Module X 1

[Table 1] Non-TOE Hardware required by the TOE

※ After Smart TV development is completed, Serial is not provided to Smart TV User.

Software	Description
webOS 6.0	Operating system based on Linux Kernel 4.4.84
OpenSSL 1.1.1g	Generates the required hash value when verifying the integrity of the Native app and creating a Whitelist Rule file

[Table 2] Non-TOE Software required by the TOE

※ LS2, LSM, SAL and OpenSSL are included in the operating system(webOS 6.0).

2. Identification

The TOE is identified as follows:

Developer	LG ELECTRONICS Co., Ltd.
TOE reference	LG App Monitoring Security Solution V1.0 for webOS TV
Detail Version	WO4S21.r01
TOE Component	AppMonitoringService-1.0.WO4S21.r01
	makeWhitelistRule-1.0.WO4S21.r01
Guide	LG App Monitoring Security Solution V1.0 for webOS TV Developer Guide V1.3

[Table 3] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	LG App Monitoring Security Solution V1.0 for webOS TV
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	EAL2
Protection Profile	N/A (ST does not claim conformance to a PP)
Developer	LG ELECTRONICS Co., Ltd.
Sponsor	LG ELECTRONICS Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	June 22, 2022
Certification Body	IT Security Certification Center

[Table 4] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST by security objectives and security requirements. The TOE provides security features to prevent execution of unauthorized Native App. For more details refer to the ST.

4. Assumptions and Clarification of Scope

4.1 Assumptions

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST, chapter 3.3):

- The TOE Developer does not have any malicious purposes, has been properly trained for use of the TOE, and performs its obligations adequately in accordance with the developer guidance. In addition, Smart TV Developers who develop services in smart TVs that interoperate with the TOE should not implement to include any malicious behaviors intentionally in the LG Smart TV services (A.TrustedDeveloper).
- The TOE uses webOS 6.0 function. webOS 6.0 support LS2, SAL and LSM. LS2 is responsible for delivering the commands (review the TOE reference information) entered by the Smart TV Developer. SAL is the ability to store security logs in the filesystem. LSM is a function that hooks information (Executed Native App ELF, Executable or text file path and PID) of Native App when Native App is executed. In addition, it receives and executes requests to allow and block Native App execution through the TOE (A.webOSFunctionSupport).

5. Architectural Information

5.1 Physical Scope of TOE

The physical scope of the TOE includes software and developer guidance.

The TOE is delivered to Smart TV Developers through a distribution site where only the Smart TV Developers of LG Electronics can access including developer guide. The TOE is installed on webOS TV. The physical scope of the TOE includes only the software that is in charge of Native App Integrity Monitoring security function, however the scope does not include the other security functions in Smart TV.

TOE Component	Description	Distribution Form	Distribution Method
AppMonitoringService-1.0.WO4S21.r01 (AppMonitoringService-1.0.WO4S21.r01.tar)	Binary and setting files that perform Native App tamper detection	S/W	Distributed in a file format through a distribution site where only the Smart TV Developers of LG Electronics can access.
makeWhitelistRule-1.0.WO4S21.r01 (makeWhitelistRule-1.0.WO4S21.r01)	Binary to create Whitelist Rule		
LG App Monitoring Security Solution V1.0 for webOS TV Developer guide V1.3 (LG App Monitoring Security Solution V1.0 for webOS TV Developer guide V1.3.pdf)	Developer Guide	Electronic document File (PDF)	

5.2 Logical Scope of TOE

The logical scope of the TOE comprises the security function (Native App Integrity Monitoring function) that are offered by the software included in the physical scope of the TOE.

In order to perform Native App Integrity Monitoring function provided by the TOE accurately, the functions offered by webOS(LSM, LS2, SAL and OpenSSL) should be supported. webOS(LSM) sends the information of the Native App to the TOE to determine whether the Native App is tampered with after changing the executed Native App to a running standby state. webOS(LS2) is responsible for delivering the commands (review the TOE reference information) entered by the Smart TV Developer using Serial to the TOE. webOS(SAL) is responsible for receiving audit logs generated by the TOE and storing them in filesystem. webOS(OpenSSL) receives the request from the TOE and generates a hash value that verifies the integrity of the native app and creates a whitelisting rules file. When a Power on signal is received via the IR Receiver, systemd is responsible for automatically executing the TOE.

The detailed security functions included in the logical scope of are as follows:

Native App Integrity Monitoring

This function provides Integrity Monitoring for Native App execution. Based on Native App Tamper Detection, this function allows or denies executions of Native Apps. The TOE creates a Whitelist Rule by using webOS(OpenSSL) to generate hash values for ELF, Executable or text files of All Native Apps installed on Smart TV at the time of initial installation of the TOE or installation of the new Native App. The Whitelist Rule includes a list of hash values that are executable Native Apps on Smart TV. When the Native App installed on the Smart TV is executed, webOS(LSM) transmits the Native App information to the TOE and requests integrity verification. The TOE generates a hash value for ELF, Executable or text files of Native Apps using webOS(OpenSSL) and compares them with the Whitelist Rule. If the comparison results match, the TOE requests the webOS(LSM) to allow the execution of the Native App. If the hash value doesn’t match, the TOE requests webOS(LSM) to block the execution of the Native App.

The TOE provides Smart TV Developer with the ability to review the TOE information. LS2 is responsible for delivering the command (review the TOE reference information) entered by the Smart TV Developer using Serial to the TOE. When the Smart TV Developer reviews the TOE information, the TOE returns version information and detailed information.

The TOE can generate security-related logs and write logs to the filesystem using SAL. The logs record a Timestamp, which is dependent on the time of the webOS operating system. This logs comprise information on the Native App that is blocked from execution. Logs generated by the TOE are delivered to webOS(SAL) and stored in the filesystem. In addition, the TOE generates a log of the results of Whitelist Rule file creation and overwrite.

6. Documentation

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

Identifier	Version
LG App Monitoring Security Solution V1.0 for webOS TV Developer Guide	V1.3

[Table 5] Documentation

7. TOE Testing

The developer took a testing approach based on the TSFIs provided by the TOE based on the operational environment of the TOE.

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.1. This means that the developer tested all the TSFI defined in the functional specification, and demonstrated that the TSF behaves as described in the functional specification.

Therefore, the developer tested all SFRs defined in the ST.

The evaluator performed all the developer’s tests, and conducted independent testing listed in ETR, based upon test cases devised by the evaluator. The evaluator set up the test configuration and testing environment consistent with the ST. The evaluator considered the followings when devising a test subset:

- TOE security functionality: The TOE is a Smart TV Security Solution that provides security functions in the form of software by being embedded on LG Smart TV based on webOS. The TOE is used to make a blocking request to webOS when an unauthorized Native Apps are executed to prevent operating Smart TV from performing unintended services offered by Native Apps.
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL2, and the evaluator tried to balance time and effort of evaluator's activities between EAL2 assurance components.

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 bypassing security functionality, 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 ETR.

8. Evaluated Configuration

The TOE is a Smart TV Security Solution that provides security functions in the form of software by being embedded on LG Smart TV based on webOS. The TOE is used to make a blocking request to webOS when an unauthorized Native Apps are executed to prevent operating Smart TV from performing unintended services offered by Native Apps.The TOE is identified by TOE and detail version. The TOE identification information is provided CLI. In addition, guidance documents listed in [Table 5] of the chapter 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] 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 EAL2.

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 (ST reference, TOE reference, TOE overview and TOE description), and these four 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 Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore, the verdict

PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.2.

The ST clearly and unambiguously defines the extended SFR component (FPT_FDI_EXP.1). Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore, the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification describes how the TOE meets each SFR, 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 configuration management document describes the method used to uniquely identify all configuration items. Therefore, the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE itself, the evaluation evidence required by the SARs, and the parts that comprise the TOE. Therefore, the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures that are necessary to maintain security when distributing the TOE to the user. Therefore, the verdict PASS is assigned to ALC_DEL.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 the 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 security architecture document is structured to ensure that TSF cannot be compromised or bypassed, and appropriately describes that the TSF which provides the security domain separates these domains from each other. Therefore, the verdict PASS is assigned to ADV_ARC.1.

The functional specifications specifies the purpose of an interface, method of use, input and output parameters, actions of an interface, and error messages generated by the TSF at equal detail level, and accurately and completely describes the TSFI. Therefore, the verdict PASS is assigned to ADV_FSP.2.

The TOE design description provides the structure of the TOE in terms of subsystems, identifies all subsystems of the TSF, describes the behavior summary of each SFR-supporting or SFR-non-interfering TSF subsystems, and summarizes the SFR-enforcing behavior of the SFR-enforcing subsystems. Therefore, the verdict PASS is assigned to ADV_TDS.1.

Therefore, the security architecture description(the TSF architecture attribute which describes how to the TSF security enforcement is not compromised or bypassed), functional specification(TSF interfaces description) and TOE design description, which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore, the verdict PASS is assigned to ATE_COV.1.

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 design documentation and had confidence in the developer's test results by performing all of the developer's tests. Therefore, the verdict PASS is assigned to ATE_IND.2.

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.2.

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 less than an enhanced-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_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.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_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS		
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
	ATE_COV.1	ATE_COV.1.1E	PASS	PASS	
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	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:

- Smart TV developer use TOE in the development process to manage the threat caused by tampering with Native App. Therefore, Smart TV developer must use TOE binary file(makeWhitelistRule) to create a hash values for authorized Native App.
- Smart TV developer create whitelist rule using TOE binary file(makeWhitelistRule). And then, Smart TV developer have to reboot Smart TV for the secure state of TSF.
- Note that LSM included in webOS must be activated for the TOE to operate in a secure state.

11. Evaluation Evidence

Identifier	Issue date
LG App Monitoring Security Solution V1.0 for webOS TV Security Target V1.7	2022.06.21
LG App Monitoring Security Solution V1.0 for webOS TV Functional Specification V1.2	2022.05.13
LG App Monitoring Security Solution V1.0 for webOS TV TOE Description Specification V1.1	2022.05.13
LG App Monitoring Security Solution V1.0 for webOS TV Security Architecture Description V1.1	2022.05.13
LG App Monitoring Security Solution V1.0 for webOS TV Developer Guide V1.3	2022.05.13
LG App Monitoring Security Solution V1.0 for webOS TV CM Documentation V1.3	2022.06.21
LG App Monitoring Security Solution V1.0 for webOS TV Delivery Documentation V1.1	2022.05.13
LG App Monitoring Security Solution V1.0 for webOS TV Test Documentation V1.1	2022.05.13

[Table 7] Evaluation evidence

12. Acronyms and Glossary

CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
App	An app refers to apps that can be installed on a Smart TV and perform various functions.
LSM	It refers to Linux Security Module (LSM), and this function is included in webOS. It helps the TOE by hooking an execution of Native App, sending information of the Native App to the TOE, and blocking an execution of tampered Native App.
LS2	LS2 means APIs that webOS service daemons provide based on the Luna-Bus which is a bus system used in webOS. The Luna Bus and APIs are implemented based on the Luna-Service2 library, and are referred to as LS2.
Native App	Native Apps are implemented based on C/C++

optimized for webOS using webOS NDK(Native Development Kit). Native App runs by directly calling the services provided by the kernel and UI framework, so the execution speed is fast and stable. Native Apps contain executable file types (ELF, Executable, text).

SAL

It refers to Security Audit Log, and this function is included in webOS. It receives audit log messages from the TOE, and it stores the audit log in the file system.

Smart TV Developer

Smart TV Developers refer to the developers who implement the services in the Smart TV which interoperate with the TOE during development of the Smart TV’s software image. Smart TV Developer performs installation, setting and testing.

Smart TV User

A Smart TV User is a person who can use the Native Service authorized by the Smart TV Developer after development of the smart TV.

Threat agent

Unauthorized users who threaten to access, change, or delete assets illegally

systemd

The systemd is an init system that bootstraps userspace instead of the init processor and finally manages all processes.

Tamper Detection

It refers that something can detect the integrity is compromised or not.

web-centric platform

A web app refers to application software that can be used in a web browser and refers to a platform on which the web app can be run.

webOS

webOS is an LG-owned, Linux-based, Smart TV operating system that is set up to allow control and access of Smart TV's more advanced features and connected devices through a graphical user interface(GUI). webOS includes LSM, LS2, SAL and OpenSSL functions and includes Native Apps essential for webOS.

webOS TV

webOS TV is a web-centric platform based on webOS and specialized for LG Smart TV. TOE is installed and operated on webOS TV.

Whitelist Rule

Whitelist Rule indicates a hash value of Native App. The Whitelist Rules are stored in a file called “whitelist.rule”, which is located in file system.

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] LG App Monitoring Security Solution V1.0 for webOS TV, Evaluation Technical Report V3.00, June 22, 2022

[4] LG App Monitoring Security Solution V1.0 for webOS TV Security Target V1.7, June 21, 2022