KECS-CR-17-19

Application Security Solution V1.0 for LG webOS TV

Certification Report

Certification No.: KECS-CISS-0783-2017

2017. 4. 19.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2017.04.19.	-	Certification report for Application Security Solution V1.0 for LG webOS TV - First documentation

This document is the certification report for Application Security Solution V1.0 for LG webOS TV of LG Electronics, Inc..

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association (TTA)

Table of Contents

1. Executive Summary 5

2. Identification 6

3. Security Policy 8

4. Assumptions and Clarification of Scope 8

5. Architectural Information 9

6. Documentation 9

7. TOE Testing 10

8. Evaluated Configuration 11

9. Results of the Evaluation 11

9.1 Security Target Evaluation (ASE) 11

9.2 Life Cycle Support Evaluation (ALC) 12

9.3 Guidance Documents Evaluation (AGD) 12

9.4 Development Evaluation (ADV) 13

9.5 Test Evaluation (ATE) 13

9.6 Vulnerability Assessment (AVA) 14

9.7 Evaluation Result Summary 14

10. Recommendations 15

11. Security Target 16

12. Acronyms and Glossary 16

13. Bibliography 18

1. Executive Summary

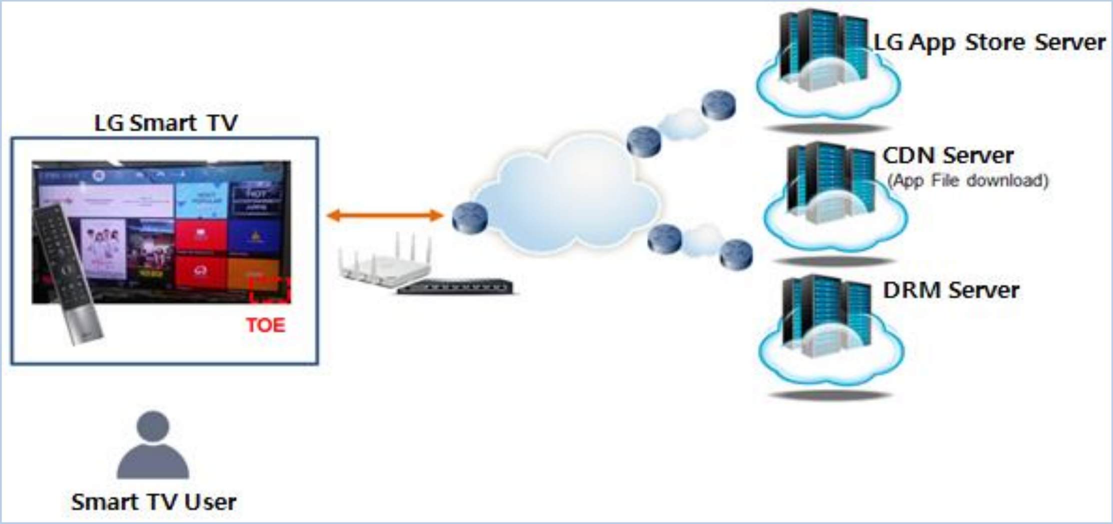
This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of Application Security Solution V1.0 for LG webOS TV of LG Electronics, Inc. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is smart TV security solutions consisting of software libraries to provide security features to install and use applications (“app” hereinafter) securely on the webOS based LG smart TV.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on April 7th, 2017. This report grounds on the evaluation technical report (ETR) TTA had submitted [5] and the Security Target (ST) [6][7].

The ST does not claim conformance to a Protection Profile. 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.

[Figure 1] shows the operational environment of the TOE.



[Figure 1] Operational environment of the TOE

The TOE is composed of 5 components: SAM which manages installation and execution of apps, WAM which manages secure execution of Web Apps, Security Manager which manages app DRMs and verifies digital signatures, Jailer which provide sandboxing execution environments for the Native Apps, and OpenSSL for encryption and decryption.

The TOE operates on the webOS based smart TV. The LG App Store server is required to register apps in the LG Contents Store and download them to the LG smart TV. CDN server is necessary to download application package files (IPK) to be installed on the LG smart TV. DRM server is used to manage DRM ROs (Right Objects) for the apps installed on the LG smart TV.

The TOE implements security features such as app installation, execution, and contents protection. For more details refer to the ST [6][7].

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

Category		Contents
Hardware	CPU	ARMv7 Cortex A9
	DDR Memory	DDR3 1GB
	Flash Memory	eMMC 2GB
	NIC	Gbit MAC + 100Mbps PHY
	SoC	M16P
Software	Web browser	Chromium 38
	OS	webOS Dreadlocks (v3.5) / Linux kernel 4.4.3

[Table 1] Hardware and software requirements for the TOE

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is software libraries consisting of the following components and related guidance documents.

TOE	Application Security Solution V1.0 for LG webOS TV	
Version	V1.0	
Build Number	drd4tv#504	
TOE Components	SAM	sam_1.0.0-192.drd4tv.93-r9_m16p.ipk appinstalld_1.0.0-96.drd4tv.24-r7_m16p.ipk
	WAM	wam_1.0.0-87-r1starfish3_m16p.ipk webappmgr3-pluggable_1.0.0-39.drd4tv.67-r11_m16p.ipk
	Security Manager	securitymanager_1.0.59-102-r24.0_m16p.ipk
	Jailer	webos-jail_2.1.2-145.drd4tv.28-r6_m16p.ipk
	OpenSSL	libcrypto1.0.0_1.0.2k0webos17-r0webos17_m16p.ipk libssl1.0.0_1.0.2k0webos17-r0webos17_m16p.ipk openssl_1.0.2k0webos17-r0webos17_m16p.ipk
Guidance Document	Application Security Solution V1.0 for LG webOS TV user guidance V1.4.pdf	

[Table 2] TOE identification

Note that the TOE is delivered in a file format through a distribution site where only the developers of LG Electronics can access.

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

Scheme	Korea Evaluation and Certification Guidelines for IT Security (June 27, 2016) Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL2
Developer	LG Electronics, Inc.
Sponsor	LG Electronics, Inc.
Evaluation Facility	Telecommunications Technology Association (TTA)
Completion Date	April 7, 2017

of Evaluation	
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [6][7] by security objectives and security requirements. Thus the TOE provides following security features.

- The TOE provides app installation protection which blocks the installation of unauthorized apps through digital signature verification when the smart TV user installs an app on the smart TV that is connected to Internet. The digital signature generation process for the app takes place from the LG App Store server side, and this enables only the apps that are downloaded from the LG App Store server to be installable on the smart TV.
- The TOE provides app execution protection based on the types of apps. For Native Apps, the TOE creates a sandboxed app execution environment based on Native App's security attributes and executes an app, which will block the app from accessing to unauthorized system directories/files, device files, or other apps' space. For Web Apps, the TOE allows them to be able to use only approved APIs, and blocks the apps from directly accessing to the webOS file system. Web Apps can access to the allowed directories that are defined in white-list only according to trust level.
- The TOE provides app contents protection based on the DRM. To verify the app content files, the TOE verifies the DRM license. The TOE allows the encrypted app contents to be decrypted only in RAM and always stores them in the encrypted state in the flash memory to protect the app contents.

4. Assumptions and Clarification of Scope

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 [6][7], chapter 3.3):

- For secure operation of the TOE, LG App Store server, CDN server, DRM server which exist in the operating environment are operated securely.

- All system service binaries and library files that are included in the smart TV firmware are installed in the read-only file system to be protected from unauthorized modification attempts.
- The TOE developer does not have any malicious intentions, 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 smart TV services.
- LG Electronics must assign unique MAC addresses to each smart TV device in order to manage smart TV devices securely. This MAC address should be unique because it is used to identify the smart TV device uniquely in LG App Store server.

Furthermore, some aspects of organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment: Secure key operation management and Secure smart TV update. Details can be found in the ST [6][7], chapter 3.2 and 4.2.

5. Architectural Information

The TOE is software libraries consisting of the following components.

- SAM manages the app lifecycle including app installation, execution, and uninstallation.
- WAM manages the secure execution of Web Apps.
- Security Manager performs app security checks such as an App DRM functions and digital signature verification.
- Jailer provides the sandboxed execution environment for Native Apps.
- OpenSSL provides cryptographic operations.

6. Documentation

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

Identifier	Release	Date
Application Security Solution V1.0 for LG webOS TV user guidance V1.4.pdf	V1.4	March 30, 2017

[Table 4] Documentation

7. TOE Testing

The developer took a testing approach based on the APIs and 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 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 for SFR-enforcing of the TOE, and demonstrated that the TSFI behaves as described in the functional specification.

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator performed all tests provided by developer and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The evaluator determined that the preparative procedures are not applicable to the TOE which is software libraries, thus the tests do not cover preparative procedures.

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.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [5].

8. Evaluated Configuration

The TOE is Application Security Solution V1.0 for LG webOS TV (Build Number: drd4tv#504). See table 2 for detailed information on the TOE components.

The TOE can be downloaded by any authorized developers of LG Electronics from the TOE distribution system. After installing the TOE, the developer can verify the TOE version by command. And the guidance documents listed in this report chapter 5, [Table 4] was 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 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 (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 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 does not define any extended component. 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 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 uses a CM system that uniquely identifies all configuration items. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE, the parts that comprise the TOE, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the configuration management used throughout TOE development and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable.

Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. Therefore the verdict PASS is assigned to ADV_TDS.1.

The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, for the SFR-enforcing TSFIs the developer has described the SFR-enforcing actions and direct error messages. Therefore the verdict PASS is assigned to ADV_FSP.2.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested TSFIs, and that 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, 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_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_CMC.2	ALC_CMC.2.1E	PASS	PASS	PASS
	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	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	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	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_COV.1	ATE_COV.1.1E	PASS	PASS	PASS
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	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 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 generation, storage, access control, and destruction of the cryptographic keys (the private key used for app digital signatures, the CEK (Content Encryption Key) used for encrypting app contents files and the RODB encryption key), which are performed securely in accordance with LG Electronics regulations and policies.

- After shipment of smart TVs, the smart TV software which includes the TOE must be updated through network service update (NSU), TV firmware update via broadcasting signal (OTA), or USB update by customer service center.
- LG Electronics must assign unique MAC addresses to each smart TV device in order to manage smart TV devices securely.
- LG App Store server, CDN server, DRM server which exist in the operating environment are operated securely.

11. Security Target

Application Security Solution V1.0 for LG webOS TV Security Target V1.5 [6] is included in this report for reference. For the purpose of publication, it is provided as sanitized version [7] according to the CCRA supporting document ST sanitizing for publication [8].

12. Acronyms and Glossary

API	Application Programming Interface
CC	Common Criteria
CDN	Content Delivery Network
CEK	Content Encryption Key
EAL	Evaluation Assurance Level
IPK	Itsy Package
MAC	Medium Access Control
PP	Protection Profile
RO	Rights Object
RODB	Rights Object Database
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

App

An app refers to apps that can be installed on a smart TV and perform various functions. It is used to expand functions according to the user's requirement.

App Content

The contents of the app correspond to the contents which compose the app and they include the app’s source code files and various resource files referenced by source codes. When referring to ‘content’ without the ‘app’ in front of it, it not only refers to apps but also includes other content such as movies, TV series, music videos, and music that are available for use on the smart TV.

App Package File

An app package file refers to various control files that are required for installing an app and data files which compose an app that are packaged in the ipk format.

Web App

Web App is implemented using HTML, CSS, JavaScript, and image resources. In webOS, it runs on WAM.

Native App

Native Apps are implemented based on C/C++ using webOS NDK (Native Development Kit) and system call APIs.

LG App Store

The LG App Store provides apps and content and users can download apps that they wish to install on the smart TV. LG App Store service is provided through LG App Store server and CDN server.

DRM Server

The DRM Server refers to a server that performs DRM encryption and decryption of an app installation file and generates an encryption key to protect an app installation file when downloading an app to install on the smart TV.

DRM

DRM (Digital Right Management) refers to the copyright management technology for digital contents. The DRM technology is based on protecting contents through encryption, and includes a technology for managing rights data to enable only a trusted user to decrypt content for use.

App DRM

It provides DRM function to ensure secure distribution of apps to be installed on the smart TV and to prevent unauthorized app distribution.

CEK

CEK (Contents Encryption Key) refers to a key used to encrypt app content files for App DRM packaging. When an app is registered on the LG App Store server, a unique CEK is generated for each app, and stored in the DRM server. When the app is installed, RO download request is made from the TV to the DRM server, and CEK, which is included in the RO, is downloaded to the TV.

RO

It is an abbreviation of Rights Object and is defined as ‘a set of permissions related to the protected contents and other attributes’ (Defined in the OMA DRM standard). ROs include contents data including CID, CEK, and xml data including permissions, outputprotection information. Currently, only CID and CEK are being used on the LG webOS Smart TV.

RODB

RODB refers to the file DB which stores RO data. Encrypted RO data is stored in this RODB.

Sandboxing

Sandboxing refers to a security function to prevent apps from accessing unauthorized smart TV resources including files and devices.

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 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
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 4, CCMB-2012-09-004, September 2012

[3] Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013)

[4] Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)

[5] TTA-CCE-16-027 Application Security Solution V1.0 for LG webOS TV

Evaluation Technical Report V1.5, April 7th, 2017

[6] Application Security Solution V1.0 for LG webOS TV Security Target v1.5, May 30th, 2017 (Confidential Version)

[7] Application Security Solution V1.0 for LG webOS TV Security Target Lite v1.5, May 30th, 2017 (Sanitized Version)

[8] ST sanitising for publication, CCDB-2006-04-004, April 2006