Application Security Solution V1.0 for LG webOS TV Security Target V1.5

Document History

Date	Version	Description
2016.09.20	1.0	Initial Version
2017.01.18	1.1	- Modifying SFR, security problem definition, and security objectives.
2017.03.03	1.2	- TOE name is changed.
2017.03.20	1.3	- Add detailed version to identify TOE. - Modifying logical scope and security requirement, TOE summary. - Modifying security problem definition and security objectives for TOE and operational environment.
2017.03.27	1.4	- Add Abbreviations, - Modify description about trusted developer - Add app security attributes - Modify FCS_CKM.4 in the security functional requirement rationale.
2017.03.30	1.5	- Modify hardware information in non-TOE HW/SW - Modify physical scope.

Table of Contents

Table of Contents (tables)

Table of Contents (Figure)

1 Introduction of Security Target

1 This chapter provides information of Security Target and TOE reference, and TOE overview as well as its description. From the Security Target and TOE Reference section, Security Target and TOE identification information will be provided. Also, TOE will be briefly explained in the TOE Overview. More details about the TOE will follow in the TOE Description section so that TOE can be explained in stages.

1.1 Security Target Reference

2 The Security Target is identified as below.

- Title: Application Security Solution V1.0 for LG webOS TV Security Target
- Security Target Version: V1.5
- Authors: LG Electronics, Inc.
- Publication Data: 2017.03.30

1.2 TOE Reference

3 This section provides TOE reference as in the following.

- TOE Title: Application Security Solution V1.0 for LG webOS TV
- TOE Version: 1.0
- Build Number: drd4tv#504
- Developer: LG Electronics, Inc.
- TOE Components (S/W)

TOE Component	Version
SAM	sam-1.0.0-192.drd4tv.93-r9
	appinstalld-1.0.0-96.drd4tv.24-r7

TOE Component	Version
WAM	wam-1.0.0-87-r1starfish3
	webappmgr3-pluggable-1.0.0-39.drd4tv.67-r11
Security Manager	securitymanager-1.0.59-102-r24
Jailer	webos-jail-2.1.2-145.drd4tv.28-r6
OpenSSL	openssl-1.0.2k0webos17-r0webos17

1.3 TOE Overview

4 This section describes information about its purpose and key security functions of the software that is provided to use apps securely on the webOS based smart TV.

5 Application Security Solution V1.0 for LG webOS TV (hereinafter TOE) is a smart TV security solution which provides security functions to use applications (hereinafter app) securely on the webOS based LG Smart TV (hereinafter smart TV). The TOE provides functions for the secure installation and use of apps on the smart TV.

6 The TOE's purpose and key security functions are as follows.

■ App installation Protection

This function 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 process for the app takes place from the LG App Store server and this enables only the apps that are downloaded from the LG App Store server to be installable on the smart TV.

■ App Execution Protection

When apps are executed on the smart TV, the TOE provides app execution protection function differently for web apps and native apps. TOE creates a sandboxed app execution environment based on native app's security attribute 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.

■ App Contents Protection

All apps downloaded from the LG App Store are protected by DRM, and TOE

provides a function to check whether these apps are protected by DRM and to decrypt DRM encrypted app contents files. To verify and decrypt the app content files, the TOE downloads ROs from the DRM server. The ROs include CEK (Contents Encryption Key), CID (Contents ID), and DRM license data. The TOE verifies the DRM license when executing web apps, and uses CEK to decrypt source files of the web app, which is included in DRM packaging. 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.

7 Table 1 and Table 2 identify hardware and software / operating system that are required for TOE installation and operation.

Table 1. TOE Hardware

Category		**Minimum Specifications**
Hardware	CPU	ARMv7 Cortex A9
	DDR Memory	DDR3 1GB
	Flash Memory	eMMC 2GB
	NIC	Gbit MAC + 100Mbps PHY
	SoC	M16P

Table 2. Software / Operating System

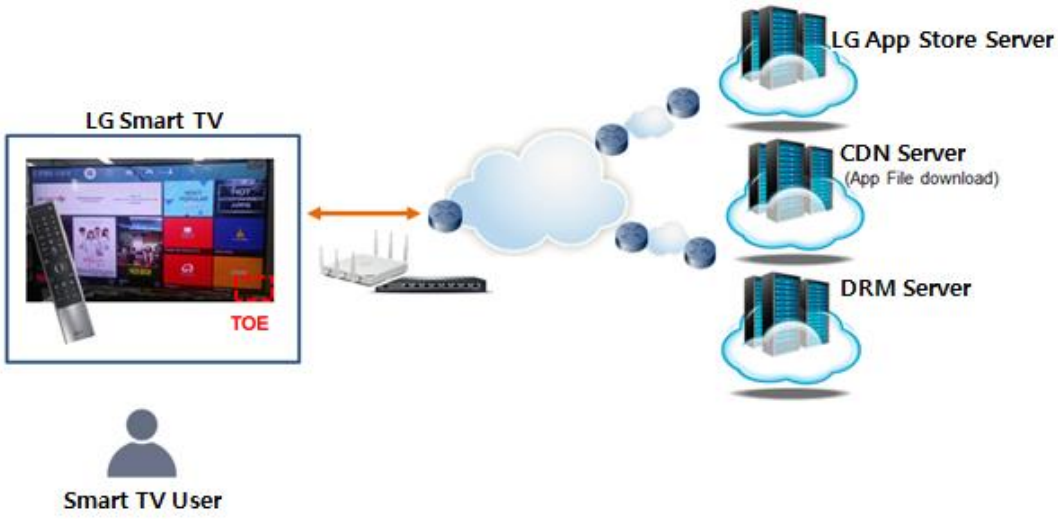
Category		**Version**
Software	Web browser	Chromium 38
Operating System	OS	webOS Dreadlocks (v3.5) / Linux kernel 4.4.3

※ Among external entities in the smart TV, LG Contents Store App, SDX, and LSM are included in the operating system, which is webOS Dreadlocks.

8 The TOE operates on the smart TV which is developed based on webOS. When it's connected to the network, apps in the LG Contents Store are downloadable from the LG App Store server and installable on the smart TV. The TOE shall be installed and executed within the read-only file system in the smart TV and the downloaded apps from the LG App Store shall be installed and executed in the read-write file system.

9 The external entities of the TOE operational environment can be divided into three groups: IT entities outside of the smart TV, external entities within the smart TV, and the user.

10 Figure 1 shows the IT entities outside of the smart TV.



[Figure 1] TOE Operational Environment - IT Entities outside of Smart TV

■ LG App Store Server

Apps for use in smart TV are registered and downloadable from the LG App Store server. When app developers register apps on the server, the apps will be digitally signed using a private key from the LG App Store server. Only authorized developers can upload apps on the LG App Store server and when uploading an app, the digital signature of the app package file will be generated. When apps are registered on the LG App Store server, app files are DRM-packaged by the app DRM packaging tool.

App data and digital signature are delivered through TLS v1.2 based secure communication channel between the Smart TV and LG App Store.

■ CDN Server (App File Download Server)

CDN Server refers to the Contents Delivery Network server which serves downloading of an application package file (IPK) for installation on the Smart TV. When the smart TV user requests to install an app, app information including the app's IPK file URL is downloaded in JSON format through the LG App Store server. The IPK URL is the CDN server URL to download the actual app IPK file. The CDN server supports One-Time URLs so that even for the same IPK file, it can be downloaded using different URLs each time.

■ DRM Server

DRM server manages DRM ROs (Rights Objects) for the installed apps in the smart TV.

When installing an app, the DRM ROs corresponding to the app are downloaded from the DRM server and installed. The DRM RO includes information such as a DRM CEK, a DRM CID, and etc..

11 TOE users are divided into two groups: the smart TV developers at the development stage and smart TV users after the smart TV production including the TOE is complete.

■ Smart TV User

This refers to the user who uses a smart TV where it provides capabilities to be connected to the Internet along with TV functionalities, and to install apps to take advantage of a variety of features the Smart TV can provide. The users do not directly call the TOE but install and use apps using the Smart TV functions.

■ 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.

12 External entities which exist within the Smart TV are as follows.

■ LG Content Store App

This is an app store application for downloading apps from the LG App Store server. It provides functions such as provision of app information details as well as installation and execution of the apps.

■ SDX

SDX provides interface functions to communicate to LG App Store Server. It performs secure communication based on TLS v1.2 between the Smart TV and the LG App Store server.

■ LSM

LSM performs graphic processing. It provides webOS key graphic UIs such as the launcher UI.

■ 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.

1.4 TOE Description

13 This section describes the TOE's scope in terms of physical and logic scope of the TOE to describe the environment in which the TOE can be operated.

1.4.1 Physical Scope of the TOE

14 The physical scope of the TOE includes software provided in the form of libraries, and developer guidance.

15 The TOE is the webOS software that provides security functions for secure use of apps in the smart TV, and is distributed to smart TV developers. The TOE includes SAM that manages the app lifecycle including app installation, execution, and uninstallation, WAM that manages the secure execution of web apps, Security Manager that performs app security checks such as an App DRM functions and digital signature verification, Jailer that provides sandboxed execution environment for native apps, and OpenSSL that is used for cryptographic operations. The physical scope of the TOE is as follows.

Table 3. Physical Scope of the TOE

Category		**Distribution Form**	**Distribution Method**
SAM	sam_1.0.0-192.drd4tv.93-r9_m16p.ipk	S/W	Distributed in a file format through a distribution site where only the developers of LG
	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		Electronics can access.
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		
Developer Guide	Application Security Solution V1.0 for LG webOS TV user guidance V1.4.pdf	Electronic document file	Distributed in a file format through a distribution site where only the developers of LG Electronics can access.

1.4.2 Logical Scope of the TOE

16 The logical scope of the TOE is as follows.

17 App Installation Protection

18 When installing an app by a request from the smart TV user, TOE performs digital signature verification for the app package file which was downloaded during installation process in order to install only the authorized apps. It installs the app only if the app has been verified successfully and if not, the app cannot be installed.

19 The TOE supports the RSA-SHA256 encryption algorithm, which is for digital signature verification. The public key for the digital signature verification is stored in the read-only file system so that the file cannot be modified or deleted.

20 App Execution Protection

21 When executing apps, the TOE provides execution protection function according to the protection policy depending on the app type whether it's a web app or a native app. The attribute information for identifying the app type exists as a "type" attribute in the appinfo.json file from an app installation file.

22 The TOE identifies app properties, 'type' and 'privilegedJail', for native apps, from the appinfo.json file of the app, to configure an appropriate sandboxed app execution environment, so that each sandboxed app cannot access to other app space. The TOE constructs the separate "jail root file system" in which a native app is executed with a

regular user (non-root user) privilege so that the native app cannot access privileged system directories or device files of the smart TV.

23 The TOE restricts the accessible APIs and files fo according to the permissions policy based on the trust level for web apps. The trust level of the web app is identified by a 'trustlevel' property in the appinfo.json file, and is set to one out of three options from default, netcast, and trusted.

24 App Contents Protection

25 The TOE provides a function to execute DRM-packaged apps. The DRM packaging involves an encryption of the app contents files and adding proper DRM header to them.

26 The TOE assumes that all apps which are downloaded from the LG App Store server are DRM-packaged, and verifies whether DRM is applied or not at the time of the app execution, and executes the app only when it is verified that DRM has been normally applied.

27 The TOE securely generates and distributes a session key, which is for encryption of the RO request message and decryption of the RO response message, based on the DH algorithm in order to securely download the ROs (rights objects) which include license data and CEK from the DRM server.

28 The TOE encrypts ROs using the RO encryption key, stores them in the RODB, and decrypts them only within the RAM for use.

29 When executing web apps, the TOE decrypts the app contents files (html, js, css, etc) that are encrypted by DRM. The app contents files are always stored being encrypted in the app installation directory and are decrypted using CEK only when they are loaded in RAM by the TOE. CEK is a unique key per each app and it is created when the app is uploaded on the LG App Store server which is an external entity outside of the smart TV, and is stored securely on LG DRM server which is an external entity outside of the smart TV.

30 The TOE provides a function for secure key destruction. CEK and RODB encryption key data are removed securely from RAM after using. The TOE also provides a function to securely remove the session key used when installing apps for encryption of RO data from the memory. The TOE provides a function to remove securely DRM license and CEK data from the RODB file when deleting apps.

31 The following functions are not included in the scope of the TOE as they are performed from external entities.

- A function to generate a private key, which is used for digital signature of

the app from the LG App Store server

- A function to generate digital signatures for apps from the LG App Store server
- A function to perform DRM encryption and packaging of apps from the LG App Store server
- A function to generate a CEK that is used for DRM encryption from the LG DRM Server
- Secured communication based on TLS v1.2 between the smart TV and LG App Store server - Provided from SDX, which is an external entity in the smart TV
- A function to generate a key which encrypts RDOB

1.5 Conventions

32 The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation.

33 The CC allows several operations to be performed for functional requirements: iteration, assignment, selection and refinement. Each operation is used in this ST.

34 Iteration

Iteration is used when a component is repeated with varying operations. The result of iteration is marked with an iteration number in parenthesis following the component identifier, i.e., denoted as (iteration No.).

35 Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of assignment is indicated in square brackets like [assignment_value].

36 **Selection**

This is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

37 **Refinement**

This is used to add details and thus further restrict a requirement. The result of refinement is shown in **bold text**.

1.6 Terms and Definitions

38 **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.

39 **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.

40 **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.

41 **Web App**

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

42 **Native App**

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

43 **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.

44 **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.

45 DRM

46 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.

47 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.

48 DRM Packaging.

DRM packaging refers to a task of applying DRM to the app contents files. It applies DRM encryption to the app contents files, and attaches a DRM header in front of the encrypted data.

49 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.

50 CID

Content ID. This is the ID for identifying the contents by the app DRM. Each app has a unique CID and the corresponding DRM RO can be identified through this CID.

51 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.

52 RODB

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

53 Sandboxing

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

54 Smart TV User

Smart TV users use the smart TV in a legitimate way and use various smart TV services such as TV broadcast content, web surfing, SNS, and etc.

55 Rootfs

Rootfs refers to the kernel's root file system which composes the smart TV and it allows easier access to files or folders in the operating system.

56 LS2 API

LS2 API 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 API.

1.7 Acronyms

57	**AES**	Advanced Encryption Standard
58	**API**	Application Programming Interface
59	**CDN**	Content Delivery Network
60	**CEK**	Content Encryption Key
61	**CID**	Content ID
62	**DH**	Diffie-Hellman
63	**DRM**	Digital Rights Management
64	**IPK**	Itsy Package
65	**JSON**	JavaScript Object Notationc
66	**LS2**	Luna Service 2
67	**MAC**	Medium Access Control
68	**MVPD**	Multichannel Video Programming Distributor
69	**RO**	Rights Object
70	**RODB**	Rights Object Database
71	**RSA**	Rivest-Shamir-Adleman
72	**SHA**	Secure Hash Algorithm
73	**TLS**	Transport Layer Security
74	**URL**	Unified Resource Location

2 Conformance Claims

75 This chapter describes the Common Criteria (CC), Protection Profiles, and the Package that this Security Target conforms to.

2.1 CC Conformance Claim

76 This Security Target conforms to the following Common Criteria.:

■ Common Criteria Identification

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 4 (CCMB-2012-09-001, Sep, 2012)
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 4 (CCMB-2012-09-002, Sep, 2012)
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 4 (CCMB-2012-09-003, Sep, 2012)

■ Common Criteria Conformance

- Common Criteria for Information Technology Security Evaluation, Part 2 conformant
- Common Criteria for Information Technology Security Evaluation, Part 3 conformant

2.2 Conformance to Protection Profiles and Packages

77 This Security Target conforms to the following Protection Profiles and Packages.

2.1.1 Protection Profiles Conformance Claim

78 This Security Target does not claim conformance to PP..

2.1.2 Packages Conformance Claim

79 This Security Target claims conformance to assurance package EAL2.

2.3 Conformance Claim Rationale

80 Since this Security Target does not declare that it conforms to other Protection Profiles, the conformance rationale is not provided.

3 Security problem definition

81 This chapter defines the threats, OSPs (Organizational Security policies) and assumptions which are intended to be addressed by the TOE and its operational environment.

82 The assets covered in the Smart TV are as follows.

■ Assets in the webOS Smart TV

- The Smart TV assets
  The Smart TV assets are service executable binary files, libraries, configuration files, device files and etc that are provided on the smart TV, and an app installed on the smart TV can access the assets, if necessary.

- Apps
  Apps are stored in the app execution path (read-write file system), and it includes execution files, source files, and contents files of each app.

- TOE execution files and configuration files
  The TOE execution files and configuration files are included in the Smart TV asset.

■ The Data transmitted between the Smart TV and external entities

- Data transmitted between the Smart TV and LG App Store server
  The digital signature value of an app package file (IPK), app size information, URL for IPK downloading (CDN server), and DRM server URL information

- Data transmitted between the Smart TV and CDN server
  App package files (IPK)

- Data transmitted between the Smart TV and DRM server
  ROs (Right Object). The RO includes content data such as CID, CEK, and etc.

3.1 Threats

The threat agents are IT entities and users that adversely act on the assets through unauthorized access or using unusual methods, and may cause the following threats: The threat agents to the TOE have Basic attack potential of expertise, resources, and motivation.

T.UnauthorizedAppInstallation

The threat agents can install apps on a smart TV by disguising as a legitimate app through an illegal route.

T.ModifyingAppPackageFile

The threat agents can install a malicious app on the smart TV by intercepting the app installation data (app package file, file URL, size, RO data) which is being sent over the network and modifying the app installation data.

T.UnauthorizedAccessToSmartTVAssets

Apps installed on a smart TV can access the smart TV assets and execute adverse actions.

T.AppCopyrightInfringement

Infringement of app copyrights may occur by illegally copying and using the app's contents like source codes, assets, and using technologies illegally.

T.UnauthorizedAccessToOtherApp'sExecutionDomain

An app installed on a smart TV can make unauthorized access to other apps' execution domains so that it may cause an abnormal behavior.

3.2 Organizational Security Policies

83 The following describes the organizational security policies, which will be performed by the TOE, TOE operational environment, or both.

P.SecureKeyOperationManagement

The private key, which is used for app digital signatures, is generated by LG Electronics based on the RSA standard, and stored securely on the LG App Store server. The app CEK used for app DRM is generated uniquely per each app, and it is generated by LG Electronics, based on the AES standard, and stored securely on the DRM server. The generation, storage, access control, and destruction of the cryptographic keys, which are managed from the LG App Store server and DRM server are performed securely in accordance with LG Electronics regulations and policies. The RODB encryption Key is uniquely generated for each smart TV and are securely provisioned in smart TVs and stored in Secure Storage during mass

production.

P.SecureSmartTVUpdate

After shipping smart TVs, the smart TV software can be updated using the secure software update function. The software update image file is encrypted using AES cryptography algorithm and digitally signed using RSA-SHA256 algorithm, so that it is protected during being transferred via network or USB memory stick. The AES key for decrypting the software update image and RSA public key for digital signature verification are stored in the secure storage of the smart TV.

3.3 Assumptions

84 The following describes the assumptions that are made on the operational environment to provide security functionality.

A.SecureExternalITEntities

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

A.SmartTVAssetsModificationProtection

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.

A.TrustedDeveloper

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.

A.SmartTVUniqueIDRegistration

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.

4 Security Objectives

85 This Security Target classifies security objectives into 2 groups: security objectives for the TOE and security objectives for the operational environment. The security objectives for the TOE are those that are directly handled by the TOE, and the security objectives for the operational environment are those that must be addressed through the technical and procedural measures which are supported by the operational environment for the TOE to provide security functionality.

4.1 Security Objectives for the TOE

86 The following are security objectives that should be directly handled by the TOE.

O. AppPackageFileVerification

The TOE verifies that the app package file (IPK) to be installed on the smart TV is an authorized app package through digital signature verification and there is no unauthorized modification during downloading process.

O.AppContentsProtection

The TOE stores content files of installed app in an encrypted form on the smart TV, and when the app is executed, verifies its DRM license and decrypts the encrypted app content files.

O.AppAccessControl

The TOE shall control apps to prevent unauthorized access to other apps' execution domain or smart TV assets.

4.2 Security Objectives for the Operational Environment

87 This section describes security objectives which should be addressed by the non-technical/procedural measures that are supported by the operational environment for the TOE to accurately provide security functionality.

OE. SecureKeyOperationsManagement

The private key, which is used for app digital signatures, is generated by LG Electronics based on the RSA standard, and stored securely on the LG App Store server. The CEK used for encrypting app contents files is generated based on the AES standard by LG App Store server and stored securely on the DRM server. The generation, storage, access control, and destruction of the cryptographic keys, which are managed from the LG App Store server and DRM server are performed securely in accordance with LG Electronics regulations and policies. The RODB encryption key are uniquely generated for each smart TV and are securely provisioned in smart TVs and stored in Secure Storage during mass production.

OE.SecureSmartTVUpdate

After shipment of smart TVs, the smart TV software which includes the TOE is updated through network service update (NSU), TV firmware update via broadcasting signal (OTA), or USB update by customer service center. The software update file (smart TV software image) is encrypted by AES, digitally signed based on RSA-SHA256, sent and downloaded in the smart TV, and securely updated through digital signature verification using a key stored in Secure Storage and decryption.

OE.SecureExternalITEntity

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

OE.SecureCommunicationChannel

A secure communication channel is provided for communication between the Smart TV and the LG App Store server based on TLS v1.2.

OE.ProtectModifyingSmartTVResource

All system service binaries and library files contained within the smart TV firmware are installed in the read-only file system to be protected from unauthorized modification attempts.

OE.TrustedDeveloper

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 smart TV services.

OE.SmartTVUniqueIDRegistration

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.

4.3 Security Objectives Rationale

88 The security objectives rationale demonstrates that the specified security objectives are adequate, sufficient to address security problems, not too excessive, and must be required.

89 The security objectives rationale demonstrates the following:

- Each threat, organizational security policies, and assumption is addressed by at least one security objective.

- Each security objective addresses at least one threat, organizational security policies, or assumption.

Table 4. Security problems and Security Objectives

	TOE Security Objectives			**Security Objectives for Operational Environment**						
	O.AppPackageFileVerification	O.AppContentsProtection	O.AppAccessControl	OE.SecureKeyOperationsManagement	OE.SecureSmartTVUpdate	OE.SecureExternalITEntity	OE.SecureCommunicationChannel	OE.ProtectModifyingSmartTVResource	OE.TrustedDeveloper	OE.SmartTVUniqueIDRegistration
T.UnauthorizedAppInstallation	X									
T.ModifyingAppPackageFile	X						X			
T.UnauthorizedAccessToSmartTVAssets			X							
T.AppCopyrightInfringement		X								

T.UnauthorizedAccessToOtherApp'sExecutionDomain			X							
P.SecureKeyOperationManagement				X						
P.SecureSmartTVUpdate					X					
A.SecureExternalITEntities						X				
A.SmartTVAssetsModificationProtection								X		
A.TrustedDeveloper									X	
A.SmartTVUniqueIDRegistration										X

4.3.1 The Security Objectives Rationale of the TOE

90 O.AppPackageFileVerification

This security objective ensures the origin authentication of the apps through the digital signature verification on the app package file to be installed on the smart TV by the TOE, which enables preventing the threat T.UnauthorizedAppInstallation. As it also ensures that app package file is not tampered, it addresses the threat T.ModifyingAppPackageFile.

91 O.AppContentsProtection

This security objective addresses the threat T.AppCopyrightInfringement by preventing the unauthorized use such as illegal copying by encrypting and storing files of the apps installed on the smart TV.

92 O.AppAccessControl

The TOE controls apps from accessing unauthorized domains such as other apps' execution domains or smart TV assets so as to address the threat of T.UnauthorizedAccessToSmartTVAssets and T.UnauthorizedAccessToOtherApp'sExecutionDomain.

4.3.2 The Security Objectives Rationale of the Operational Environment

93 OE.SecureKeyOperationsManagement

This security objective for operational environment executes OSP (organizational security policy), P.SecureKeyOperationManagement by performing the following. The

private key for generation of app digital signature is generated by LG Electronics based on the RSA standard, and stored securely on the LG App Store server. The App DRM CEK used for encrypting the app content files is generated based on the AES standard by LG Electronics and stored securely on the DRM server. The generation, storage, access control, and destruction of the cryptographic keys, which are managed from the LG App Store server and DRM server are performed securely in accordance with LG Electronics regulations and policies.

94 OE.SecureSmartTVUpdate

This security objective for operational environment executes organizational security policy, P.SecureSmartTVUpdate by executing the following. After shipping smart TVs, the smart TV software can be updated using the secure software update function. The software update image file is encrypted using AES cryptography algorithm and digitally signed using RSA-SHA256 algorithm, so that it is protected during being transferred via network or USB memory stick. The AES key for decrypting the software update image and RSA public key for digital signature verification are stored in the secure storage of the smart TV.

95 OE.SecureExternalITEntity

This security objective for operational environment supports the assumption A.SecureExternalITEntities by executing the following. For secure operation of the TOE, LG App Store server, CDN server, and DRM server which exist in the operational environment are operated securely.

96 OE.SecureCommunicationChannel

This security objective for operational environment addresses Threat T.ModifyingAppPackageFile by executing the following. SDX, which is the external entity within the smart TV, provides a secure communication channel between the smart TV and LG App Store server based on TLS v1.2.

97 OE.ProtectModifyingSmartTVResource

This security objective for operational environment supports the assumption A.SmartTVAssetsModificationProtection by executing the following. All system service binaries and library files included in the smart TV firmware are installed in the read-only file system to be protected from unauthorized modification attempts.

98 OE.TrustedDeveloper

This security objective for operational environment supports the assumption A.TrustedDeveloper by executing the following. 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.

99 OE.SmartTVUniqueIDRegistration

This security objective for operational environment supports the assumption A.SmartTVUniqueIDRegistration by executing the following. LG Electronics must assign unique MAC addresses to each smart TV in order to manage securely. This MAC address should be unique because it is used to identify the smart TV device uniquely in LG App Store server.

5 Extended components definition

100 This Security Target does not include any extended components that are extended from the Common Criteria (CC) Part 2 or Part 3.

6 Security Requirements

101 This chapter describes security functional requirements and security assurance requirements which should be satisfied in the TOE.

6.1 Security Functional Requirements

102 The security functional requirements defined in this Security Target are based on the functional requirements in Part 2 of the Common Criteria.

103 Table 5 shows the Subject/Object, security attributes, and operations that are used for SFR

Table 5. SFR Subject / Object, Security Attribute, Operation

SFR	Subject	Subject Security Attribute	Object	Object Security Attribute	Operation
FDP_ACC.1(1) **FDP_ACF.1(1)**	Smart TV User	N/A	App Package File	Digital Signature	Install app on Smart TV
FDP_ACC.1(2) **FDP_ACF.1(2)**	Smart TV User	RO Data	Web App Content	CID of App DRM package Header	Decrypt App DRM encrypted App files to execute an app
FDP_ACC.1(3) **FDP_ACF.1(3)**	Native App	App Type, privilegedJail	App Execution Domain	Access right (permission)	Read, Write, Execute
FDP_ACC.1(4) **FDP_ACF.1(4)**	Web App	App Trust Level	Smart TV Resource (LS2 API, Local File)	API type (Public API, Private API), File type	API Call, File Read

104 Table 6 shows the security attribute of the native app and web app.

Table 6. Native App, Web App Security Attribute

Subject	type/trust level	Description
Native App	Native	Normal native type app.
	Native_builtin	In-house prebuilt native app.

	Native_mvpd	Native app that is developed by MVPD or partner
Web App	default	Default permission level for normal web type app.
	netcast	Web app that is compatible to NetCast platform.
	trusted	Top-level trust level that is assigned to the web app that is developed by LG itself or partners.

Table 7. Object and Operation according to Native App type and Web App trust level

subject	type/trust level	Object	Operation
Native App	Native	App Execution Domain, Smart TV Resource	read, write, execute
	Native_builtin		
	Native_mvpd		
Web App	default	LS2 API Local File	API call File read
	netcast		
	trusted		

105 Table 8 shows the object security attribute for app execution domain and smart TV resource.

Table 8. Object Security Attribute

Object		Access Permission / type	Description
App Execution Domain		Access permission to app execution domain	Permission to access the app's home directory or jail root directory
Smart TV Resource	LS2 API	public	Public APIs that are published via SDK for non-LG developers
		private	Unpublished Private APIs (LG Internal APIs)
	Local File	Local File	Whole files in webOS rootfs file system.
		White List File	Files that are allowed for Web App to access with a 'read' permission.

106 Table 9 shows the key, subject generating the keys, repository.

Table 9 Keys for TOE Operation

TSF	Key	Generator Subject	Repository
App Installation Protection	Digital Signature Signing Key (Private Key)	External IT Entity (LG App Store)	External IT Entity (LG App Store Server)
	Digital Signature Verifying Key (Public Key)		Smart TV (Read-Only File System)
App Content Protection	DH Session Key	external IT Entity (DRM Server) and	N/A (used only in RAM)

		TOE	
	CEK (Content Encryption Key)	External IT Entity (DRM Server)	RODB in Smart TV (Read-Write File System)
	RODB Encryption Key	External Entiry inside Smart TV	Smart TV (Read-Only File System)

107 Table 10 shows the security functional requirements that are used in this Security Target document.

Table 10. Security Functional Requirements

Index	Security Functional Class	Security Functional Components
1	Cryptographic Support (FCS)	FCS_CKM.2 Cryptographic key distribution
2		FCS_CKM.4 Cryptographic key destruction
3		FCS_COP.1(1) Cryptographic Operation(1)
4		FCS_COP.1(2) Cryptographic Operation(2)
5		FCS_COP.1(3) Cryptographic Operation(3)
6	User Data Protection (FDP)	FDP_ACC.1(1) Subset Access Control(1)
7		FDP_ACC.1(2) Subset Access Control(2)
8		FDP_ACC.1(3) Subset Access Control(3)
9		FDP_ACC.1(4) Subset Access Control(4)
10		FDP_ACF.1(1) Access Control Functions(1)
11		FDP_ACF.1(2) Access Control Functions(2)
12		FDP_ACF.1(3) Access Control Functions(3)
13		FDP_ACF.1(3) Access Control Functions(3)
14	TRUSTED PATH/CHANNELS (FTP)	FTP_ITC.1 Inter-TSF trusted channel

6.1.1 Cryptographic Support (FCS)

108 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

109 FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Diffie-Hellman Key agreement mechanism] that meets the following: [PKCS#3 DIFFIE-HELLMAN KEY AGREEMENT STANDARD].

110 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [Table 11. Cryptographic Key Destruction Method] that meets the following: [None]

Table 11. Cryptographic Key Destruction Method

Key	Location	Destruction Method
Digital Signature Verifying Key (Public Key)	RAM	Overwrite it with random data and overwrite it again with zero
DH Session Key	RAM	Overwrite it with random data and overwrite it again with zero
CEK	RAM	Overwrite it with random data and overwrite it again with zero
RODB Encryption Key	RAM	Overwrite it with random data and overwrite it again with zero

Application note : Generation, distribution and destruction of Cryptographic key and cryptographic operation are performed on TOE and operational environment.

TSF	**App Installation Protection**	**App Content Protection**		
Encryption Key / SFR	Digital Signature Verifying Key (Public Key)	DH Session Key	RODB Encryption Key	CEK
FCS_CKM.1	N/A (OE.SecureKeyOperationsManagement)	N/A (Generated by DH Key	N/A (OE.SecureKeyOperationsManagement)	N/A (OE.SecureKeyOperationsManagement)

		agreement)		
FCS_CKM.2	N/A (Included in Smart TV Firmware)	O	N/A (Included in Smart TV Firmware)	N/A (Included in RO and RO is encrypted with DH Session Key)
FCS_CKM.4	O	O	O	O
FCS_COP.1	O (FCS_COP.1(3))	O (FCS_COP.1(2))	O (FCS_COP.1(2))	O (FCS_COP.1(1))

111 FCS_COP.1(1) Cryptographic operation(1)

Hierarchical to: No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [decryption of App DRM encrypted content file] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bits] that meet the following: [NIST FIPS-197 ADVANCED ENCRYPTION STANDARD (AES)].

112 FCS_COP.1(2) Cryptographic operation(2)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [RO and RODB Encryption / Decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bits] that meet the following: [NIST FIPS-197 ADVANCED ENCRYPTION STANDARD (AES)].

Application note : TOE downloads an encrypted RO data from DRM server via FTP_ITC.1, decrypt the RO data using a shared key which is distributed by FCS_CKM.2, and write the RO data into RODB and encrypt the whole RODB. TOE decrypts RODB and retrieves CEK for the cryptographic operation FCS_COP.1(1) when launching an app.

113 FCS_COP.1(3) Cryptographic operation(3)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [verification of App Digital Signature] in accordance with a specified cryptographic algorithm [RSA-SHA256] and cryptographic key sizes [1024bits] that meet the following: [PKCS #1 V2.1: RSA CRYPTOGRAPHY STANDARD].

6.1.2 User Data Protection (FDP)

114 FDP_ACC.1(1) Subset access control(1)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [App Installation Protection Policy] on [Following list of subjects, objects, and operations].

a) Subject: Smart TV User

b) Object: App Package File

c) Operation: Install app on Smart TV

115 FDP_ACC.1(2) Subset access control(2)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [App Content Protection Policy] on [Following list of subjects, objects, and operations].

a) Subject: Smart TV User

b) Object: Web App Content

c) Operation: Decrypt App DRM encrypted App files to execute an app

116 FDP_ACC.1(3) Subset access control(3)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Native App Execution Protection Policy] on [Following list of subjects, objects, and operations].

a) Subject: Native App

b) Object: App Execution Domain

c) Operation: Read, Write, Execute

117 FDP_ACC.1(4) Subset access control(4)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [Web App Execution Protection Policy] on [Following list of subjects, objects, and operations].

a) Subject: Web App

b) Object: Smart TV Resource (LS2 API, Local File)

c) Operation: API Call, File Read

118 FDP_ACF.1(1) Security attribute based access control(1)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [App Installation Protection Policy] to Objects based on the following: :

[

a) subject: Smart TV User

b) Object: App Package File

c) Subject Security Attribute: N/A

d) Object Security Attribute: Digital Signature]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) App installation is allowed if App Digital Signature Verifying is successful

b) App installation is denied if App Digital Signature Verifying is failed]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [N/A]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [N/A]

119 FDP_ACF.1(2) Security attribute based access control(2)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [App Content Protection Policy] to Objects based on the following:

[

a) Subject: Smart TV User

b) Subject Security Attribute: RO Data

c) Object: Web App Content

d) Object Security Attribute: CID of App DRM package Header]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) If the RODB has a RO of which the CID is same to the CID in the app's DRM packaging header, decrypt the app content and execute the app.

b) If there is no RO which has the CID which is same to the CID in app's DRM packaging header, the app content cannot be decrypted and app execution is denied.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [N/A]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [N/A]

120 FDP_ACF.1(3) Security attribute based access control(3)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Native App Execution Protection Policy] to Objects based on the following:

[

a) Subject: Native App

b) Subject Security Attribute: App type, privilegedJail

c) Object: App Execution Domain

d) Object Security Attribute: Access right (permission)]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) If an app type is 'native', the app is executed in a jail environment (jail root file system) that is constructed using the jail conf file

"jailer_native.conf".

b) If an app type is 'native_builtin', the app is executed in a jail environment (jail root file system) that is constructed using the jail conf file "jailer_native_builtin.conf".

c) If an app type is 'native' and the value of 'privilegedJail' property is true (or an app type is 'native_mvpd'), the app is executed in a jail environment (jail root file system) that is constructed using the jail conf file "jailer_native_mvpd.conf"]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [N/A]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [N/A]

Application note: 'jailer_native_builtin.conf, jailer_native_mvpd.conf, and jailer_native.conf' are the jail conf files that define the jail configurations suitable for each native type. Constructing jail environment means to construct an app's own jail root file system according to the jailer configurations.

121 FDP_ACF.1(4) Security attribute based access control(4)

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [Web App Execution Protection Policy] to Objects based on the following:

[

a) Subject: Web App

b) Subject Security Attribute: App Trust Level

c) Object: Smart TV Resource (LS2 API, Local File)

d) Object Security Attribute: API type (Public API, Private API), File type]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation

among controlled subjects and controlled objects is allowed: [

a) If the trust level of a web app is 'default', calling LS2 public API is allowed to the app, but private API is denied.
Read operation is allowed to only files that are defined in whitelist, and denied to the other files that are not defined in whitelist.

b) If the trust level of a web app is 'netcast', read operation is allowed to only files that are defined in whitelist.

c) If the trust level of web app is 'trusted', calling both LS2 public and private APIs are allowed. It is allowed to read whole smart TV files.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [N/A]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [N/A]

6.1.3 Inter-TSF trusted channel (FTP)

122 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [RO download for App content protection function].

6.2 Security Assurance Requirements

123 Security assurance requirements (SAR) defined in this document consists of assurance component in Common Criteria for Information Technology Security Evaluation, Part 3. The Evaluation Assurance Levels (EALs) is EAL2. Table 12 shows the summary of the security assurance requirements.

Table 12. Security Assurance Requirements

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.2.1 Security Target evaluation

124 ASE_INT.1 ST introduction

Dependencies: No dependencies

Developer action elements

125 ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

126 ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

127 ASE_INT.1.2C The ST reference shall uniquely identify the ST.

128 ASE_INT.1.3C The TOE reference shall identify the TOE.

129 ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

130 ASE_INT.1.5C The TOE overview shall identify the TOE type.

131 ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

132 ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

133 ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

134 ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

135 ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

136 ASE_CCL.1 Conformance claims

Dependencies:

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

137 ASE_CCL.1.1D The developer shall provide a conformance claim.

138 ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

139 ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

140 ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

141 ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

142 ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

143 ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

144 ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

145 ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

146 ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement

of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

147 ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

148 ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

149 ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

150 ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

151 ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

152 ASE_SPD.1.1C The security problem definition shall describe the threats.

153 ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

154 ASE_SPD.1.3C The security problem definition shall describe the OSPs.

155 ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

156 ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

157 ASE_OBJ.2 Security objectives

Dependencies:

ASE_SPD.1 Security problem definition

Developer action elements:

158 ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

159 ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

160 ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

161 ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

162 ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

163 ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

164 ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

165 ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

166 ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

167 ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

168 ASE_ECD.1.1D The developer shall provide a statement of security requirements.

169 ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

170 ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

171 ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

172 ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

173 ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

174 ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

175 ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all

requirements for content and presentation of evidence.

176 ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

177 ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

178 ASE_REQ.2.1D The developer shall provide a statement of security requirements.

179 ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

180 ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

181 ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

182 ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

183 ASE_REQ.2.4C All operations shall be performed correctly.

184 ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

185 ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

186 ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

187 ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

188 ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

189 Evaluator action elements:

190 ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

191 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

192 ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

193 ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

194 ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

195 ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development

196 **ADV_ARC.1 Security architecture description**

Dependencies: ADV_FSP.1 Basic functional specification

197 ADV_TDS.1 Basic design

Developer action elements:

198 ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

199 ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

200 ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

201 ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

202 ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

203 ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

204 ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

205 ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

206 ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

207 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

208 ADV_FSP.2.1D The developer shall provide a functional specification.

209 ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

210 ADV_FSP.2.1C The functional specification shall completely represent the TSF.

211 ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

212 ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

213 ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

214 ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

215 ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

216 ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

217 ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

218 ADV_TDS.1 Basic design

219 Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

220 ADV_TDS.1.1D The developer shall provide the design of the TOE.

221 ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

222 ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

223 ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

224 ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

225 ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR enforcing subsystems.

226 ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

227 ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

228 ADV_TDS.1.1EThe evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

229 ADV_TDS.1.2EThe evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance documents

230 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

231 AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

232 AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

233 AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

234 AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

235 AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

236 AGD_OPE.1.5C The operational user guidance shall identify all possible modes of

operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

237 AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

238 AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

239 AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

240 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

241 AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

242 AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

243 AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

244 AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

245 AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Life-cycle support

246 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

247 ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

248 ALC_CMC.2.2D The developer shall provide the CM documentation.

249 ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

250 ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

251 ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

252 ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

253 Evaluator action elements:

254 ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

255 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

256 ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

257 Content and presentation elements:

258 ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

259 ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

260 ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

261 ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

262 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

263 ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

264 ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

265 ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

266 ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Tests

267 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification,

ATE_FUN.1 Functional testing

Developer action elements:

268 ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

269 ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

270 ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

271 ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

272 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

273 ATE_FUN.1.1D The developer shall test the TSF and document the results.

274 ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

275 ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

276 ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the

scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

277 ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

278 ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

279 ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

280 **ATE_IND.2 Independent testing - sample**

Dependencies: ADV_FSP.2 Security-enforcing functional specification,

AGD_OPE.1 Operational user guidance,

AGD_PRE.1 Preparative procedures,

ATE_COV.1 Evidence of coverage,

ATE_FUN.1 Functional testing

Developer action elements:

281 ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

282 ATE_IND.2.1C The TOE shall be suitable for testing.

283 ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

284 ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

285 ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation

to verify the developer test results.

286 ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

287 **AVA_VAN.2 Vulnerability analysis**

Dependencies: ADV_ARC.1 Security architecture description,

ADV_FSP.2 Security-enforcing functional specification,

ADV_TDS.1 Basic design,

AGD_OPE.1 Operational user guidance,

AGD_PRE.1 Preparative procedures

Developer action elements:

288 AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

289 AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

290 AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

291 AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

292 AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

293 AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Security Requirements Rationale

294 Security Requirements Rationale demonstrates that the described security requirements are suitable to satisfy security objectives and, as a result, appropriate to address security problems.

6.3.1 Security Functional Requirements Rationale

295 Rationale of security functional requirements demonstrates the followings.

296 Each TOE security objective has at least one security functional requirement tracing to it.

297 Each TOE security functional requirement traces back to at least one TOE security objectives.

Table 13. Summary of Mappings between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	O.AppPackageFileVerification	O.AppContentsProtection	O.AppAccessControl
FDS_CKM.2		X	
FCS_CKM.4	X	X	
FCS_COP.1(1)		X	
FCS_COP.1(2)		X	
FCS_COP.1(3)	X		
FDP_ACC.1(1)	X		
FDP_ACC.1(2)		X	
FDP_ACC.1(3)			X
FDP_ACC.1(4)			X
FDP_ACF.1(1)	X		
FDP_ACF.1(2)		X	
FDP_ACF.1(3)			X
FDP_ACF.1(4)			X
FTP_ITC.1		X	

298 **FCS_CKM.2 Cryptographic key distribution**

This component satisfies the TOE security objective O.AppContentsProtection because the session key to be used for secure download of a RO which is used for the app content protection function is distributed.

299 **FCS_CKM.4 Cryptographic key Destruction**

This component satisfies the TOE security objective O.AppPackageFileVerification because the digital signature verification key (public key) which is used for the app installation protection function is destructed securely.

This component also satisfies the TOE security objective O.AppContentsProtection because a DH session key, a CEK, and a RODB encryption key which are used for the app content protection function are destructed securely.

300 **FCS_COP.1(1) Cryptographic Operation(1)**

This component satisfies the TOE security objective O.AppContentProtection because the encrypted app content files can be decrypted (AES 128bits) only if the DRM validation check is OK.

301 **FCS_COP.1(2) Cryptographic Operation(2)**

This component satisfies the TOE security objective O.AppContentProtection because it decrypts the encrypted RO data, which is used for the app content protection function, using the DH session key after downloading the RO from DRM server. In addition, it encrypts RODB after adding a new RO and decrypts RODB to retrieve a CEK.

302 **FCS_COP.1(3) Cryptographic Operation(3)**

This component satisfies the TOE security objective O.AppPackageFileVerification because it performs the digital signature verification (RSA-SHA256) for the app package file before installing the app on the smart TV.

303 **FDP_ACC.1(1) Subset access control(1)**

This component satisfies the TOE security objective O.AppPackageFileVerification because it ensures access control to the app package file when a smart TV user installs an app.

304 **FDP_ACC.1(2) Subset access control(2)**

This component satisfies the TOE security objective O.AppContentProtection because it ensures access control to the app content when a smart TV user executes an app.

305 **FDP_ACC.1(3) Subset access control(3)**

This component satisfies the TOE security objective O.AppAccessCpontrol because it ensures access control to app execution domain.

306 **FDP_ACC.1(4) Subset access control(4)**

This component satisfies the TOE security objective O.AppAccessControl because it ensures access control to the APIs that the web app can use and and the file path which the web app can access to.

307 **FDP_ACF.1(1) Security attribute based access control(1)**

This component satisfies the TOE security objective O.AppPackageFileVerification because it ensures access control to app installation by the digital signature verification. If the digital signature verification is successful, the app installation requested by a smart TV user is allowed, but it is failed the app installation is denied.

308 **FDP_ACF.1(2) Security attribute based access control(2)**

This component satisfies the TOE security objective O.AppContentProtection because it ensures access control to decrypt the app content files, that are encrypted by DRM, according to the result of DRM validation check. When a smart TV user executes an app, the DRM validation check is performed by checking if there is a correspond RO in the RODB. If there is a RO of which the CID is identical to the CID retrieved from the app's DRM package header.

309 **FDP_ACF.1(3) Security attribute based access control(3)**

This component satisfies the TOE security objective O.AppAccessControl because it ensures access control to the app execution domain according to the app's security attribute (type, privilegedJail) when the native app is executed.

310 **FDP_ACF.1(4) Security attribute based access control(4)**

This component satisfies the TOE security objective O.AppAccessControl because it ensures access control to the APIs which are usable and the file path which are accessable by the web App according to the app security attribute (TrustLevel) when the web app is executed.

311 **FTP_ITC.1 Inter-TSF trusted channel**

This component satisfies the TOE security objective O.AppContentProtection because it provides the secure communication channel to download RO data, which is used for the app content protection function, from the DRM server.

6.3.2 Security Assurance Requirements Rationale

312 The security assurance level of this Security Target was selected as EAL2 in consideration of the value and threat level of the assets protected by the TOE.

313 EAL2 requires only the effort to submit design information and test results to the extent that developers are dealing with robust commercial methodologies.

314 EAL2 is applicable when all development records are not readily available and when developers or users need low to medium levels of independently assured security.

315 EAL2 provides assurance by analyzing the security functional requirements contained in the complete ST using the functional and interface specifications, documentation, and basic descriptions of the TOE structure to understand the security behavior. This analysis demonstrates the independent testing of the TSF, the proof of the tests performed by the developer based on the functional specification, the independent verification of the developer's sample of the test results, and the immunity from the attacker's penetration attack with the basic attack potential (Based on the provided functional specification, TOE design, structural design, and documentation evidence).

316 EAL2 provides assurance through the proof of configuration management system and secure distribution procedures.

317 In addition, in order to respond to vulnerability analysis attacks, AVA_VAN.2, vulnerability analysis is requested, and the penetration test is performed by the evaluator to confirm that the potential vulnerability cannot be exploited in the TOE operational environment. The evaluator assumes basic attack potential and performs penetration testing.

6.4 Security requirements rationale

318 Rationale of dependency is demonstrated by dependency of security functional requirements and dependency of security assurance requirements.

6.4.1 Dependency rationale of Security Functional Requirements

319 Table 14 shows dependencies of security functional requirements.

Table 14. Dependencies rationale of Functional Components for the TOE

No.	Functional Components	Dependencies	Ref. No.
1	FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	*Rational 2
2	FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	*Rational *OE.SecureKeyOperationsManagement
3	FCS_COP.1(1)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	*OE.SecureKeyOperationsManagement 2
4	FCS_COP.1(2)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security	*Rational

		attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	2
5	FCS_COP.1(3)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	*OE.SecureKeyOperationsManagement *Rational
6	FDP_ACC.1(1)	FDP_ACF.1 Security attribute based access control	10
7	FDP_ACC.1(2)	FDP_ACF.1 Security attribute based access control	11
8	FDP_ACC.1(3)	FDP_ACF.1 Security attribute based access control	12
9	FDP_ACC.1(4)	FDP_ACF.1 Security attribute based access control	13
10	FDP_ACF.1(1)	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	6 Rational
11	FDP_ACF.1(2)	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	7 Rational
12	FDP_ACF.1(3)	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	8 Rational
13	FDP_ACF.1(4)	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	9 Rational
14	FTP_ITC.1	N/A	N/A

320 FCS_CKM.2 has a dependency on FCS_CKM.1 but the key used for decrypting RO data which is downloaded from DRM server is generated through the DH key agreement by FCS_CKM.2, so a dependency is not required.

321 FCS_CKM.4 has a dependency on FCS_CKM.1 but each cryptography key doesn't require dependency as following:

- The DH session key used for decrypting RO data which is downloaded from DRM server is generated through the DH key agreement by FCS_CKM.2

- The RODB encryption key used for encrypting and decrypting of RODB is provisioned securely into webOS Smart TV firmware after being generated uniquely. The provisioned key is stored in the secure storage. It is also described in

OE.SecureKeyOperationsManagement.

- The CEK, which is used for decryption of the DRM encrypted app content files, is generated based on AES standard from LG Electronics. It is also described in OE.SecureKeyOperationsManagement.

- The RSA public key which is used for the app digital signature verification is generated based on RSA standard from LG Electronics. It is also described in OE.SecureKeyOperationsManagement.

322 FCS_COP.1(1) has a dependency on FCS_CKM.1 but the CEK, which is used for decryption of the DRM encrypted app content files, is generated based on AES standard from LG Electronics and it is described in OE.SecureKeyOperationsManagement. Therefore the dependency of FCS_COP.1(1) is satisfied by replacement with the security objective of operational environment OE.SecureKeyOperationsManagement.

323 FCS_COP.1(2) has a dependency on FCS_CKM.1 but the DH session key used for decrypting RO data which is downloaded from DRM server is generated through the DH key agreement by FCS_CKM.2 therefore dependency is not required, and also the RODB encryption key is provisioned securely into webOS Smart TV firmware after being generated uniquely, and stored in the secure storage of webOS Smart TV, and is described in OE. SecureKeyOperationsManagement.

324 FCS_COP.1(3) has a dependency on FCS_CKM.1 but the RSA public key which is used for the app digital signature verification is generated based on RSA standard from LG Electronics, and is also described in OE.SecureKeyOperationsManagement. Therefore the dependency of FCS_COP.1(3) is satisfied by replacement with the security objective of operational environment OE.SecureKeyOperationsManagement.

325 FCS_COP.1(3) has a dependency on FCS_CKM.4 but the RSA public key which is used for the app digital signature verification is distributed being stored in the read-only filesystem area of a smart TV firmware. In addition, a fixed key is used according to Smart TV service operational feature, so cryptographic key destruction feature is not required. Therefore this dependency is not required.

326 FDP_ACF.1(1), FDP_ACF.1(2), FDP_ACF.1(3), and FDP_ACF.1(4) have a dependency on FMT_MSA.3 but no security management function is required because the all security attributes configurations are delivered being included in read-only configuration files in the smart TV firmware and they never be changed.

6.4.2 Dependency rationale of Security Assurance

Requirements

327 The dependency of each assurance package provided in the CC has already satisfied.

7 TOE summary specification

328 This section summarizes security functions provided by TOE in terms of how they satisfy the security functional requirements.

329 The TOE security functions are categorized into the app installation protection, app execution protection, app content protection. Following sections describe how each TOE security function satisfies the security functional requirements which are described in the section 6 Security Requirements.

7.1 App Installation Protection

330 TOE performs digital signature verification for the app package file which was downloaded during installation process in order to install only the authorized apps.

331 When a smart TV user requests to install an app through LG Content Store, the TOE requests the app installation file to the LG App Store server and receives the URL of CDN server from which the app installation file can be downloaded from LG App Store Server. The TOE downloads the app package file (IPK) from the CDN server and performs Digital Signature verification. TOE supports RSA-SHA256 cryptographic algorithm based on PKCS#1 V2.1: RSA CRYPTOGRAPHY STANDARD. The digital signature verification key(public key) is stored in the "read-only" filesystem so that the file cannot be tampered with or deleted. When the signature verification is done, the public key loaded in RAM is overwritten with an arbitrary value generated randomly and again overwritten with zero to destruct it securely'.

332 The TOE installs the app only if the digital signature verification is successful and does not install the app if the signature verification fails

Related SFRs: FCS_COP.1(3), FCS_CKM.4, FDP_ACC.1(1), FDP_ACF.1(1), FTP_ITC.1

7.2 App Execution Protection

333 When executing apps, the TOE provides execution protection function according to the protection policy depending on the app type whether it's a web app or a native app. The attribute information for identifying the app type exists as a "type" attribute in the appinfo.json file from an app installation file.

334 The TOE identifies app properties, 'type' and 'privilegedJail', for native apps, from the appinfo.json file of the app, to configure an appropriate sandboxed jailer execution environment where execution domains will be separated for each app to prevent unauthorized access to other apps' execution domains. The TOE constructs the separate root filesystem in which native apps are executed separately, and restricts the privilege for app execution to a regular user (non-root user) only so that apps cannot access unauthorized main system directories or device files of the smart TV.

335 The TOE restricts the accessible API and file system in the smart TV according to the permissions policy per web app trust level by identifying the attribute information of web apps. The trust level information of the web app exists as a 'trustlevel' attribute in the appinfo.json file, and is set to one out of three options from default, netcast, and trusted. The web app of which trust level is the 'default' level is allowed to use only LS2 public API and to access only file paths defined in the whitelist with a 'read' right. The web app of which trust level is the 'netcast' level is not allowed to used LS2 APIs but allowed to access file paths defined in the whitelist with a 'read' right. The web app of which the trust level is the 'trusted' level is allowed to use all LS2 API (both public and private APIs) and also to access all file paths with a 'read' right in the webOS smart TV.

Related SFRs: FDP_ACC.1(3), FDP_ACC.1(4), FDP_ACF.1(3), FDP_ACF.1(4)

7.3 App Content Protection

336 The TOE checks the DRM packaging when the app is executed, and provides the app contents protection so that only the DRM-packaged apps can be normally executed in the LG App Store server. If the DRM verification is successful, it decrypts and executes the contents of the application, and if the DRM verification fails, the application is not executed.

337 The TOE securely generates and distributes a session key, which is for encryption of the RO request message and decryption of the RO response message, based on the DH algorithm in order to securely download the ROs (rights objects) which include license data and CEK from the DRM server. With the session key, TOE encrypts a RO request message and decrypts a RO response message.

338 The TOE encrypts ROs using the RO encryption key, stores them in the RODB, and decrypts them only within the RAM for use.

339 When executing a web app, the TOE decrypts the app contents files (html, js, css, etc) that are encrypted by DRM. The app contents files are always stored being encrypted

in the app installation directory and are decrypted using CEK only when they are loaded in RAM by the TOE. CEK is a unique key per each app and it is created when the app is uploaded on the LG App Store server which is an external entity outside of the smart TV, and is stored securely on LG DRM server which is an external entity outside of the smart TV.

340 The TOE provides a function for secure key destruction. CEK and RODB encryption key data are removed securely from RAM after using. The TOE also provides a function to securely remove the session key used when installing apps for encryption of RO data from the memory. The TOE provides a function to remove securely DRM license and CEK data from the RODB file when deleting apps.

Related SFRs: FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FDP_ACC.1(2), FDP_ACF.1(2) , FTP_ITC.1