KECS-CR-16-60

Samsung Smart TV Security Solution V1.0

Certification Report

Certification No.: KECS-CISS-0741-2016

2016. 8. 30

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2016.8.30	-	Certification report for Samsung Smart TV Security Solution V1.0 - First documentation

This document is the certification report for Samsung Smart TV Security Solution V1.0 of SAMSUNG ELECTRONICS Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory (KSEL)

Table of Contents

1. Executive Summary 5

2. Identification 7

3. Security Policy 9

4. Assumptions and Clarification of Scope 9

5. Architectural Information 10

5.1 Physical Scope of TOE 10

5.2 Logical Scope of TOE 11

6. Documentation 14

7. TOE Testing 14

8. Evaluated Configuration 15

9. Results of the Evaluation 15

9.1 Security Target Evaluation (ASE) 16

9.2 Life Cycle Support Evaluation (ALC) 16

9.3 Guidance Documents Evaluation (AGD) 17

9.4 Development Evaluation (ADV) 17

9.5 Test Evaluation (ATE) 18

9.6 Vulnerability Assessment (AVA) 18

9.7 Evaluation Result Summary 19

10. Recommendations 20

11. Evaluation Evidence 21

12. Acronyms and Glossary 22

13. Bibliography 24

1. Executive Summary

This report describes the result of the EAL1 evaluation of Samsung Smart TV Security Solution V1.0 from SAMSUNG ELECTRONICS Co., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation ("CC" hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on August 16, 2016. This report grounds on the evaluation technical report ("ETR" hereinafter)[3] and the Security Target ("ST" hereinafter)[4]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based only upon functional components in CC Part 2, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

The Target of Evaluation ("TOE" hereinafter) is a Smart TV Security Solution that provides security functions in the form of library by being embedded on Samsung Smart TV. The TOE provides functions for the secure operation of Samsung Smart TV with system(kernel of Tizen OS) integrity verification, blocking the execution of unauthorized Web App, and blocking access to phishing sites. In addition, the TOE also provides encryption/decryption function for data used in Web App, and updating the database for the list of phishing sites by communicating with Update Server. The TOE is distributed to the developers of Samsung Smart TV in the form of a library which is a kind of software, and is not in charge of all kinds of security functions provided in Samsung Smart TV. The TOE provides only the security function defined in the above.

The TOE is a library included in the firmware of Samsung Smart TV, and performs the role of being in charge of security function of Samsung Smart TV. The TOE allows a secure web surfing of a Samsung Smart TV User who accesses a web site using Web Browser by providing Phishing Site Blocking function. In addition, by blocking the execution of unauthorized Web App, the TOE prevents the execution of an unauthorized Web App from accessing the resource of Samsung Smart TV. Important data used in Web App are stored securely with encryption. With System Integrity Monitoring function, the verification on the integrity of the system(kernel of Tizen OS) is performed to guarantee secure operation of Samsung Smart TV. The TOE communicates with an external IT entity. Communication with external IT entity can be done in the form of a wired communication using Ethernet and a wireless communication using Wi-Fi. Google Safe Browsing server and Update server are external IT entities which communicate with Phishing Site Blocking function. TOE provides the function of updating the database for the list of phishing sites by communicating with Update Server. The TOE uses TLS 1.2 Protocol (OpenSSL) provided in the operational environment so as to protect transmitted data when communicating with Update server.

The TOE is a security solution that is in the form of library running in Samsung Smart TV and has the hardware and the software requirements as in the following [Table 1].

[Table 1] shows TOE’s hardware and software requirements.

Category		Contents
H/W	CPU	ARM architecture (Cortex A17 Quad)
	DDR Memory	2GB
	Flash Memory	eMMC 8GB
	NIC	10/100 MB Ethernet*1
	Wi-Fi	802.11a/b/g/n
S/W	Web Brower	Tizen Browser 1.1
	OpenSSL	V1.0.1s
	Web App	Web App running in Samsung Smart TV
	REE OS	Tizen 2.4
	TEE OS	TrustWare V1.5

[Table 1] Hardware and software requirements for TOE

External IT entities needed for the TOE operation are as follows. The TOE uses TLS V1.2 protocol(OpenSSL) provided in the operational environment when communicating with the external IT entity as below.

- Google Safe Browsing Server : A server provided by Google that informs whether a relevant URL is a phishing site or not.
- Update Server : A server that performs updates of phishing site database used in the Phishing Site Blocking function.

2. Identification

The TOE is identified as follows:

Developer	SAMSUNG ELECTRONICS Co., Ltd.
Name	Samsung Smart TV Security Solution
Version	V1.0
TOE Component	TV_SYSTEM_001_V1.0_Release_1.armv7l.rpm TV_PLATFORM_001_V1.0_Release_1.armv7l.rpm TV_PLATFORM_002_V1.0_Release_1.armv7l.rpm TV_SERVICE_001_V1.0_Release_1.armv7l.rpm TV_SERVICE_002_V1.0_Release_1.armv7l.rpm

[Table 2] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (June 27, 2016) Korea Evaluation and Certification Regulation for IT Security (November 1, 2012)
TOE	Samsung Smart TV Security Solution V1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 , CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL1
Protection Profile	N/A (ST does not claim conformance to a PP)
Developer	SAMSUNG ELECTRONICS Co., Ltd.
Sponsor	SAMSUNG ELECTRONICS Co., Ltd.
Evaluation Facility	Korea Security Evaluation Laboratory (KSEL)
Completion Date of Evaluation	August 16, 2016
Certification Body	IT Security Certification Center

[Table 3] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST by security objectives and security requirements. The TOE provides security features to verify system integrity, to prevent execution of unauthorized Web App, to encrypt and decrypt important data used in Web App, to block access of phishing site, and updating the database for the list of phishing sites by communicating with Update Server. For more details refer to the ST.

4. Assumptions and Clarification of Scope

There are no any Assumptions in the Security Problem Definition in the ST.

The scope of this evaluation was limited to the functionality and assurance covered in the Security Target. Other functionality included in Samsung Smart TV was not assessed as part of this evaluation. All other functionality provided by Samsung Smart TV needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation.

Note that:

- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. .(for the detailed information of TOE version and TOE Components version refer to the [Table 2])

5. Architectural Information

The architecture of Samsung Smart TV is basically composed based on the ARM TrustZone technology provided by ARM CPU. The execution environment of Samsung Smart TV is classified as Trusted Execution Environment(TEE) and Rich OS Application Environment. TEE functions based on TrustWare V1.5(Operating System Self-Developed by Samsung Electronics) and Rich OS Application Environment functions in Tizen 2.4 Operating System. Among the security functions of the TOE, System Integrity Monitoring function is executed in TEE and REE, whereas Web App Protection function, Data Encryption/Decryption function, Phishing Site Blocking function, Update Server Communication function are executed in REE.

5.1 Physical Scope of TOE

The TOE consists of software provided in the form of a library, and developer guidance. The TOE is distributed to the developers of Samsung Smart TV, and is operated in the form of a library for its operation after installation. The scope of the TOE includes only some of the library that is in charge of security function out of all the elements that compose the whole Samsung Smart TV. That is, the physical scope of TOE includes the library and the developer guidance of the API provided by the library. The following security functions are provided in the form of a library by the TOE

- System Integrity Monitoring
- Web App Protection
- Data Encryption/Decryption
- Phishing Site Blocking
- Update Server Communication

5.2 Logical Scope of TOE

Logical scope of the TOE includes all the aspects that are included in the physical scope of TOE. That is, all the functions provided by the library are included in the logical scope of TOE. The following security functions are provided by the TOE

System Integrity Monitoring

The TOE periodically performs the verification on the kernel integrity of Tizen OS while in normal operation through System Integrity Monitoring function so as to ensure safe operation of Samsung Smart TV.

System Integrity Monitoring function can be separated into three parts: the part that starts System Integrity Monitoring function on the application area of REE; the part that does system integrity monitoring on the dynamic kernel memory area, while operating on the kernel module area of REE, when TOE gets operated; the part that does the system integrity monitoring on the static area while operating on the application area of TEE.

The System Integrity Monitoring function that operates on Application of REE starts the monitoring process after being installed in the Application area of Tizen OS, and inserts the part that performs system integrity monitoring on the dynamic kernel memory area into kernel as a LKM(Loadable Kernel Module) so that the monitoring function can get operated on the kernel area of REE.

As mentioned earlier, the System Integrity Monitoring function that operates on the kernel module area of REE performs a part of functions of TOE. Thus, this operates while being inserted as a LKM(Loadable Kernel Module) by the System Integrity Monitoring function that operates on the application of REE. When monitoring function starts, this performs system integrity monitoring for dynamic kernel memory area.

The System Integrity Monitoring function that operates in the application area of TEE detects whether there is any distortion or not by periodically comparing the memory value of the static kernel memory and the original value. This also receives the detected result from the System Integrity Monitoring function that operates on the kernel module area of REE, and saves the result along with the result detected in static kernel memory.

Web App Protection

The TOE provides Web App Protection function in order to prevent execution of an unauthorized Web App in Samsung Smart TV. Samsung Smart TV can download and store only the Web App provided in App Store (hereinafter “App Contents Server”) provided by Samsung Electronics. When registering Web App in App Contents server, Samsung Electronics registered after encrypting the Web App, and Samsung Smart TV User can download the Web App from App Contents Server and store it on Samsung Smart TV. In order to execute the stored Web App, the decryption process is required. During the decryption process of the Web App, if the Web App is determined to be modified, the execution of the relevant Web App will be blocked. The TOE uses AES Algorithm (CTR mode) for decryption of Web App, and the 128-bit sizes of the cryptographic key.

Data Encryption/Decryption

The TOE provides encryption/decryption function for important data used in Web App. The TOE uses AES algorithm (CBC mode) for encryption, and the 128-bit sizes of the cryptographic key. The cryptographic key is derived from hardware using PBKDF2 algorithm. The Cryptographic key exists on memory after being generated, and is destroyed after encryption/decryption operation is completed. The zeroization is used as the cryptographic key destruction method.

Phishing Site Blocking

The TOE provides Phishing Site Blocking function in order to prevent private information from being exposed to any risks through the access to a harmful phishing site by Samsung Smart TV User. If Samsung Smart TV User accesses web sites using Web Browser(Tizen Browser), Phishing Site Blocking function checks the site based on the phishing site database stored in Smart TV. If the site is suspected for being a phishing site, Google Safe Browsing service is used to check whether the relevant site is a phishing site or not. If the relevant site is confirmed to be a phishing site, the information of such for the site being a phishing site is informed to the user. If the user selects to block the access to the site, the access to the phishing site is blocked to protect private information of the user. The TOE also provides Smart TV user the ability to either disable or enable the Phishing Site Blocking function. If a user disables to use the Phishing Site Blocking function, the Phishing Site Blocking function is not performed.

The list of Phishing Site on the database is updated periodically through Update Server.

※ When communicating with the TOE and Google Safe Browsing server, the transmitted data is protected by using TLS protocol provided by the operational environment.

Update Server Communication

TOE provides the function of updating the database for the list of phishing sites by communicating with Update Server. The TOE uses OpenSSL provided in the operational environment so as to protect transmitted data when communicating with Update server.

6. Documentation

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

Identifier	Version
Samsung Smart TV Security Solution V1.0 Developer's Guide	V1.4

[Table 4] Documentation

7. TOE Testing

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

- TOE security functionality: The TOE is a Smart TV Security Solution that provides security functions in the form of library by being embedded on TV. The TOE provides functions for the secure operation of Samsung Smart TV with system(kernel of Tizen OS) integrity verification, blocking the execution of unauthorized Web App, and blocking access to phishing sites. In addition, the TOE also provides encryption/decryption function for data used in Web App, and Update Server communication for updating the database for the list of phishing sites by communicating with Update Server.
- Balance between evaluator's activities: The targeted evaluation assurance level is EAL1, and the evaluator tried to balance time and effort of evaluator's activities between EAL1 assurance components.

In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, flaws in networking protocol implementation, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR.

8. Evaluated Configuration

The TOE is a Smart TV Security Solution that provides security functions in the form of library by being embedded on Samsung Smart TV. The TOE provides functions for the secure operation of Samsung Smart TV with system(kernel of Tizen OS) integrity verification, blocking the execution of unauthorized Web App, and blocking access to phishing sites. In addition, the TOE also provides encryption/decryption function for data used in Web App, and Update Server communication for updating the database for the list of phishing sites by communicating with Update Server.

The TOE is identified by TOE name and version number. The TOE identification information is provided CLI.

And the guidance documents listed in this report chapter 6, [Table 4] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL1.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives clearly define operational environment. Therefore the verdict PASS is assigned to ASE_OBJ.1.

The ST doesn't define any extended component. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent. Therefore the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be use as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer clearly identifies the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE, and the evaluation evidence. Therefore, the verdict of ALC_CMS.1 is the Pass.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

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

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

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

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The functional specification provides high-level description of SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict of ADV_FSP.1 is the Pass.

Therefore, the functional specification(TSF interface description) which are included in the development documentation, are adequate to give understanding about how the TSF satisfies the SFRs, and how these SFRs implementation are not damaged or bypassed.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no easily identifiable exploitable vulnerabilities in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don’t allow attackers possessing less than an enhanced-basic attack potential to violate the SFRs. The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
ATE	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	PASS
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 5] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- Smart TV User shall install immediately when an alert for firmware update pops up on TV so that the security functions can be maintained in a most up-to-date version.
- Smart TV shall provide secure communication channel when communicating with the TOE and Google Safe Browsing server.
- Default settings of the Phishing Site Blocking functions should be developed to be enabled.
- Smart TV developers should insert a warning label informing about the dangers of accessing a phishing site so that Smart TV user to select access phishing site or not.
- To protect the sensitive data of user, to be developed using a data encryption and decryption functions when developing Web App.

11. Evaluation Evidence

Identifier	Issue date
Samsung Smart TV Security Solution V1.0 Security Target V1.4	2016.08.08
Samsung Smart TV Security Solution V1.0 Functional Specification V1.3	2016.08.08
Samsung Smart TV Security Solution V1.0 Developer’s Guide V1.4	2016.08.08
Samsung Smart TV Security Solution V1.0 CM documentation V1.3	2016.08.08

[Table 6] Evaluation Evidence

12. Acronyms and Glossary

CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
Google Safe Browsing	Google Safe Browsing is a service provided by Google offering URL list that contains phishing contents and open API that can use the list.
OR	Observation Report
REE(Rich Execution Environment)	This is a concept that is contradictory to TEE, and refers to execution environment provided by general operating environment such as Tizen, Android.
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
Smart TV User	Users installing and executing Web App in order to use various smart functions embedded on TV and using management function supported in TV.
ST	Security Target
TEE(Trusted Execution Environment)	This refers to execution environment providing the security of a quality higher than the execution environment provided in general operating environment. This defined the function of security hardware and software providing execution

environment based on safe reliability of security related applications in devices such as smartphone, smart TV. Global Platform, which is a standard group, establishes the standard in the architecture of TEE and related API.

Tizen OS
Tizen is based on the Linux kernel of Linux foundation, and is made based on HTML5 and C++. It is an open source operating system having the purpose of being included in mobile devices including smart phone, and electronic devices such as TV.

TOE
Target of Evaluation

TrustWare V1.5
This is an operating environment installed for the application of TEE(ARM TrustZone) technology, and TrustWare V1.0 is the operating system self-developed by Samsung Electronics even from the kernel stage.

TSF
TOE Security Functionality

Update Server
Server that performs the update on the database for the list of phishing site used in Phishing Site Blocking function

Web App
Application for Tizen OS based on HTML5 which can be used by being downloaded on TV

13. Bibliography

The evaluation facility has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Samsung Smart TV Security Solution V1.0, Evaluation Technical Report V2.00, August 29, 2016

[4] Samsung Smart TV Security Solution V1.0, Security Target V1.5, August 16, 2016