Smart TV Security Solution V7.0 for Samsung Knox

Certification Report

Certification No.: KECS-CISS-1190-2022

2022. 11. 01

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2022.11.01	-	Certification report for Smart TV Security Solution V7.0 for Samsung Knox - First documentation

This document is the certification report for Smart TV Security Solution V7.0 for Samsung Knox of SAMSUNG ELECTRONICS Co., Ltd.

<u>The Certification Body</u>

<u>IT Security Certification Center</u>

<u>The Evaluation Facility</u>

<u>Korea Security Evaluation Laboratory (KSEL)</u>

Table of Contents

1. Executive Summary

This report describes the result of the EAL1 evaluation of "Smart TV Security Solution V7.0 for Samsung Knox" 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.

Samsung Knox is a brand name given to a secure platform and security solutions that are equipped with the products released from Samsung Electronics.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on October 31, 2022. This report grounds on the evaluation technical report ("ETR" hereinafter)[3] and the Security Target ("ST" hereinafter)[4]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level 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.

Smart TV Security Solution V7.0 for Samsung Knox (hereinafter 'TOE') is a Smart TV Security Solution that provides security functions in the form of library by being embedded on Samsung Smart TV. For the secure operation of Samsung Smart TV, The TOE provides 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.

The TOE provides the security functions as follows.

- System Integrity Monitoring function: Integrity verification function for the kernel of Tizen OS

- Web App Protection function: Function to block the execution of unauthorized

Web App in Smart TV

- Data Encryption/Decryption function: Function to encrypt and decrypt data that developer designates for protection out of the data used in Web App

- Phishing Site Blocking function: Function to verify whether the site to access is a phishing site or not when Smart TV user accesses the site by using Web Browser (linked to Google Safe Browsing)

The TOE is delivered 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 security functions defined in the above.

The operating systems of TOE uses Tizen 6.5 and TrustWare V3.1.0. This is the operating environment of TOE. Tizen 6.5 includes Crypto Module, Update Manager, OpenSSL 1.1.1l, and SQLite 3.33.0 required for TOE operation, and TrustWare V3.1.0 includes Crypto Module. The Crypto Module provides a cryptographic algorithm required by the security function of the TOE, and the Update Manager provides a function of communicating with the Security Care Server. OpenSSL provides secure communication of TLS V1.3 when communicating with an external IT entity (Google Safe Browsing Server, Security Care Server). SQLite is used to retrieve the DB list of phishing sites.

The TOE performs security functions using the cryptographic algorithm provided by the Crypto Module included in the operating systems. For System Integrity Monitoring function and Phishing Site Blocking function, the Secure Hash Algorithm (SHA) provided by the Crypto Module is used, and for Data Encryption/Decryption function and Web App Protection function, the Advanced Encryption Standard (AES) block cryptographic algorithm provided by the Crypto Module is used to perform security functions.

The Update Manager provided in the operating environment of the TOE communicates with an external IT entity using the secure communication protocol of TLS V1.3 based on OpenSSL. Communication with external IT entity can be done in the form of a wired communication using Ethernet and a wireless communication using Wi-Fi.

The external IT entities required for TOE operation are as follows.

- Google Safe Browsing Server: A server operated by Google that communicates to check whether the URL is a phishing site in the Phishing Site Blocking function

- Security Care Server: Server that collects problems by receiving reports detected by the System Integrity Monitoring function of Samsung Smart TV and provides online update function of phishing site DB list

The System Integrity Monitoring function of the TOE transmits the detected integrity verification report to the Update Manager provided by the operating environment, and the Update Manager periodically communicates with the Security Care Server to transmit the report to the server.

The Update Manager provided by the operating environment of the TOE communicates with the Security Care Server to download and install the phishing site DB list file to update the phishing site DB list used by the Phishing Site Blocking function. The Phishing Site Blocking function first checks the URL of the site opened by the browser based on the list of phishing sites stored in the phishing site DB. If it is suspected to be a phishing site, it communicates with the Google Safe Browsing Server to make sure that the URL is a phishing site. Retrieving the DB list of phishing sites uses the SQLite provided by the TOE operating environment. The developer can communicate with Samsung Smart TV using the serial port when developing applications for Smart TV using TOE. Serial port communication is not provided to Smart TV users who are not developers.

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

Category		Contents
H/W	CPU	ARM architecture (Cortex A53 Quad) or higher
	DDR Memory	1.5GB or higher
	Flash Memory	eMMC 8GB or higher
	Ethernet	1 x 10/100Mb RJ45
	Wi-Fi	802.11 a/b/g/n
	Serial Port	RS-232C
S/W	Web Browser	Tizen Browser 5.1.08160
	REE OS	Tizen 6.5 (kernel 5.4.77)
	TEE OS	TrustWare V3.1.0

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

2. Identification

The TOE is identified as follows:

Developer	SAMSUNG ELECTRONICS Co., Ltd.
TOE reference	Smart TV Security Solution V7.0 for Samsung Knox
Version	V7.0
TOE Component	Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_PLATFORM_001_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_PLATFORM_002_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_PLATFORM_003_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_001_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_002_V7.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_003_V7.0_Release_1-1-1.armv7l

	Samsung_Smart_TV_Security_Solution_SERVICE_004_V7.0_ Release_1-1-1.armv7l
Guide	Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2

[Table 2] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 24, 2017) Korea Evaluation and Certification Regulation for IT Security (May 17, 2021)
TOE	Smart TV Security Solution V7.0 for Samsung Knox
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1
Protection Profile	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	October 31, 2022
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. 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 V3.1.0(Operating System developed by Samsung Electronics) and Rich OS Application Environment functions in Tizen 6.5 Operating System. Among the security functions of the TOE, System Integrity Monitoring function is executed in TEE and Rich Execution Environment (REE), Data

Encryption/Decryption function is executed in TEE or REE according to the developer selection, whereas Web App Protection function and Phishing Site Blocking 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 delivered to the developers of Samsung Smart TV, and is operated in the form of a library. The scope of the TOE includes only some libraries that are in charge of security functions. That is, only the distributed libraries and developer guide are included in the physical scope of the TOE. Since the Update Manager, SQLite, OpenSSL, and Crypto Module required for TOE operation are included in the operating systems, they are excluded from the physical scope of the TOE. The Crypto Module is a form of library in which a cryptographic algorithm is implemented and provides an interface for using the cryptographic algorithm. The Update Manager is a software package consisting of a module that communicates with a Security Care Server, a module that manages reports sent to a Security Care Server, a module that manages update functions through a Security Care Server, and a common library used by each module.

TOE is directly delivered to developers in a form of CD, including instruction.

TOE Components	Delivery Form	Note
Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l.rpm)	Software (CD)	System Integrity Monitoring
Samsung_Smart_TV_Security_Solution_PLAT		Data Encryption/Decryption

FORM_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLA TFORM_001_V7.0_Release_1-1-1.armv7l.rpm) Samsung_Smart_TV_Security_Solution_PLAT FORM_003_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLAT FORM_003_V7.0_Release_1-1-1.armv7l.rpm)		
Samsung_Smart_TV_Security_Solution_PLAT FORM_002_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLAT FORM_002_V7.0_Release_1-1-1.armv7l.rpm)		Web App Protection
Samsung_Smart_TV_Security_Solution_SER VICE_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SER VICE_001_V7.0_Release_1-1-1.armv7l.rpm)		Phishing Site Blocking
Samsung_Smart_TV_Security_Solution_SER VICE_002_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SER VICE_002_V7.0_Release_1-1-1.armv7l.rpm) Samsung_Smart_TV_Security_Solution_SER VICE_003_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SER VICE_003_V7.0_Release_1-1-1.armv7l.rpm) Samsung_Smart_TV_Security_Solution_SER		System Integrity Monitoring Phishing Site Blocking

VICE_004_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SER VICE_004_V7.0_Release_1-1-1.armv7l.rpm)		
Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2 (Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2.pdf)	Document File (CD)	

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 security functions provided within the logical scope of the TOE are as follows.

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 secure 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 Tizen OS

- The part that does System Integrity Monitoring on the dynamic kernel memory area, while operating on the kernel module area of Tizen OS, when TOE gets operated

- The part that does the System Integrity Monitoring on the static area while

operating on the application area of TrustWare.

As mentioned earlier, the System Integrity Monitoring function that operates on the kernel module area of Tizen OS performs a part of functions of TOE. Thus, this operates while being inserted as a Loadable Kernel Module(LKM) by the System Integrity Monitoring function that operates on the application of Tizen OS. 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 TrustWare 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 Tizen OS, 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) that is provided by the Crypto Module in an operating environment, and the cryptographic key is 128-bit sizes.

Data Encryption/Decryption

The TOE provides Encryption/Decryption function for important data used in Web App. The TOE uses AES algorithm (CBC mode) that is provided by the Crypto Module in an operating environment for encryption, and the 256-bit sizes of the cryptographic key. Data Encryption and Decryption can be performed in REE or TEE according to the developer selection. The cryptographic key is derived 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 Security Care Server.

6. Documentation

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

Identifier	Version
Smart TV Security Solution V7.0 for Samsung Knox Developer Guide	V1.2

[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 Samsung Smart TV. For the secure operation of Samsung Smart TV, The TOE provides system (kernel of Tizen OS) integrity verification, blocking 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.
- 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. For the secure operation of Samsung Smart TV, The TOE provides system (kernel of Tizen OS) integrity verification, blocking 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.

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[1] and CEM[2].

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

9.1 Security Target Evaluation (ASE)

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

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to 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:

- Developer must use a data encryption and decryption functions provided by the TOE to protect the sensitive user data when developing Web App.

- Developer must enable default settings of the Phishing Site Blocking functions for Smart TV user to use a Smart TV securely.

- Developer must insert warning label informing access to phishing site for Smart TV user to select access phishing site or not.

- Smart TV User shall install firmware update immediately when an alert occurs 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.

11. Evaluation Evidence

Identifier	Issue date
Smart TV Security Solution V7.0 for Samsung Knox Security Target V1.5	2022.10.19
Smart TV Security Solution V7.0 for Samsung Knox Functional Specification V1.0	2022.06.10
Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2	2022.10.11
Smart TV Security Solution V7.0 for Samsung Knox CM Documentation V1.3	2022.10.19

[Table 6] Evaluation Evidence

12. Acronyms and Glossary

CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
TSF	TOE Security Functionality
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
Google Safe Browsing	Google Safe Browsing is a service provided by Google that provides a URL list containing phishing content and a public API to use it.
Security Care Server	Server to collect problems by receiving reports delivered by the System Integrity Monitoring function of smart TVs and to provide online update of the DB list of internal phishing sites used for phishing site blocking function.
Update Manager	It delivers the report of System Integrity Monitoring function to the Security Care Server and downloads the phishing site DB list from the Security Care Server.
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.
Web App	Application for Tizen OS based on HTML5 which by being downloaded on TV
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.
Trusted Execution Environment(TEE)	This refers to an 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.
Rich Execution Environment(REE)	This is a concept that is contradictory to TEE, and refers to execution environment provided by general operating environment such as Tizen and Android.

TrustWare	Samsung Electronics developed its own TEE operating system from kernel based on ARM TrustZone tech.
Samsung Knox	Brand name given to a secure platform and security solutions that are equipped with the products released from Samsung Electronics.

13. Bibliography

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

[1]   Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017

[2]   Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017

[3]   Smart TV Security Solution V7.0 for Samsung Knox, Evaluation Technical Report V3.00, October 21, 2022

[4]   Smart TV Security Solution V7.0 for Samsung Knox Security Target V1.5, October 19, 2022