KECS-CR-24-13

Smart TV Security Solution V8.0 for Samsung Knox

Certification Report

Certification No.: KECS-CISS-1291-2024

2024. 2. 23.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2024.02.23.	-	Certification report for Smart TV Security Solution V8.0 for Samsung Knox - First documentation

This document is the certification report for Smart TV Security Solution V8.0 for Samsung Knox of SAMSUNG ELECTRONICS Co., Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Security Evaluation Laboratory Co., Ltd. (KSEL)

Table of Contents

1. Executive Summary

This report describes the result of the EAL1 evaluation of “Smart TV Security Solution V8.0 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.

The evaluation of the TOE has been carried out by Korea Security Evaluation Laboratory (KSEL) and completed on February 7, 2024. 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 V8.0 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. Samsung Knox is a brand name given to a secure platform and security solutions that are equipped with the products released from Samsung Electronics. For the secure operation of Samsung Smart TV, The TOE provides System (kernel of Tizen OS) Integrity Monitoring function, Phishing Site Blocking function, SE Communication Channel Protection function, and SE Client Apps Access Control function.

The TOE provides the security functions as follows.

- System Integrity Monitoring: Function to check the integrity of the kernel of

the Tizen OS and a function to send the inspection results to the Security Care Server

- Phishing Site Blocking: 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 the Google Safe Browsing)
- SE Communication Channel Protection: Function of protecting communication channel between the TOE and the SE, which is trusted IT products mounted on Smart TV, by establishing a secure channel based on the SCP 03 protocol
- SE Client Apps Access Control: When the SE Client Apps attempt to access the SE which is trusted IT products mounted on Smart TV, function that allows only SE Client Apps to access the SE Slot

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 the security function defined in the above.

The operating systems of TOE uses Tizen 8.0 and TrustWare V3.2.0. This is the operating environment of TOE. Tizen 8.0 includes the Crypto Module (CryptoCore 0.2.9-1), the Update Manager, OpenSSL 3.0.9, and SQLite 3.40.1 required for TOE operation, and TrustWare V3.2.0 includes the Crypto Module (CryptoCore 0.2.9-1). 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 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 using 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 User who is not developer.

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 show in [Table 1].

Category		Contents
H/W	CPU	ARM architecture (Cortex A53 Quad) or higher
	DDR Memory	2GB or higher
	Flash Memory	eMMC 8GB or higher
	Secure Element	S3SSE1A (optional) ※ SE is provided only in a specific operating environment (Cortex A76 Quad) and not in other operating environments
	NIC	10/100 MB Ethernet*1
	Wi-Fi	802.11b/g/n
	Serial Port	RS-232C
S/W	REE OS	Tizen 8.0 (kernel 5.4.249)
	TEE OS	TrustWare V3.2.0
	OpenSSL V3.0.9	Used to protect communication data with external IT entities (Security Care Server, Google Safe Browsing Server)
	SQLite V3.40.1	Used when searching the phishing site DB list for the Phishing Site Blocking function
	Crypto module (CryptoCore 0.2.9-1)	Providing the cryptographic algorithm used in the System Integrity Monitoring function, Phishing Site Blocking function, and SE Communication Channel Protection function
	Update manager	Transmitting a system integrity monitoring detection result report to the Security Care Server, and performing an update of the phishing site DB received from the Security Care Server
	Web Browser	Tizen Browser 7.1.01080

[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 V8.0 for Samsung Knox
Version	V8.0
TOE Component	Samsung_Smart_TV_Security_Solution_SYSTEM_001_V8.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_KVS_001_V8.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_001_V8.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_002_V8.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_003_V8.0_Release_1-1-1.armv7l
	Samsung_Smart_TV_Security_Solution_SERVICE_004_V8.0_Release_1-1-1.armv7l
Guide	Smart TV Security Solution V8.0 for Samsung Knox developer guidance V1.1

[Table 2] TOE identification

Scheme	Korea Evaluation and Certification Guidelines for IT Security (October 31, 2022) Korea Evaluation and Certification Scheme for IT Security (May 17, 2021)
TOE	Smart TV Security Solution V8.0 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	February 7, 2024
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 such as System Integrity Monitoring, Phishing Site Blocking, SE Communication Channel Protection, and SE Client Apps Access Control. 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. Samsung Smart TV's operating system consists of Rich Execution Environment (REE) and Trusted Execution Environment (TEE). REE refers to an execution environment provided by a general operating system and operates based on Tizen 8.0, TEE refers to an execution environment that provides a higher level of security than REE and operates based on TrustWare V3.2.0 (Operating System developed by Samsung Electronics). Among the security functions of the TOE, the System Integrity Monitoring function is executed in TEE and REE, Phishing Site Blocking function is executed in REE and SE Communication Channel Protection function and SE Client Apps Access Control function are executed in TEE.

5.1 Physical Scope of TOE

The TOE consists of software provided in the form of a library, and developer guidance as shown in [Table 4]. 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 guidance are included in the physical scope of the TOE. Update Manager, SQLite, OpenSSL, Crypto Module and SE required for TOE operation are

excluded from the physical scope of the TOE.

TOE is directly delivered to Samsung Smart TV developer in the form of CD including developer guidance.

TOE Components	Delivery Form	Note
• Samsung_Smart_TV_Security_Solution_SYSTEM_001_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SYSTEM_001_V8.0_Release_1-1-1.armv7l.rpm)	Software (CD)	System Integrity Monitoring
• Samsung_Smart_TV_Security_Solution_KVS_001_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_KVS_001_V8.0_Release_1-1-1.armv7l.rpm)		SE Communication Channel Protection, SE Client Apps Access Control
• Samsung_Smart_TV_Security_Solution_SERVICE_001_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_001_V8.0_Release_1-1-1.armv7l.rpm)		Phishing Site Blocking
• Samsung_Smart_TV_Security_Solution_SERVICE_002_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_002_V8.0_Release_1-1-1.armv7l.rpm) • Samsung_Smart_TV_Security_Solution_SERVICE_003_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_003_V8.0_Release_1-1-1.armv7l.rpm) • Samsung_Smart_TV_Security_Solution_SERVICE_004_V8.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_004_V8.0_Release_1-1-1.armv7l.rpm)		System Integrity Monitoring, Phishing Site Blocking
• Smart TV Security Solution V8.0 for Samsung Knox developer guidance V1.1 (Smart TV Security Solution V8.0 for Samsung Knox developer guidance V1.1.pdf)	Document File (CD)	

[Table 4] Physical scope of the TOE

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 the System Integrity Monitoring function so as to ensure secure operation of Samsung Smart TV. When integrity verification fails, a result report including terminal information and a tampering detection area is transmitted to the Security Care Server. The System Integrity Monitoring function can be separated into three parts.

- The part on the application area of Tizen OS that starts System Integrity Monitoring and report to the Security Care Server when integrity tampering is detected
- The part that does system integrity monitoring on the dynamic area, while operating on the kernel module area of Tizen OS, when TOE gets operated
- The part that does system integrity monitoring on the static area while operating on the application area of TrustWare

The System Integrity Monitoring function that operates in the application of the Tizen OS starts the monitoring process after being installed in the application area of the Tizen OS, it is inserted as a kernel module in the form of LKM (Loadable Kernel Module) so that the monitoring function can operate in the kernel area of the Tizen OS. In

addition, the results of tampering are confirmed from the System Integrity Monitoring function operated on the application of Trustware and reported to the Security Care Server.

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 in Trustware's memory area along with static memory tampering detection results.

Phishing Site Blocking

The TOE provides the 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), the 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, the 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 the Phishing Site Blocking function, the Phishing Site Blocking function does not work. The list of phishing site on the database is updated periodically through the Security Care Server.

SE Communication Channel Protection

When the SE Client Apps requests communication with the SE to the TOE, the TOE establishes a secure channel based on the SCP 03 protocol and SE which are trusted IT products mounted on the Smart TV, to safely protect data transmitted between the TOE and the SE. When the SE Client Apps request the TOE to access the SE, the TOE allows access to the SE through a secure channel only if the SE Client Apps have access rights to the SE, and does not establish a secure channel otherwise.

SE Client Apps Access Control

When the SE Client Apps installed on a smart TV attempts to access SE, a trusted IT product built in the smart TV, the TOE performs the SE Client Apps Access Control function that allows only SE Client Apps that are permitted to access the SE. When a running SE Client Apps tries to access the SE slot, the SE Client Apps Access Control policy allows access only if the SE Client App ID has access rights (Read, Write) registered for the SE Slot Number.

6. Documentation

The following documentation is evaluated and provided with the TOE to the Samsung Smart TV Developer.

Identifier	Version
Smart TV Security Solution V8.0 for Samsung Knox developer guidance	V1.1

[Table 5] 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 Integrity Monitoring, Phishing Site Blocking, SE Communication Channel Protection, and SE Client Apps Access Control.
- 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 Integrity Monitoring, Phishing Site Blocking, SE Communication Channel Protection, and SE Client Apps Access Control.

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 5] 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 6] Evaluation Result Summary

10. Recommendations

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

- Smart TV Developer must develop the default settings for the Phishing Site Blocking function to be activated in order for Smart TV User to use the smart TV safely.
- Smart TV Developer must insert a warning message informing them of the dangers of accessing phishing sites so that Smart TV User can choose to block when phishing sites are detected.
- Smart TV User must install the Smart TV software update immediately when an alarm occurs in order to always maintain the latest version of the security technology applied to the Smart TV operating environment.
- The TOE must protect transmitted data using a secure encrypted communication protocol between the TOE and Google Safe Browsing Server/Security Care Server.
- Smart TV Developer must check whether the encryption module used in the System Integrity Monitoring function, Phishing Site Blocking function, and SE Communication Channel Protection function operates normally.
- When developing SE Client Apps, Smart TV Developer must check whether the permissions (read, write) corresponding to the SE Client App ID and SE Slot Number are set to allow.

11. Security Target

Identifier	Issue date
Smart TV Security Solution V8.0 for Samsung Knox Security Target V1.2	2024.02.21
Smart TV Security Solution V8.0 for Samsung Knox Functional Specification V1.1	2023.12.29
Smart TV Security Solution V8.0 for Samsung Knox developer guidance V1.1	2023.12.22
Smart TV Security Solution V8.0 for Samsung Knox CM Documentation V1.2	2024.02.21

[Table 7] Evaluation Evidence

12. Acronyms and Glossary

CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OR	Observation Report
TSF	TOE Security Functionality
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
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 the Phishing Site Blocking function.
Google Safe Browsing	The Google Safe Browsing is a service provided by Google that provides a URL list containing phishing content and a public API to use it.
Update Manager	It delivers the report of the 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 who install and run apps to use various smart functions installed on the TV and utilize management functions supported within the TV.
Smart TV Developer	Developers who are provided with an environment to use the Serial Port and develop applications to be installed on smart TVs using the security functions of the TOE.
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	This refers to an execution environment providing

(TEE)	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 secure 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.
Secure Element (SE)	It is an independent system with its own processor and memory, as well as dedicated non-volatile memory, and provides anti-tampering functions to prevent hardware attack.
SE (Secure Element) Client	Apps installed in the TOE that store and use

App	important data such as personal information and encryption keys in the Secure Element.
Secure Channel Protocol (SCP)	A standard for how to encrypt and authenticate smart card (CCID) messages from GlobalPlatform, a consortium of hardware security vendors.

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 V8.0 for Samsung Knox, Evaluation Technical Report V2.00, February 21, 2024

[4] Smart TV Security Solution V8.0 for Samsung Knox Security Target V1.2, February 21, 2024