Smart TV Security Solution V8.0 for Samsung Knox Security Target Lite V1.1

SAMSUNG ELECTRONICS CO., Ltd.

This document is a translation of the Security Target written in Korean which has been evaluated.

Document History

VERSION	DESCRIPTION OF CHANGE	DATE
1.0	Sanitized version of ST V1.1	2024. 02. 02
1.1	Sanitized version of ST V1.2	2024. 02. 21

CONTENTS

LIST OF TABLE

1. Security Target Introduction

1.1. Security Target Reference

This section provides information to refer to the Security Target (ST) as in the following Table. The ST is identified by the ST Title and the ST Version as shown in [Table 1].

[Table 1] ST reference information

ST Title	Smart TV Security Solution V8.0 for Samsung Knox Security Target Lite
ST Version	V1.1
Authors	SAMSUNG ELECTRONICS Co., Ltd.
CC Identification	Common Criteria for Information Technology Security Evaluation (CC Version 3.1 Revision 5)
Evaluation Assurance Level	EAL1

1.2. TOE Reference

This section provides information to refer to the TOE as in the following Table. The TOE is identified by the TOE Title and the TOE Version as shown [Table 2].

[Table 2] TOE reference information

	Smart TV Security Solution V8.0 for Samsung Knox
TOE 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_Rele

	ase_1-1-1.armv7l
Developer	SAMSUNG ELECTRONICS Co., Ltd.

1.3. TOE Overview

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 security functions 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 shown in [Table 3].

[Table 3] Hardware/software for operating TOE

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

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

1.4. TOE Description

1.4.1. Physical scope of the 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 guide 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.

[Table 4] Physical scope of the TOE

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)	

TOE is delivered in the form of rpm package as shown in [Table 4]. As for its operation after installation, it is operated in the form of a library.

1.4.2.Logical scope of the 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.

1.5. Conventions

The Common Criteria allows iteration, selection, refinement, and assignment operations to be performed on security functional requirements. Each operation is used in this Security Target.

- ✓ 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.).

- ✓ 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].

- ✓ 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*.

- ✓ 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

- ✓ 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 (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 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 App

Apps installed in the TOE that store and use 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.

2. Conformance claim

This chapter describes how the Security Target conforms to the Common Criteria, Protection Profile and Package.

2.1. CC conformance claim

This Security Target conforms to the following Common Criteria.

✓ Common Criteria Identification

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
  - Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 Revision 5, 2017. 4, CCMB-2017-04-001
  - Common Criteria for Information Technology Security Evaluation, Part 2: SFR (Security Functional Requirement), Version 3.1 Revision 5, 2017. 4, CCMB-2017-04-002
  - Common Criteria for Information Technology Security Evaluation, Part 3: SAR (Security Assurance Requirement), Version 3.1 Revision 5, 2017. 4, CCMB-2017-04-003

✓ 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. Package conformance claim

This Security Target conforms to the following assurance package.

- Assurance Package: EAL1

2.3. PP conformance clam

- This Security Target does not claim conformance to other PPs

3. Security objectives

3.1. Security objectives for the operational environment

[Table 5] is the security objectives handled by technical and procedural method supported from operational environment in order to provide the TOE security functionality accurately.

[Table 5] Security objectives for the operational environment

Category	Contents
OE. Firmware Update	Smart TV users should install firmware update notifications as soon as they are notified to always keep their security technology up to date.
OE. Secure Channel	The TOE should perform secure communication with the Google Safe Browsing server through an encrypted communication protocol.
OE. Trusted Developer	The developer shall not have any malicious intention, should receive proper education for the use of the TOE and shall perform the obligation accurately.
OE.Crypto Module	To generate a hash value for the monitoring target in the System Integrity Monitoring function and to generate a hash value for the URL accessed by the web browser in the Phishing Site Blocking function, TOE use the Crypto Module provided by the operating environment(OS).
OE.Google Safe Browsing server	If the TOE suspects that the web browser access URL is a phishing site, it must call the Google Safe Browsing server to check whether it is an actual phishing site.

OE.Update Manager and Security Care Server	The TOE should send the system integrity monitoring detection result report to the Security Care Server through the Update Manager through secure communication and update the phishing site DB received from the Security Care Server through the Update Manager through secure communication.

4. Security requirements

The security requirements specify security functional requirements and assurance requirements that must be satisfied by the TOE.

4.1. Security functional requirements

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

[Table 6] summarizes the security functional requirements defined by this ST.

[Table 6] Security functional requirements

Security Functional class	Security functional component	
User data protection(FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Security management(FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TEE.1	Testing of external entities
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel

4.1.1. User data protection(FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [SE Client Apps Access Control policy]

on [The following list of subjects, objects, and operations].

- List of subjects: SE Client Apps
- List of objects: SE Slot
- List of operations: Read, Write

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [SE Client Apps Access Control policy] to objects based on the following: [The following list of subjects and objects, and for each, the SFP-relevant security attributes].

- List of subjects: SE Client Apps
- List of objects: SE Slot
- Security attributes of subjects: SE Client App ID
- Security attributes of objects: SE Slot Number

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [If access rights (Read, Write) are registered for the SE Slot Number for the SE Client App ID].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None].

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [Phishing Site Blocking policy] on [The following list of subjects, information, and operations].

- List of subjects: Smart TV User
- List of information: HTTP Address Information
- List of operations: Blocking Web Site

※ Application None: In certain regions, the phishing site blocking function does not work because Samsung Smart TV and the Security Care Server are not linked.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [Phishing Site Blocking policy] based on the following types of subject and information security attributes: [The following list of subjects and information, and for each, the security attributes].

- List of subjects: Smart TV User
- List of information: HTTP Address Information
- Security attributes of subjects: None
- Security attributes of information: URL

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [If the destination URL included in the security attributes of information is not included in the phishing sites list].

FDP_IFF.1.3 The TSF shall enforce the [None].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [When the security attribute of the information URL is included in the list of phishing sites, but the Smart TV User decides to access the phishing URL as 'Access'].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [None].

※ Application None: When determining a phishing site, two steps are taken. In step 1, if it is suspected to be a phishing site by comparing it with the internal phishing site database list, in step 2, it is finally determined whether it is a phishing site using the Google Safe Browsing service.

4.1.2. Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the functions [Phishing Site Blocking] to [Smart TV User].

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [Phishing Site Blocking policy] to restrict the ability to *[send]* the security attributes [Destination URL] to [Smat TV User].

※ Application None: Sending means sending the destination URL that the Smart TV user wants to access to the Google Safe Browsing server.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Phishing Site Blocking policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Smart TV Developer] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Enable/disable Phishing Site Blocking function].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Smart TV User, Smart TV Developer].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

4.1.3.Protection of the TSF

FPT_TEE.1 Testing of external entities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1 The TSF shall run a suite of tests *periodically during normal operation* to check the fulfillment of [Kernel integrity of the Tizen operating system] .

FPT_TEE.1.2 If the test fails, the TSF shall [A result report including terminal information, tampering detection area, and hash value for inspection

target area is transmitted to the Security Care Server].

※ Application None: In certain regions, Samsung Smart TV and the Security Care Server are not linked, so result reports are not sent.

4.1.4. Trusted path/channels

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 [SE Client Apps Access Control function].

4.2. Security assurance requirements

Assurance requirements of this security target are comprised of assurance components in CC part 3, and the evaluation assurance level is EAL1. [Table 7] summarizes assurance components.

[Table 7] Security assurance requirements

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_ECD.1	Extended components definition
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

4.2.1. Security Target evaluation

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

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

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:

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

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

Content and presentation elements:

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.

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.

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.

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

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

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

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.

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.

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.

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:

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

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements:

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

presentation.

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:

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

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

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

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

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

Evaluator action elements:

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

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:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

4.2.2. Development

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

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

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

4.2.3.Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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.

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.

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.

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.

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.

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.

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

Evaluator action elements:

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

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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.

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:

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

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

4.2.4.Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

Evaluator action elements:

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

requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

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

4.2.5. Tests

ATE_IND.1 Independent testing – conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

4.2.6. Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E 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.

4.3. Security requirements rationale

4.3.1. Dependency rationale of security functional requirements

[Table 8] shows dependency of security functional requirements.

[Table 8] Dependency of security functional requirements

No	Security Functional Component	Dependencies
1	FDP_ACC.1	FDP_ACF.1
2	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
3	FDP_IFC.1	FDP_IFF.1
4	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
5	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
6	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1
7	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
8	FMT_SMF.1	−
9	FMT_SMR.1	FIA_UID.1
10	FPT_TEE.1	−
11	FTP_ITC.1	−

FMT_SMR.1 has a dependent relationship on FIA_UID.1, but in general, Smart TVs are owned by individual Smart TV user and grant all rights to the personal owner, so they do not provide separate identification and authentication functions.

FDP_ACF.1 has a dependent relationship on FMT_MSA.3 and FMT_MSA.3 has a dependent relationship on FMT_MSA.1, but the value of the security attribute used in the SE Client Apps Access Control policy is included in the TOE and delivered, so management functions for security attributes are not provided.

4.3.2. Dependency rationale of security assurance requirements

The dependency of EAL1 assurance package provided in the CC is already satisfied.

5. TOE Summary Specification

5.1. 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 on application of Tizen OS 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 Loadable Kernel Module (LKM) so that system monitoring can get operated on the kernel area of 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. However, if the kernel has not been modified, it is not reported to the security management server.

As mentioned earlier, the System Integrity Monitoring function that operates on the

kernel module area of Tizen OS, performs some of functions of the TOE. Thus, this operates while being inserted as a 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 scope of monitoring for the dynamic kernel memory area is LKM that has kernel authority while operating as a part of kernel while being inserted to kernel.

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. The scope of monitoring for the static kernel memory area is the protection for the Read-Only which is the Read-Only data of kernel, for Text which is the kernel code, for Exception Vector Table which deals with interrupt or exception.

When the TOE operates, the physical memory address for the protection area is received from the System Integrity Monitoring function operating in the kernel module area of the Tizen operating system, and the original Hash (SHA256) for the corresponding memory value is stored in the Trustware memory area. The Read-Only and Text areas are 64K each, and the hash value of the memory in the protection area is compared with the original, and if the memory in the area has been tampered with, it is detected.

The integrity verification report detected by the System Integrity Monitoring function is collected and transmitted to the Security Care Server through the Update Manager provided by the TOE operating environment at a set time.

Relevant SFR: FPT_TEE.1

5.2. 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 (SQLite) 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 default value for the Phishing Site Blocking function is enable.

- ✓ The URL you are trying to access through a web browser is initially analyzed to see if it is a suspected phishing site by referring to the phishing site database that exists locally on the Smart TV. The list of saved phishing sites is hashed and stored using a hash algorithm (SHA-256).

  * The list of phishing site DB stores only hash values, and the generation of hash values is performed by the developer and distributed as part of the TV firmware. The update of the phishing site DB list communicates with the Security Care Server to update the new list.

- ✓ As a result of the analysis, if it is suspected to be a phishing site, the Google Safe Browsing service is used to make a final determination as to whether the site is a phishing site.

- ✓ It informs the user that it is a phishing site and relies on the user's judgment as to whether to access the URL. You can choose to allow or block access to the judged site, and if you decide to block, you can block access to the phishing site.

The list of phishing site on the database is updated periodically through the Security Care Server.

TOE provides an online update function for the phishing site DB list. The Update Manager provided in the operational environment communicates with the Security Care Server to download the update file to Smart TV and performs integrity verification(electronic signature) for the update file. TOE performs the update by installing the update file downloaded from Smart TV.

Relevant SFR: FDP_IFC.1, FDP_IFF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

5.3. 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. To establish a secure channel, the TOE generates a challenge value and requests communication with the SE, and the TOE and the SE generate a data encryption key based on the challenge value and a previously registered shared key (48 bytes).

When the SE Client Apps requests to the TOE to access the SE, the TOE makes the SE Client Apps communicate with the SE through a secure channel. The secure channel can only be used if the SE Client Apps has access permission to the SE. The TOE uses the data encryption key to protect data transmitted to the SE from exposure through the AES256 (CBC mode) encryption algorithm and protects data

communicated with the SE from tampering using the MAC algorithm.

Relevant SFR: FTP_ITC.1

5.4. 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. The TOE includes an SE Client Apps Access Control policy (Acccess Control List), which defines SE slots and access rights (read, write) accessible by the SE Client Apps.

When a running SE Client Apps attempts to access the SE Slot, TOE checks the SE Client Apps Access Control policy to determine whether the SE Client App ID is registered to access the SE Slot Number. The SE Client App ID is a unique identifier (a string of 32 characters consisting of numbers and lowercase alphabet) given when developing an SE Client Apps installed on a Smart TV. The SE Slot Number refers to an identifier for a storage space provided by SE to store important data or encryption keys of the SE Client Apps.

In the SE Client Apps Access Control policy, access is allowed only when the SE Client App ID is registered with access permissions (Read, Write) for the SE Slot Number. The read permission can perform reading data stored in the SE slot, encrypting or decrypting using the encryption key stored in the SE slot. Write permission may perform writing or deleting data or encryption keys stored in SE Slot.

Relevant SFR: FDP_ACC.1, FDP_ACF.1