Smart TV Security Solution V9.0
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 V1.0	2026. 01. 21
1.1	developer guidance version modification	2026. 02. 02

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 and Monitor Security Solution V9.0 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:2022 Revision 1)
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

TOE reference	Smart TV and Monitor Security Solution V9.0 for Samsung Knox
TOE Version	V9.0
TOE Component	✓ Knox_Solution_SYSTEM-V9.0-1-1-1.armv7l ✓ Knox_Solution_BROWSER-V9.0-1-1-1.armv7l ✓ Knox_Solution_SERVICE_A-V9.0-1-1-1.armv7l ✓ Knox_Solution_SERVICE_U-V9.0-1-1-1.armv7l ✓ Knox_Solution_SERVICE_R-V9.0-1-1-1.armv7l ✓ Knox_Solution_UEP-V9.0-1-1-1.armv7l
Developer	SAMSUNG ELECTRONICS Co., Ltd.

1.3. TOE Overview

Smart TV and Monitor Security Solution V9.0 for Samsung Knox (hereinafter

‘TOE’) is security solution that provides security functions in the form of library by being embedded on Samsung Smart TV/Monitor. For the secure operation of Samsung Smart TV/Monitor, The TOE provides System(kernel of Tizen OS) Integrity Monitoring function, Phishing Site Blocking function, and Script File Signature Verification function. 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 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 and Monitor User accesses the site by using Web Browser (linked to the Google Safe Browsing)
- ✓ Script File Signature Verification: Before executing the script file stored in the writable partition, Samsung Smart TV/Monitor requests the TOE to verify the signature stored in the script file, allowing execution of only the authenticated script file.

The TOE is delivered to the developers of Samsung Smart TV/Monitor 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/Monitor. The TOE provides only security functions defined in the above.

The operating systems of TOE uses Tizen 10.0 and TrustWare V3.5.0. This is the operating environment of TOE. Tizen 10.0 includes the Crypto module(CryptoCore 0.2.9-1), the Update Manager, OpenSSL 3.0.18, and SQLite 3.50.2 required for TOE operation, and TrustWare V3.5.0 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 entities using the secure communication protocol of TLS V1.3 using OpenSSL. For communication with external IT entities, Smart TV can perform wired communication using Ethernet and wireless communication using Wi-Fi, and Smart Monitor can perform 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 /Monitor 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/Monitor using the serial port when developing applications for Smart TV/Monitor using TOE. Serial port communication is not provided to Smart TV/Monitor User who is not developer.

The TOE is a security solution that is in the form of library running in Samsung Smart TV/Monitor 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	1.5GB or higher
	Flash Memory	eMMC 8GB or higher
	Ethernet	10/100 MB Ethernet(optional) ※ Smart Monitor does not have an Ethernet port
	Wi-Fi	802.11 abgn
	Serial Port	RS-232C
S/W	REE OS	Tizen 10.0 (Linux kernel 5.4.261 32-bit)
	TEE OS	TrustWare V3.5.0
	OpenSSL V3.0.18	Used to protect communication data with external IT entities (Security Care Server, Google Safe Browsing Server)
	SQLite V3.50.2	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..
	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 10.0.12280

The architecture of Samsung Smart TV/Monitor is basically composed based on the ARM TrustZone technology provided by ARM CPU. Samsung Smart TV/ Monitor'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 10.0, TEE refers to an execution environment that provides a higher level of security than REE and operates based on TrustWare V3.5.0 (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 and Script File Signature Verification function is executed in REE.

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/Monitor, 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, and Crypto module required for TOE operation are excluded from the physical scope of the TOE.
TOE is directly delivered to Samsung Smart TV/Monitor developer in the form of CD including developer guidance.

[Table 4] Physical scope of the TOE

TOE Components	Delivery Form	Note
✓ Knox_Solution_SYSTEM-V9.0-1-1-1.armv7l (Konx_Solution_SYSTEM-V9.0-1-1-1.armv7l.rpm)	Software (CD)	System Integrity Monitoring

✓ Knox_Solution_BROWSER-V9.0-1-1-1.armv7l (Knox_Solution_BROWSER-V9.0-1-1-1.armv7l.rpm)		Phishing Site Blocking
✓ Knox_Solution_SERVICE_A_V9.0-1-1-1.armv7l (Knox_Solution_SERVICE_A_V9.0-1-1-1.armv7l.rpm) ✓ Knox_Solution_SERVICE_U_V9.0-1-1-1.armv7l (Knox_Solution_SERVICE_U_V9.0-1-1-1.armv7l.rpm) ✓ Knox_Solution_SERVICE_R_V9.0-1-1-1.armv7l (Knox_Solution_SERVICE_R_V9.0-1-1-1.armv7l.rpm)		System Integrity Monitoring, Phishing Site Blocking
✓ Knox_Solution_UEP-V9.0-1-1-1.armv7l (Knox_Solution_UEP-V9.0-1-1-1.armv7l.rpm)		Script File Signature Verification
✓ Smart TV and Monitor Security Solution V9.0 for Samsung Knox developer guidance V1.1 (Smart TV and Monitor Security Solution V9.0 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/Monitor. 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 access to a harmful phishing site by Samsung Smart TV/Monitor Users. If Samsung Smart TV/Monitor Users accesse web sites using a Web Browser(Samsung Browser), the Phishing Site Blocking function checks the site based on the phishing site database stored in the Smart TV/Monitor. If the site is suspected of 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 user is informed that the site is a phishing site. If the user chooses to block access to the site, access to the phishing site is blocked to protect the user's private information. The TOE also provides Samsung Smart TV/Monitor 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 sites in the database is updated periodically through the Security Care Server.

- ✓ Script File Signature Verification

Before executing the script file stored in the writable partition, Samsung Smart TV/Monitor requests the TOE to verify the signature stored in the script file, allowing execution of only the authenticated script file.

The TOE goes through three steps to verify the signature of the script file. First, calculate the unique hash value of the script file to be executed. Next, the signature included in the script file is decrypted using the public key, and the signed hash value is extracted. The TOE compares the unique hash value of the last calculated file with the decrypted hash value of the signature to see if the two values match exactly.

Since only Samsung Smart TV/Monitor developers can sign script files using private keys in advance, Samsung Smart TV/Monitor can check the integrity and origin of script files through functions provided by the TOE.

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 <u>*underlined and italicized*</u>.

- ✓ 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 TV/Monitor 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/Monitor User

Users who install and run apps to use various smart functions installed on the TV/Monitor and utilize management functions supported within the TV/Monitor.

- ✓ Smart TV/Monitor Developer

Developers who are provided with an environment to use the Serial Port and develop applications to be installed on Smart TV/Monitor 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/Monitor. 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.

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 (CC:2022 Revision 1)
  - Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 1: Introduction and general model (CCMB-2022-11-001)
  - Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 2: Security functional components (CCMB-2022-11-002)
  - Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1,November 2022 — Part 3: Security assurance components (CCMB-2022-11-003)
  - Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities (CCMB-2022-11-004)
  - Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Part 5: Pre-defined packages of security requirements (CCMB-2022-11-005)

✓ **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

2.4. Conformance claim rationale

Since this Security Target does not claim conformance to any Protection Profile, a conformance claim rationale is not applicable.

2.5. Reference to evaluation methods/activities

This Security Target uses the evaluation methods and activities defined in section 5.2.1; there are no additional evaluation methods or activities.

3. Security problem definition

3.1. Assets

The main assets protected by the TOE are as follows.

- Kernel of Tizen operating system
- Smart TV/Monitor User's personal information

3.2. Threats

T. OS kernel modification

The threat source can modulate the kernel of the operating system for malicious purposes.

T. Phishing site connection induction

The threat source may leak the Smart TV/Monitor user's personal information by inducing the user to access a harmful phishing site.

T. Script file modification

The threat source may leak the Smart TV/Monitor user's personal information by modifying a script file stored in a writable partition for malicious purposes.

3.3. Organizational security policies

P. Firmware update

Smart TV/Monitor users must install firmware update notifications immediately and apply the latest security technology.

P. Digital signature management

The private key for script file digital signature must be managed safely.

3.4. Assumptions

A. Firmware update
Firmware on Smart TV/Monitor should always be kept up-to-date.

A. Secure Channel
The TOE must perform secure communication using cryptographic communication with the Google Safe Browsing server and the Security Care Server.

A. Trusted Developer
Developers using TOE are harmless and must be properly trained in development using TOE and perform their obligations accurately according to developer guidelines.

A. Operational environment function support
OpenSSL, SQLite, Crypto module, and update manager required for TOE operation included in the TOE operating system (Tizen) are reliable and safe.

A. Secure external IT entity
The Google Safe Browsing Server and Security Care Server that exist outside the TOE are reliable and safe. In addition, the Google Safe Browsing server provides the result of checking whether it is a phishing site to the TOE, and the Security Care Server provides the phishing site DB to the TOE.

A. Digital signature management
The private key for digital signing a script file is reliable and safe.

4. Security objectives

4.1. 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/Monitor 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. Hash value generation	The Crypto module used for the system integrity monitoring function of the TOE and the phishing site blocking function and the OpenSSL used for the script file signature verification function of the TOE must provide a trusted hash value.
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.

OE. Digital signature management	Private and public keys for script file digital signature must be managed safely.
OE. Operational environment function support	OpenSSL, SQLite, Crypto module, and update manager required for TOE operation must ensure reliability and safety.

4.2. Security objectives rationale

[Table 6] is the security objectives rationale that traces, for each security objective related to the operational environment, the organizational security policies implemented in response to the security objectives and the assumptions supported by the security objectives.

[Table 6] Security objectives rationale

	OE. Keep firmware version up-to-date	OE. Secure channel	OE. Trusted developer	OE. Hash value generation	OE. linked to the Google Safe Browsing	OE. Update Manager and Security Care Server	OE. Digital signature management	OE. Operational environment function support
P. Firmware update	O							
P. Digital signature management							O	
A. Firmware update	O							
A. Secure channel		O				O		
A. Trusted developer			O					
A. Operational environment function support				O				O
A. Secure external IT entity					O	O		
A. Digital Signature Management							O	

OE. Keep firmware version up-to-date(P. Firmware update, A. Firmware update)

Smart TV/Monitor users ensure that security technologies are always kept up-to-date by installing them as soon as firmware update notifications appear, so they are needed to perform P.Firmware update and support A.Firmware update.

OE. Secure channel (A. Secure channel)

Since the TOE must perform secure communication with the Google Safe Browsing server and the Security Care Server through the encrypted communication protocol, it is necessary to support the A. Secure channel.

OE. Trusted developer (A. Trusted developer)

Smart TV/Monitor developers are harmless, need to be properly trained for the use of TOE, and perform their obligations accurately according to developer guidelines, so they are necessary to support A.Trusted Developer.

OE. Hash value generation (A. Operational environment function support)

The Crypto module used for the system integrity monitoring function of the TOE and the phishing site blocking function and the OpenSSL used for the script file signature verification function of the TOE must provide a trusted hash value, so it is necessary to support A. Operational environment function support.

OE. linked to the Google Safe Browsing (A. Secure external IT entity)

If the web browser access URL is suspected to be a phishing site, the TOE must call the Google Safe Browsing server to check if it is an actual phishing site, so it is necessary to support A. Secure external IT entity.

OE. Update Manager and Security Care Server (A. Secure channel, A. Secure external IT entity)

The TOE must transmit the system integrity monitoring detection result report to the Security Care Server through secure communication through the update manager and update the phishing site DB received through secure communication from the Security Care Server through the update manager, so it is necessary to support **A. Secure channel** and **A. Secure external IT entity**.

OE. Digital signature management (P. Digital signature management, A. Digital signature management)

Since private and public keys for script file digital signature must be safely managed and reliable, it is necessary to perform **P. Digital Signature Management** and support **A. Digital Signature Management**.

OE. Operational environment function support (A. Operational environment function support)

OpenSSL, SQLite, Crypto module, and update manager required for TOE operation must be guaranteed reliability and safety, so it is necessary to support
A. Operational environment function support.

5. Security requirements

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

5.1. 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 7] summarizes the security functional requirements defined by this ST.

[Table 7] Security functional component

Security Functional class	Security functional component	
User data protection(FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_SDI.2	Stored data integrity monitoring and action
Security management(FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TEE.1	Testing of external entities

5.1.1. User data protection(FDP)

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/Monitor 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/Monitor 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 initialization

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/Monitor 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/Monitor 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.

FDP_ SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies,

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [Integrity error in script file] on all objects, based on the following attributes: [Digital signature].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [Prevent execution of modified script files].

※ Application None: This SFR addresses integrity checking and response behavior for script files stored in writable partitions.

5.1.2. 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/Monitor 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 [Smart TV/Monitor User].

※ Application None: Sending means sending the destination URL that the Smart TV/Monitor 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/Monitor 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/Monitor User, Smart TV/Monitor Developer].

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

5.1.3. 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/Monitor and the Security Care Server are not linked, so result reports are not sent.

5.2. 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 8] summarizes assurance components.

[Table 8] Security assurance requirements

Security assurance class	Security assurance component	
Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	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

5.2.1. 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 For a multi−assurance ST, the TOE overview shall describe the TSF organization in terms of the sub−TSFs defined in the PP−Configuration the ST claims conformance to.

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

ASE_INT.1.9C 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 Direct rationale 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 identify the edition of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The 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 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 conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify a PP-Configuration, or 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 shall describe any conformance of the ST to a PP as PP-Conformant.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being claimed.

ASE_CCL.1.9C 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 PP-Configuration, PPs and any functional packages for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PP-Configuration, PPs, and any functional package for which conformance is being claimed.

ASE_CCL.1.11C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PP-Configuration, PPs, and any functional packages for which conformance is being claimed.

ASE_CCL.1.12C The conformance claim for PP(s) or a PP−Configuration shall be exact, strict, or demonstrable or a list of conformance types.

ASE_CCL.1.13C If the conformance claim identifies a set of Evaluation methods and Evaluation activities derived from CEM work units that shall be used to evaluate the TOE then this set shall include all those that are included in any package, PP, or PP−Module in a PP−Configuration to which the ST claims conformance, and no others.

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_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements

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

Content and presentation elements

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

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

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

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

Evaluator action elements

ASE_SPD.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: ASE_SPD.1 Security problem definition

Developer action elements

ASE_OBJ.1.1D The developer shall provide a statement of security objectives for the operational environment.

ASE_OBJ.1.2D The developer shall provide a security objectives rationale for the operational environment.

Content and presentation elements

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

ASE_OBJ.1.2C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.1.3C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

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 may 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 may be clearly expressed using existing components.

ASE_REQ.1 Direct rationale security requirements

Dependencies: ASE_ECD.1 Extended components definition
ASE_OBJ.1 Security objectives for the operational environment
ASE_SPD.1 Security problem 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 For a single-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE.

The sets of SARs shall be consistent with the PPs or PP-Configuration to which the ST claims conformance.

ASE_REQ.1.3C For a multi-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE and the sets of SARs that apply to each sub-TSF. The sets of SARs shall be consistent with the multi-assurance PP-Configuration to which the ST claims conformance.

ASE_REQ.1.4C 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.1.5C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.6C All operations shall be performed correctly.

ASE_REQ.1.7C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.8C The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) counter all threats for the TOE.

ASE_REQ.1.9C The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) enforce all OSPs.

ASE_REQ.1.10C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.1.11C The statement of security requirements shall be internally consistent.

ASE_REQ.1.12C If the ST defines sets of SARs that expand the sets of SARs of the PPs or PP−Configuration it claims conformance to, the security requirements rationale shall include an assurance rationale that justifies the consistency of the extension and provides a rationale for the disposition of any Evaluation methods and Evaluation activities identified in the conformance statement that are affected by the extension of the sets of SARs

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 Direct rationale 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.

5.2.2. 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.

5.2.3. 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 controls 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.

5.2.4. 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.

5.2.5. Independent testing

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.

5.2.6. Vulnerability analysis

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.

5.3. Security requirements rationale

5.3.1. Dependency rationale of security functional requirements

[Table 9] shows dependency of security functional components.

[Table 9] Dependency of security functional component

No	Security Functional Component	Dependencies
1	FDP_IFC.1	FDP_IFF.1
2	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
3	FDP_SDI.2	-
4	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
5	FMT_MSA.1	[FDP_ACC.1 또는 FDP_IFC.1], FMT_SMF.1, FMT_SMR.1
6	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
7	FMT_SMF.1	-
8	FMT_SMR.1	FIA_UID.1
9	FPT_TEE.1	-

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

5.3.2. Dependency rationale of security assurance requirements

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

5.4. Security requirements rationale

5.4.1. Rationale for the security functional requirements

[Table 10] is the security functional requirements rationale that traces each SFR to the threats addressed by the SFR. The security requirements rationale demonstrates that the SFRs, together with the security objectives for the operational environment, address all identified threats to the TOE.

[Table 10] Rationale for the security functional requirements

	T. OS kernel modification	T. Phishing site connection induction	T. Script file modification	P.Firmware update	P. Digital signature management
FDP_IFC.1		O			
FDP_IFF.1		O			
FDP_SDI.2			O		O
FMT_MOF.1		O			
FMT_MSA.1		O			
FMT_MSA.3		O			
FMT_SMF.1		O			
FMT_SMR.1		O			
FPT_TEE.1	O			O	

FDP_IFC.1, FDP_IFF.1 (T. Phishing site connection induction)

These SFRs provide the ability to block access based on HTTP address information when smart TV and monitor users access phishing sites, so it corresponds to **T. Phishing site connection induction**.

FDP_SDI.2 (T. Script file modification, P. Digital signature management)

This SFR performs integrity check and response actions for script files stored in writable partitions based on digital signatures, so it corresponds to **T. Script file**

modification, P. Digital signature management.

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1 (T. Phishing site connection induction)

These SFRs provide security functions, security attributes, and security roles for phishing site blocking functions to smart TV and monitor users, so they correspond to **T. Phishing site connection induction**.

FPT_TEE.1 (T. OS kernel modification, P.Firmware update)

This SFR corresponds to the **T. OS kernel modification, P.Firmware update** because the TSF provides the function of testing an external entity (Tizen OS kernel).

5.4.2. Rationale for the security assurance requirements

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious.

EAL1 provides a basic level of assurance by a limited ST and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functionality (TSF).

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

6. TOE Summary Specification

6.1. 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/Monitor. 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 Care 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

6.2. 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/Monitor User. If Samsung Smart TV/Monitor User accesses web sites using Web Browser (Samsung Browser), the Phishing Site Blocking function checks the site based on the phishing site database (SQLite) stored in Smart TV/Monitor. 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/Monitor 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/Monitor. 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/Monitor and performs integrity verification(electronic signature) for the update file. TOE performs the update by installing the update file downloaded from Smart TV/Monitor.

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

6.3. Script File Signature Verification

The Smart TV/Monitor requests the TOE to verify the signature of the script file to check the integrity and origin of the script file before executing the script file stored in the writable partition.

The TOE proceeds through three steps to verify the signature of the script file.

- ✓ Calculate the unique hash value of the script file requested for signature verification using the hash algorithm (SHA-256) provided by OpenSSL.
- ✓ Decrypt the signature included in the script file with the RSA 4096 or RSA 2048 algorithm using the public key to extract the signed hash value.
- ✓ Compare the calculated unique hash value of the script file with the decrypted hash value in the signature to see if the two values match exactly.

The RSA 4096 and RSA 2048 public keys used to decrypt signatures are installed on the TOE, and the TOE selects the RSA 4096 or RSA 2048 algorithm by referring to the tags included in the signature to decrypt the signatures included in the script file.

The private key paired with the public key is stored on a key management server accessible only to developers of smart TVs and monitors. Developers of smart TVs and monitors can sign script files using private key.

Relevant SFR: FDP_SDI.2