Smart TV Security Solution V7.0 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	1. Sanitized version of the ST Lite V1.0	2022. 10. 13
1.1	2. Document proofreading 3. Change the term Encryption module to Crypto module	2022. 10. 19

CONTENTS

LIST OF TABLES

1. Introduction of Security Target

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 V7.0 for Samsung Knox Security Target Lite
ST Version	V1.1
Publication Date	2022. 10. 19
Authors	SAMSUNG ELECTRONICS Co., Ltd.
CC Identification	Common Criteria for Information Technology Security (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 Component

TOE reference	Smart TV Security Solution V7.0 for Samsung Knox
TOE Version	V7.0
TOE Component	✓ Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_PLATFORM_001_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_PLATFORM_002_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_PLATFORM_003_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_SERVICE_001_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_SERVICE_002_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_SERVICE_003_V7.0_Release_1-1-1.armv7l ✓ Samsung_Smart_TV_Security_Solution_SERVICE_004_V7.0_Release_1-1-1.armv7l
Developer	SAMSUNG ELECTRONICS CO., Ltd.

1.3. TOE Overview

Smart TV Security Solution V7.0 for Samsung Knox (hereinafter 'TOE') is a Smart TV Security Solution that provides security functions in the form of library by being embedded on Samsung Smart TV. 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 verification, blocking execution of unauthorized Web App, and blocking access to phishing sites. In addition, the TOE also provides encryption/decryption function for data used in Web App.

The TOE provides the security functions as follows.

- ✓ System Integrity Monitoring function: Integrity verification function for the kernel of Tizen OS
- ✓ Web App Protection function: Function to block the execution of unauthorized Web App in Smart TV
- ✓ Data Encryption/Decryption function: Function to encrypt and decrypt data that developer designates for protection out of the data used in Web App
- ✓ Phishing Site Blocking function: Function to verify whether the site to access is a phishing site or not when Smart TV User accesses the site by using Web Browser (linked to the Google Safe Browsing)

The TOE is delivered to the developers of Samsung Smart TV in the form of a library which is a kind of software, and is not in charge of all kinds of security functions provided in Samsung Smart TV. The TOE provides only security functions defined in the above.

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

The TOE performs security functions using the cryptographic algorithm

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

The Update Manager provided in the operating environment of the TOE communicates with an external IT entity using the secure communication protocol of TLS V1.3 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	1.5GB or higher
	Flash Memory	eMMC 8GB or higher
	NIC	10/100 MB Ethernet*1
	Wi-Fi	802.11a/b/g/n
	Serial Port	RS-232C
S/W	Web Browser	Tizen Browser 5.1.08160
	REE OS	Tizen 6.5 (kernel 5.4.77)
	TEE OS	TrustWare V3.1.0

The architecture of Samsung Smart TV is basically composed based on the ARM TrustZone technology provided by ARM CPU. The execution

environment of Samsung Smart TV is classified as Trusted Execution Environment (TEE) and Rich OS Application Environment. TEE functions based on TrustWare V3.1.0 (Operating System developed by Samsung Electronics) and Rich OS Application Environment functions in Tizen 6.5 Operating System. Among the security functions of the TOE, the System Integrity Monitoring function is executed in TEE and Rich Execution Environment (REE), the Data Encryption/Decryption function is executed in TEE or REE according to the developer selection, whereas the Web App Protection function and the Phishing Site Blocking function are executed in REE.

1.4. TOE Description

1.4.1. Physical Scope of TOE

The TOE consists of software provided in the form of a library, and developer guidance as shown in [Table 4]. The TOE is delivered to the developers of Samsung Smart TV, and is operated in the form of a library. The scope of the TOE includes only some libraries that are in charge of security functions. That is, only the distributed libraries and developer guide are included in the physical scope of the TOE. Since the Update Manager, SQLite, OpenSSL, and the Crypto Module required for TOE operation are included in the operating systems, they are excluded from the physical scope of the TOE. The Crypto Module is a form of library in which a cryptographic algorithm is implemented and provides an interface for using the cryptographic algorithm. The Update Manager is a software package consisting of a module that communicates with the Security Care Server, a module that manages reports sent to the Security Care server, a module that manages update functions through the Security Care Server, and a common

library used by each module.

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

[Table 4] Functional TOE Components

TOE Components	Delivery Form	Note
✓ Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SYSTEM_001_V7.0_Release_1-1-1.armv7l.rpm)	Software (CD)	System Integrity Monitoring
✓ Samsung_Smart_TV_Security_Solution_PLATFORM_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_001_V7.0_Release_1-1-1.armv7l.rpm) ✓ Samsung_Smart_TV_Security_Solution_PLATFORM_003_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_003_V7.0_Release_1-1-1.armv7l.rpm)		Data Encryption/Decryption
✓ Samsung_Smart_TV_Security_Solution_PLATFORM_002_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_002_V7.0_Release_1-1-1.armv7l.rpm)		Web App Protection
✓ Samsung_Smart_TV_Security_Solution_SERVICE_001_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_001_V7.0_Release_1-1-1.armv7l.rpm)		Phishing Site Blocking
✓ Samsung_Smart_TV_Security_Solution_SERVICE_002_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_002_V7.0_Release_1-1-1.armv7l.rpm) ✓ Samsung_Smart_TV_Security_Solution_SERVICE_		System Integrity Monitoring Phishing Site Blocking

003_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_003_V7.0_Release_1-1-1.armv7l.rpm) ✓ Samsung_Smart_TV_Security_Solution_SERVICE_004_V7.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_004_V7.0_Release_1-1-1.armv7l.rpm)		
✓ Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2 (Smart TV Security Solution V7.0 for Samsung Knox Developer Guide V1.2.pdf)	Document File (CD)	

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 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.

The System Integrity Monitoring function can be separated into three parts.

- The part that starts System Integrity Monitoring function on the

application area of Tizen OS

- The part that does system integrity monitoring on the dynamic kernel memory area, while operating on the kernel module area of Tizen OS, when TOE gets operated

- The part that does system integrity monitoring on the static area while operating on the application area of TrustWare

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

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

- ✓ Web App Protection

The TOE provides Web App Protection function in order to prevent execution of an unauthorized Web App in Samsung Smart TV. Samsung Smart TV can download and store only the Web App provided in App Store (hereinafter “App Contents Server”) provided by Samsung Electronics. When registering Web App in App Contents server, Samsung Electronics

registered after encrypting the Web App, and Samsung Smart TV User can download the Web App from App Contents Server and store it on Samsung Smart TV. In order to execute the stored Web App, the decryption process is required. During the decryption process of the Web App, if the Web App is determined to be modified, the execution of the relevant Web App will be blocked. The TOE uses AES Algorithm (CTR mode) that is provided by the Crypto Module in an operating environment, and the cryptographic key is 128-bit sizes.

- ✓ Data Encryption/Decryption

The TOE provides encryption/decryption function for important data used in Web App. The TOE uses AES algorithm (CBC mode) that is provided by the Crypto Module in an operating environment for encryption, and the 256-bit sizes of the cryptographic key. The Data Encryption/Decryption can be performed in REE or TEE according to the developer selection. The cryptographic key is derived using PBKDF2 algorithm. The Cryptographic key exists on memory after being generated, and is destroyed after encryption/decryption operation is completed. The zeroization is used as the cryptographic key destruction method.

- ✓ Phishing Site Blocking

The TOE provides 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 to use the Phishing Site Blocking function, the Phishing Site Blocking function is not performed.

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

1.5. Conventions

This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Four presentation choices are discussed here.

- ✓ Iteration

Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, for example, FIA_AFL.1 (1) and FIA_AFL.1 (2).

- ✓ Assignment

The assignment operation is used to assign a specific value to an unspecified parameter such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

✓ Selection

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

✓ Refinement

The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinement of security requirements is denoted by **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 installing and executing Web App in order to use various smart functions embedded on TV and using management function supported in TV.

- ✓ Web App

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

- ✓ Tizen OS

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

- ✓ Trusted Execution Environment (TEE)

This refers to an execution environment providing the security of a quality higher than the execution environment provided in general operating environment. This defined the function of security hardware and software providing execution environment based on 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.

2. Conformance Claims

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

2.1. Conformance to Common Criteria

This Security Target conforms to the following Common Criteria.

- ✓ Common Criteria
  - 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. Conformance to Packages

This Security Target conforms to the following Protection Profile.

- ✓ Assurance Package: EAL1

2.3. Conformance to Protection Profiles

- ✓ There is no Protection Profile that this Security Target.

3. Security Objectives

3.1. Security Objectives for Operational Environment

This section describes the Security Objectives that must be fulfilled by technical and procedural measures in the operational environment of the TOE.

[Table 5] Security Objectives for the Operational Environment

Category	Contents
OE. Firmware Update	Smart TV User shall install immediately when an alert for firmware update pops up on TV so that the security functions can be maintained in a most up-to-date version.
OE. Secure Communication	Smart TV shall provide secure communication channel when the TOE communicates with Update Server and the Google Safe Browsing server.
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.

4. Security Requirements

This chapter describes security functional requirements and security assurance requirements which should be satisfied in the TOE.

4.1. Security Functional Requirements

The security functional requirements defined in this Security Target are based on the 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

Class	Component	
Cryptographic Support	FCS_CKM.1	Cryptographic key generation (Data Encryption/Decryption)
	FCS_CKM.4	Cryptographic key destruction (Data Encryption/Decryption)
	FCS_COP.1(1)	Cryptographic operation (Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic operation (Web App Protection)
	FCS_COP.1(3)	Cryptographic operation (System Integrity Monitoring)
	FCS_COP.1(4)	Cryptographic operation (Phishing Site Blocking)
User Data Protection	FDP_DAU.1	Basic Data Authentication
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Security Management	FMT_MOF.1	Management of security functions behavior
	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

4.1.1.Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation (Data Encryption/Decryption)

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Password Based Key Derivation Function (PBKDF2)] and specified cryptographic key sizes [256-bit] that meet the following: [RFC2898].

* Application Note: The cryptographic key generation algorithm (PBKDF2) used to generate cryptographic key in the Data Encryption/Decryption function is provided by the Crypto Module included in TOE operating environment.

FCS_CKM.4 Cryptographic key destruction (Data Encryption/Decryption)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [None].

FCS_COP.1(1) Cryptographic operation (Data Encryption/Decryption)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Data Encryption/Decryption] in accordance with a specified cryptographic algorithm [Advanced Encryption Standard (AES-CBC)] and cryptographic key sizes [256-bit] that meet the following: [FIPS PUB 197].

* Application Note: The cryptographic algorithm (AES-CBC) used for the Data Encryption/Decryption functions is provided by the Crypto Module included in TOE operating environment.

FCS_COP.1(2) Cryptographic operation (Web App Protection)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [data decryption] in accordance with

a specified cryptographic algorithm [Advanced Encryption Standard (AES-CTR)] and cryptographic key sizes [128-bit] that meet the following: [FIPS PUB 197]

* Application Note: The cryptographic algorithm (AES-CTR) used in the Web App Protection function is provided in the Crypto Module included in TOE operating environment.

FCS_COP.1(3) Cryptographic operation (System Integrity Monitoring)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Create Checksum for Integrity Verification] in accordance with a specified cryptographic algorithm [Secure Hash Algorithm (SHA)] and cryptographic key sizes [256-bit] that meet the following: [FIPS PUB 180-4].

* Application Note: The cryptographic algorithm SHA256 used for the System Integrity Monitoring function is provided in the Crypto Module included in TOE operating environment.

FCS_COP.1(4) Cryptographic operation (Phishing Site Blocking)

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Create Checksum for Integrity Verification] in accordance with a specified cryptographic algorithm [Secure Hash Algorithm (SHA)] and cryptographic key sizes [256-bit] that meet the following: [FIPS PUB 180-4].

* Application Note: The cryptographic algorithm (SHA256) used for the Phishing Site Blocking function is provided by the Crypto Module included in TOE operating environment.

4.1.2. User data protection(FDP)

FDP_DAU.1 Basic Data Authentication

Hierarchical to: No other components

Dependencies: No dependencies

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [Web App].

FDP_DAU.1.2 The TSF shall provide [library for Web App Protection function] with the ability to verify evidence of the validity of the indicated information.

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 SFP] on [the below list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

- subject: Smart TV User
- information: URL
- operation: web site blocking

* Application Note: In a certain area, Samsung Smart TV and the Security Care Server are not interoperated, the Phishing Site Blocking function is not operated.

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 SFP] based on the following types of subject and information security attributes: [the below list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

- subject: Smart TV User
- information: URL
- subject security attribute: None
- information security attribute: destination 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 information security attribute is not included in the list of phishing sites].

* Application Note: For determination of a phishing site, two steps should be performed. The first step is to compare with the list of phishing site in the database, and if suspected for being a phishing site after the comparison, the second step of using the Google Safe Browsing service should finally determine whether the site is a phishing site or not.

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [If the destination URL included in the information security attribute is included in the list of phishing sites, but if the user decided to access the relevant URL].

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

4.1.3. Security management (FMT)

FMT_MOF.1 Management of security functions behavior

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

behavior of the function [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 SFP] to restrict the ability to *[send]* the security attributes [destination URL] to [Smart TV User].

※ Application Note: The meaning of transmission means sending any destination URL that the Smart TV User wants to access to the Google Safe Browsing server.

FMT_MSA.3 Static attribute initialization

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 SFP] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Smart TV User] 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 function: [Phishing Site Blocking].

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].

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

4.1.4.Protection of the TSF (FPT)

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 for Tizen OS].

FPT_TEE.1.2 If the test fails, the TSF shall [report when kernel integrity violation is detected].

[Transmit the result report including the hash value for the device information, the modulation detection area, and the inspection target area to the Security Care Server.]

※ Application Note: In some areas, the Samsung Smart TV and the Security Care Server are not connected, so the result report is not transmitted.

4.2. Security Assurance Requirements

Security assurance requirements (SAR) defined in this document consists of assurance component in Common Criteria for Information Technology Security Evaluation, Part 3. The Evaluation Assurance Levels (EALs) is EAL1. Table 7 shows the summary of assurance components.

[Table 7] Security Assurance Requirements

Assurance Class	Assurance Component	
ASE: 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
ADV: Development	ADV_FSP.1	Basic functional specification
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
ATE: Tests	ATE_IND.1	Independent testing - conformance
AVA: 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. Dependency Rationale

4.3.1. SFR Dependencies

Table 8 shows the dependencies on the TOE Security Functional Components.

[Table 8] Dependencies on the TOE Security Functional Components

No	TOE Security Functional Component	Claimed Dependencies	Note
1	FCS_CKM.1	FCS_COP.1, FCS_CKM.4	
2	FCS_CKM.4	FCS_CKM.1	
3	FCS_COP.1(1)	FCS_CKM.1, FCS_CKM.4	
4	FCS_COP.1(2)	-	
5	FCS_COP.1(3)	-	
6	FCS_COP.1(4)	-	
7	FDP_DAU.1	-	
8	FDP_IFC.1	FDP_IFF.1	
9	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	
10	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	
11	FMT_MSA.1	FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	
12	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	
13	FMT_SMF.1		
14	FMT_SMR.1	FIA_UID.1	
15	FPT_TEE.1	-	

The dependency of some functional components is not satisfied, and the description for the justification of such is as follows.

FIA_UID.1

- Smart TV embedded with security function of TOE is generally the possession of the individual of the Smart TV User, and all the rights

are given to individual users, and thus identification or authentication is not provided.

FCS_CKM.1, FCS_CKM.4 (Dependencies: FCS_COP.1 (2)):

- The cryptographic key used to decrypt the Web App in the Web App Protection function is provided in the Operational Environment, and thus does not have a process for generation and destruction of the cryptographic key.

FCS_CKM.1, FCS_CKM.4 (Dependencies: FCS_COP.1 (3)):

- The System Integrity Monitoring function uses SHA-256 hash algorithm in order to verify the integrity of the kernel, and thus does not have a process for generation and destruction of the cryptographic key.

FCS_CKM.1, FCS_CKM.4 (Dependencies: FCS_COP.1 (4)):

- The Phishing Site Blocking function uses SHA-256 hash algorithm in order to check whether the web site is a phishing site or not, and thus does not have a process for generation and destruction of the cryptographic key.

4.3.2. SAR Dependencies

The dependency of each assurance package (EAL1) provided by 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 to ensure secure operation of Samsung Smart TV.

The System Integrity Monitoring function can be separated into three parts.

- The part that starts System Integrity Monitoring function on the application area of Tizen OS
- The part that does system integrity monitoring on the dynamic kernel memory area, while operating on the kernel module area of Tizen OS, when TOE gets operated
- The part that does 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.

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 the Page Table that does translating from the virtual address of memory to a physical address, 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 along with the result detected in static kernel memory. 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.

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, FCS_COP.1 (3)

5.2. Web App Protection

The TOE provides the Web App Protection function in order to prevent execution of an unauthorized Web App in Samsung Smart TV. Samsung Smart TV can download and store only the Web App provided in App Store (hereinafter “App Contents Server”) provided by Samsung Electronics.

When registering Web App in App Contents server, Samsung Electronics registered after encrypting the Web App, and Samsung Smart TV User can download the Web App from App Contents Server and store it on Samsung Smart TV. In order to execute the stored Web App, the decryption process is required. During the decryption process of the Web App, if the Web App is determined to be modified, the execution of the relevant Web App will be blocked. The TOE uses AES Algorithm (CTR mode) that is the Crypto Module provided in a TOE operating environment for decryption of Web App, and the 128-bit sizes of the cryptographic key.

Relevant SFR: FDP_DAU.1, FCS_COP.1 (2)

5.3. Data Encryption/Decryption

The TOE provides encryption/decryption function for important data used in Web App. The TOE uses AES algorithm (CBC mode) that is the Crypto Module provided in a TOE operating environment for encryption, and the 256-bit sizes of the cryptographic key. The cryptographic key is derived from hardware using PBKDF2 algorithm. The Data Encryption/Decryption function can be performed in REE OS or TEE OS according to the developer selection. The Cryptographic key exists on memory after being generated, and is destroyed after encryption/decryption operation is completed. The zeroization is used as the cryptographic key destruction method.

The Data Encryption/Decryption function has the lifecycle of 1) Cryptographic key generation, 2) Encryption and Decryption operation, 3) Cryptographic key destruction.

Relevant SFR: FCS_CKM.1, FCS_CKM.4, FCS_COP.1 (1)

5.4. 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 to use the Phishing Site Blocking function, the Phishing Site Blocking function is not performed. The list of phishing site on the database is updated periodically through 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 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