

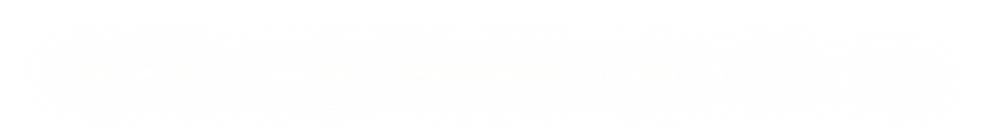
**Embedded Common**

**Firmware for**

**VESTEL Smart TVs**

**V0.1**

**SECURITY TARGET V1.3**



**VESTEL ELEKTRONİK SAN. TİC. A.Ş.**

Table of Content

[**1** **SECURITY TARGET INTRODUCTION** 5](#_Toc95386747)

[**1.1** **ST Reference** 5](#_Toc95386748)

[**1.2** **TOE Reference** 5](#_Toc95386749)

[**1.3** **TOE Overview** 5](#_Toc95386750)

[1.3.1 TOE Usage and Major Security Features 5](#_Toc95386751)

[1.3.2 TOE Type 7](#_Toc95386752)

[1.3.3 Non-TOE Hardware, Software and/or Firmware 7](#_Toc95386753)

[**1.4** **TOE Description** 7](#_Toc95386754)

[1.4.1 Physical Scope of the TOE 7](#_Toc95386755)

[1.4.2 Logical Scope of the TOE 9](#_Toc95386756)

[**2** **CONFORMANCE CLAIM** 11](#_Toc95386757)

[**2.1** **CC Conformance Claim** 11](#_Toc95386758)

[**2.2** **PP Claim** 11](#_Toc95386759)

[**2.3** **Package Claim** 11](#_Toc95386760)

[**2.4** **Conformance Claim Rationale** 11](#_Toc95386761)

[**3** **SECURITY PROBLEM DEFINITION** 12](#_Toc95386762)

[**3.1** **Overview** 12](#_Toc95386763)

[**3.2** **Threats** 12](#_Toc95386764)

[**3.3** **Organizational Security Policies** 13](#_Toc95386765)

[**3.4** **Assumptions** 13](#_Toc95386766)

[**4** **SECURITY OBJECTIVES** 14](#_Toc95386767)

[**4.1** **Overview** 14](#_Toc95386768)

[**4.2** **Security Objectives for the TOE** 14](#_Toc95386769)

[**4.3** **Security Objectives for Operational Environment** 14](#_Toc95386770)

[**4.4** **Security Objectives Rationale** 16](#_Toc95386771)

[**5** **EXTENDED COMPONENT DEFINITION** 19](#_Toc95386772)

[**5.1** **Extended Family FPT\_SCB – TSF initialisation** 19](#_Toc95386773)

[5.1.1 Family behavior 19](#_Toc95386774)

[5.1.2 Component levelling 19](#_Toc95386775)

[5.1.3 Management: FPT\_ SCB.1 19](#_Toc95386776)

[5.1.4 Audit: FPT\_ SCB.1 19](#_Toc95386777)

[5.1.5 FPT\_SCB.1 TSF Initialisation 19](#_Toc95386778)

[**6** **SECURITY REQUIREMENTS** 21](#_Toc95386779)

[**6.1** **Security Functional Requirements** 22](#_Toc95386780)

[6.1.1 Cryptographic Support (FCS) 24](#_Toc95386781)

[6.1.1.1 FCS\_CKM Cryptographic Key Management 24](#_Toc95386782)

[6.1.1.2 FCS\_COP Cryptographic Operation 24](#_Toc95386783)

[6.1.2 User Data Protection (FDP) 26](#_Toc95386784)

[6.1.2.1 FDP\_ACC Access Control Policy 26](#_Toc95386785)

[6.1.2.2 FDP\_ACF Access Control Functions 26](#_Toc95386786)

[6.1.2.3 FDP\_ETC Export from the TOE 27](#_Toc95386787)

[6.1.2.4 FDP\_IFC Information Flow Control Policy 27](#_Toc95386788)

[6.1.2.5 FDP\_IFF Information Flow Control Functions 28](#_Toc95386789)

[6.1.2.6 FDP\_ITC Import of User Data with Security Attributes 29](#_Toc95386790)

[6.1.2.7 FDP\_ROL Rollback 30](#_Toc95386791)

[6.1.2.8 FDP\_UCT Inter-TSF User Data Confidentiality Transfer Protection 30](#_Toc95386792)

[6.1.2.9 FDP\_UIT Inter-TSF User Data Integrity Transfer Protection 30](#_Toc95386793)

[6.1.3 Identification and Authentication (FIA) 31](#_Toc95386794)

[6.1.3.1 FIA\_AFL Authentication Failures 31](#_Toc95386795)

[6.1.3.2 FIA\_ATD User Attribute Definition 31](#_Toc95386796)

[6.1.3.3 FIA\_UAU User Authentication 31](#_Toc95386797)

[6.1.3.4 FIA\_UID User Identification 31](#_Toc95386798)

[6.1.4 Security Management (FMT) 32](#_Toc95386799)

[6.1.4.1 FMT\_MOF Management of Functions 32](#_Toc95386800)

[6.1.4.2 FMT\_MSA Management of Security Attributes 32](#_Toc95386801)

[6.1.4.3 FMT\_SMR Security Management Roles 33](#_Toc95386802)

[6.1.4.4 FMT\_SMF Specification of Management Functions 34](#_Toc95386803)

[6.1.5 Protection of the TSF (FPT) 35](#_Toc95386804)

[6.1.5.1 FPT\_FLS Fail Secure 35](#_Toc95386805)

[6.1.5.2 FPT\_SCB TSF Initialisation 35](#_Toc95386806)

[6.1.6 Resource Utilisation (FRU) 35](#_Toc95386807)

[6.1.6.1 FRU\_FLT Fault Tolerance 35](#_Toc95386808)

[6.1.7 Trusted Path/Channels (FTP) 36](#_Toc95386809)

[6.1.7.1 FTP\_TRP Trusted Path 36](#_Toc95386810)

[**6.2** **Security Assurance Requirements** 37](#_Toc95386811)

[**6.3** **Security Requirements Rationale** 38](#_Toc95386812)

[6.3.1 SFR Dependency 38](#_Toc95386813)

[6.3.2 SFR - Objective Rationale 42](#_Toc95386814)

[6.3.3 SAR Rationale 50](#_Toc95386815)

[**7** **TOE SUMMARY SPECIFICATION** 51](#_Toc95386816)

[**7.1** **OTA Firmware Update** 51](#_Toc95386817)

[**7.2** **Profile File Update** 51](#_Toc95386818)

[**7.3** **Local Network Services** 51](#_Toc95386819)

[**7.4** **Secure Communication** 51](#_Toc95386820)

[**7.5** **User Authentication and Operations** 52](#_Toc95386821)

[**7.6** **Secure Boot Operation** 52](#_Toc95386822)

Table 1 Table of Terms

|  |  |
| --- | --- |
| **Terms** | **Description** |
| TOE | Target of Evaluation |
| HTTPs | Hypertext Transfer Protocol Secure |
| OS | Operating System |
| URL | Uniform Resource Locator |
| OTA | Over-The-Air |
| CPU | Central Processing Unit |
| RAM | Random Access Memory |
| PIN | Personal Identification Number |
| TCP | Transmission Control Protocol |
| TV | Television |
| TLS | Transport Layer Security |
| CC | Common Criteria |
| PP | Protection Profile |
| ID | Identification |
| ST | Security Target |
| TEE | Trusted Execution Environment |
| TSF | Trusted Security Functionality |
| Smart TV | Connected TV whose software runs on Linux OS |
| End-user | Defines owner of the Smart TV |
| PIN-code | Is authorization credential defined by end-user |
| General Usage of Smart TV | Defines the usage of features related to Smart services such as YouTube, Netflix etc. and TV operations such as watching a channel, volume UP/DOWN, changing channel etc. |
| The Authorised Identified Roles | The identities such as technical services and developers that can modify device configuration settings |
| Third Party Services | Value added services such as YouTube, Netflix, Amazon Prime etc. |
| Smart TV Trust Manager | The role that is responsible for establishment of TLS. |

Table 2 Document Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| V1.0 | 03.12.2021 | First Draft |
| V1.1 | 18.01.2022 | Revision of Security Functions |
| V1.2 | 28.01.2022 | Revision of SFRs |
| V1.3 | 10.02.2022 | Revision of Extended Component |

# **SECURITY TARGET INTRODUCTION**

## **ST Reference**

|  |  |
| --- | --- |
| **ST Title** | VESTEL SMART TV COMMON FIRMWARE V0.1 Security Target |
| **ST Version** | V1.3 |
| **Date** | 10 February 2022 |

## **TOE Reference**

|  |  |
| --- | --- |
| **TOE Title** | VESTEL SMART TV COMMON FIRMWARE |
| **TOE Version** | V0.1 |

## **TOE Overview**

Smart TV Common Firmware implemented on VESTEL Smart TVs provides security functions. Herewith, TOE’s purpose and key security functions are: OTA Firmware Update, Profile File Update, Local Network Service, Secure Communication, User Authentication and Operations, and Secure Boot Operation. The details are given in the next section.

### TOE Usage and Major Security Features

The TOE provides secure OTA Firmware Update feature to the Smart TV users. The user can be informed in case of that new firmware update image is released when the TOE is on. Then, the user can start the update process by selecting the confirm option. After user confirmation, TOE downloads the firmware update image and installs that image protected by the cryptographic processes given in Table 2. If the user cancels to start update process, TOE informs the user about waiting software update once in 12 hours.

Besides, Smart TV has a service setting that allows to change physical and software features such as debug port enable/disable and connectivity features. Herewith, since this mechanism is used by technical services and development teams, end-users cannot make adjustments of features by changing of this mechanism. In order to ensure authorized access, TOE verifies the configuration file (profile update file) protected by the cryptographic processes given in Table 2. Therefore, an attacker or unauthorized person cannot change physical and software features.

Another feature of the TOE is Local Network Services that allows to pair Smart TV and mobile devices such as smartphone or tablet, connected to the same local network, for enabling second-screen (Smart TV) applications to discover and launch first-screen (mobile devices) applications on first-screen. Herewith, thanks to these services on TV, users can establish communication between Smart TV and third party applications (Netflix, Youtube…) or native Smart TV control purposed mobile application (Smart Center) to share screen between devices, control Smart TV on mobile application instead of remote controller. Moreover, the TOE is protected against security leakages in case of any outages such as, power cut or network issues.

In addition, Smart TV provides an application market that the users can select an application icon on. Herewith, all information such as URL, page, icon etc. about applications such as BBC, FilmBox etc. are stored on VESTEL Portal Clouds. When the user selects an application icon, TOE communicates with VESTEL Portal Server on secure communication channel to get the related information (URL). Then, the application URL is opened on Browser of Smart TV.

Moreover, TOE provides authentication mechanism to the users. The user can easily determine a PIN-code for preventing the unauthorized access to the Smart TV settings. In order to make changes on Smart TV settings, TOE can allow the authorized user by verification of PIN-code inserted by the user. In addition, user can delete user specific configuration and personal data including PIN-code by resetting to factory state.

At last, TOE supports measures against risks about that the device OS has been modified in an unauthorized way. To provide this, the integrity of boot loader, OS kernel, file systems, etc. is verified by using of digital signature verification method during system launches. This process is named as Secure Boot Operation.

Table 3 The Security Functions

|  |  |
| --- | --- |
| **Security Function** | **Description** |
| OTA Firmware Update | This function of TOE is secure software update mechanism over the Air (OTA) that consists of;   * secure communication over TLS between smart TV and the server, * encryption of software image by using symmetric algorithm * integrity verification of encrypted software image before decryption on smart TV, * decryption of encrypted software image before installation of authorized firmware on smart TV, |
| Profile File Update | This function of TOE is secure profile file update mechanism that enables to modify (enable/disable) physical and software features of smart TV. This feature prevents unauthorized profile file installation by the verification of digital signature. |
| Local Network Services | This feature of TOE covers the security of network services and network ports that consist of value-added services. Here with, the feature;   * blocks unauthorized access, * prevents a malicious input, * provides availability, * prevents security leakage in case of any outages. |
| Secure Communication | The TOE provides a secure communication channel for communication between the connected device and the VESTEL Cloud /Server over the newer version of TLS (TLS 1.2). |
| User Authentication and Operations | The TOE requires a PIN-code for user authentication for prevention of unauthenticated user in order to make modification on Settings, Wi-Fi Settings, Connected Services etc. Also, the TOE provides factory reset mechanism in order to delete user specific data. |
| Secure Boot Operation | The TOE supports secure boot operation that consists in authenticating things such as boot loader, OS kernel, file systems that are not expected to change in unauthorized ways, and this is accomplished by verification of cryptographic integrity measurements such as digital signature verification. |

### TOE Type

TOE implemented on VESTEL Smart TVs is an embedded firmware that consists of “OTA Firmware Update”, “Profile File Update”, “Local Network Services”, “Secure Communication”, “User Authentication and Operations” and “Secure Boot Operation” security features.

### Non-TOE Hardware, Software and/or Firmware

|  |  |  |
| --- | --- | --- |
| **Category** | | **Minimum System Requirement** |
| H/W | CPU | Dual Cortex-A9 application processor 1 Ghz |
| RAM | 768 MB |
| Flash Memory | 512 MB |
| Remote Controller | Infrared Remote Controller |
| S/W | OpenSSL | openssl-1.1.1i |
| OS | Linux Kernel revision: 3.10 |
| Mobile Application | Smart Center / Third Party Applications | Requires Android 5.0/iOS 11.0 or later mobile operating systems |

## **TOE Description**

### Physical Scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

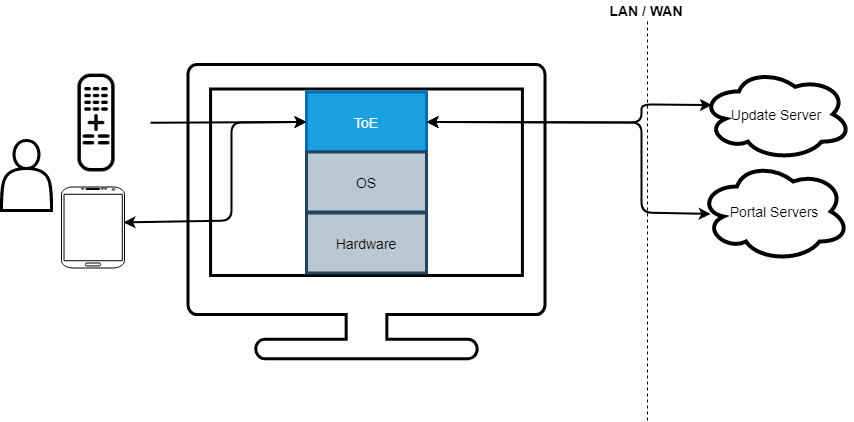


Figure 1 External Entities of the TOE Operational Environment

The user accesses TOE via Mobile Application on local area network by pairing of Mobile Application and Smart TV. After pairing the Mobile Application to Smart TV, the user can control the TV by changing TV channels, setting volume, opening URL on the browser of TV, sharing the screen and selecting application icon on application store. To open application, TOE is connected to portal server for getting the link. In addition, Remote Controller is another access method to TV in order to control it directly. Moreover, the TOE is connected to Update Server in order to download software image. All communications between servers and the TOE are protected by minimum secure version of TLS (TLS 1.2).

The TOE is a firmware element that is a part of Smart TV firmware. The firmware is implemented on Smart TV electronic card on production process. After the production process, Smart TV is delivered to the user and the first installation is performed by VESTEL Service. Also, the User Guide is provided to the user during the delivery.

### Logical Scope of the TOE

The security functions of the TOE are compliant with the technical items of ETSI 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements. The table that matches the requirements of ETSI 303 645 Standard and the TOE can be seen below.

Table 4 The Security Functions' matching with ETSI 303 645 Standards' Items

|  |  |
| --- | --- |
| **The Item of ETSI 303 645 Standard** | **The Security Function of the TOE** |
| No universal default passwords | User Authentication and Operations |
| Implement a means to manage reports of vulnerabilities | N/A. Since the item is non-technical, it is not in the scope of Common Criteria. |
| Keep software updated | OTA Firmware Update |
| Securely store sensitive security parameters | Secure Boot Operation |
| Communicate securely | Secure Communication |
| Minimize exposed attack surfaces | Profile File Update |
| Local Network Services |
| User Authentication and Operations |
| Ensure software integrity | Secure Boot Operation |
| Ensure that personal data is secure | N/A. Since there is no personal data, the item is not in the scope of Common Criteria. |
| Make systems resilient to outages | Local Network Services |
| Examine system telemetry data | N/A. Since there is no telemetry data collected, the item is not in the scope of Common Criteria. |
| Make it easy for users to delete user data | User Authentication and Operations |
| Make installation and maintenance of devices easy | N/A. Since the item is not security-related, it is not in the scope of Common Criteria. |
| Validate input data | Local Network Services |

* OTA Firmware Update

This feature defines the items of security for OTA firmware update. Smart TVs authenticate and connect to update server for checking of their update image periodically. If there is a new signed and encrypted upd0ate image uploaded on server, smart TVs download that image over secure communication protected by using of minimum secure version of TLS (TLS 1.2). After downloading encrypted software update image, the TOE checks the integrity of the image by verification of digital signature, and then decrypt the image. After completed of these processes, authorized software update image is installed on smart TVs.

* Profile File Update

This feature defines the items of security for profile file update for enable/disable physical and logical features. A USB memory that includes signed profile file is plugged on smart TVs, smart TV downloads the signed profile file over USB by trigger of USB operation option on smart TV settings. After downloading profile update file, the TOE checks the integrity of the file by verification of digital signature. After completed of these processes, authorized profile update file is updated on smart TVs.

* Local Network Services

This feature of TOE covers the security of network services and network ports that consist of value-added services. Herewith, the feature blocks unauthorized access, prevents a malicious input and injection attacks, provides availability for that the connection between Smart TV and third party applications (Netflix, YouTube etc.) or native Smart TV control purposed mobile application (Smart Center) is established to share screen between devices, control Smart TV on mobile application instead of remote controller. On the other hand, the TOE is protected against security leakages in case of any outages such as, power cut or network issues.

* Secure Communication

Smart TV can connect to VESTEL Portal Server that provides the information about the application URL. When user wants to open an application. Herewith, the connection between smart TV and VESTEL Portal Server is secured by minimum secure version of TLS (TLS 1.2).

* User Authentication and Operations

The feature of TOE provides a user authentication and verification mechanisms based on a PIN-code determined by users during the first time installation of Smart TV. Before making of modification on Settings, Wi-Fi Settings, Connected Services etc. user should authenticate to the Smart TV for prevention of unauthenticated access. Also, the feature prevents brute force attacks by blocking the attempts for 30 minutes after 5 failure attempts. In addition, factory reset mechanism is provided for deletion of user specific data.

* Secure Boot Operation

The feature of the TOE provides integrity verification of OS during OS is launching and this feature prevents manipulating items on OS by unauthorized access. In this process, there are verification operations based on master keys in secure area, boot loader verification and, signature verification OS boot. The public keys used in integrity verification process of boot loader and signature verification of OS are stored encrypted and verified by master public key before used. In this process, after the integrity of public key is verified, the integrity of OS is verified and checked against any manipulation on OS by signature verification by public keys.

# **CONFORMANCE CLAIM**

## **CC Conformance Claim**

This ST and TOE claims conformance to

• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, and Revision 5, April 2017

• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017

• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017

As conformance claim is as follows:

* Part 2 extended
* Part 3 conformant

Has to be taken into account.

## **PP Claim**

This ST does not claim conformance to any protection profile

## **Package Claim**

Evaluation Assurance Level is EAL2-conformant.

## **Conformance Claim Rationale**

Since the Security Target does not claim any conformance with any Protection Profiles, there is no conformance rationale provided here.

# **SECURITY PROBLEM DEFINITION**

## **Overview**

The security problem describes the nature of the security problem that the TOE is designed to address. It is described through:

a) a series of threats that the TOE has been designed to mitigate,

b) any relevant organizational security policies statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

c) specific assumptions about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

The assets implemented in the Smart TV are as follows.

* OTA Update Image of Smart TV.
* Profile Update File of Smart TV.
* Local Network Service Interfaces and Network Ports
* Encryption keys for secure communication
* User PIN-code
* TV Settings
* Application URL
* Security services provided by the TOE

## **Threats**

The threat agents are described below;

• Attackers who have knowledge of how the TOE operates and are assumed to possess a basic skill level, and intend to alter TOE configuration settings/parameters and no physical access to the TOE.

The TOE addresses the following threats are applicable listed in table below;

|  |  |
| --- | --- |
| **Identifier** | **Threat Statement** |
| **T.UnverifiedUptImg** | Attacker could gain unauthorized access to the OTA Update Image of Smart TV by by-passing the verification of signature requirements. |
| **T.ModifyUptImg** | Attacker may send a malicious software update image to the TOE by intercepting of secure communication between the server and the TOE. |
| **T.UnverifiedPrfUpt** | Attacker could gain unauthorized access to the Profile Update File of Smart TV by bypassing the verification of signature requirements. |
| **T.ModifyPrfUpt** | Attacker may send a malicious profile update file instead of Profile Update File of Smart TV by using of USB memory to gain the access right by changing of physical and software features. |
| **T.MITM** | Attacker may eavesdrop the messages between the TOE and the servers by manipulating of Encryption keys for secure communication. |
| **T.ModifyInpt** | Attacker could gain unauthorized access to the Local Network Service Interfaces and Network Ports by sending a malicious input or commands. |
| **T.Unauth** | An unauthorized person may attempt to by-pass authentication mechanism of the PIN-code verification for changing of TV settings. |
| **T.UnautBrtFrc** | Attacker may capture the user’s PIN-code by applying of brute force attack. |
| **T.FakeUrl** | Attacker may send a fake URL of application by manipulating of secure communication between the TOE and VESTEL Portal servers. |
| **T.ModifyOS** | Attacker may bypass TSF by modifying OS in an unauthorized access. |
| **T.Outages** | Attacker may take an advantage of security leakages that occurs because of outages. |
| **T.OwnershipTransfer** | Attacker may take the information when Smart TV is sold to another user (potential attacker) without deleting the personal data before ownership transfer process. |

## **Organizational Security Policies**

|  |  |
| --- | --- |
| **Identifier** | **Policy Statement** |
| **P.UptStrategy** | The secure firmware update procedure is given in “Software Update Strategy” document. |

## **Assumptions**

The assumptions are described in below;

|  |  |
| --- | --- |
| **Identifier** | **Assumption Statement** |
| **A.ScrUptSrvr** | It is assumed that, for secure operation of TOE, the VESTEL update server which exists in the operating environment is operated securely. |
| **A.ScrPrtlSrvr** | It is assumed that, for secure operation of TOE, the VESTEL portal server which exists in the operating environment is operated securely. |
| **A.SignTool** | It is assumed that, for the sign process of software update image and profile update file, the sign tool is accessed by an authorized person. Also, this tool stores the private keys securely. |
| **A.MobileApp** | It is assumed that, all third party applications and Smart Center are secure and have no vulnerabilities. |
| **A.Ports** | It is assumed that, all unnecessary and unused ports and services are closed or disable. |
| **A.User** | It Is assumed that, the user protects the PIN-code and never shares it with others. |
| **A.Protocol** | It is assumed that, all application protocols used in Local Network Services have no vulnerabilities, they are secure. |

# **SECURITY OBJECTIVES**

## **Overview**

The security objectives are concise statement of the expected response to the safety issues defined in Section 3. They are the safety goals addressed by the TOE and additional goals that provide specific directions for the anticipated environment in which the TOE will operate.

## **Security Objectives for the TOE**

|  |  |
| --- | --- |
| **Identifier** | **Objective Statement** |
| **O.SWUptImgVerification** | The TOE verifies that the software update image to be installed on the product is an authorized package through digital signature verification and there is no unauthorized modification during installation process. |
| **O.SWUptImgProtection** | The software update image is signed with asymmetric algorithms and then encrypted with a symmetric encryption algorithm. Herewith, the TOE stores software update image downloaded in an encrypted form on the product, and before the image is installed, the TOE verifies its integrity and decrypts the encrypted software update image. |
| **O.PrflUptFileVerification** | The TOE verifies that the profile update files to be installed on the product is an authorized package through digital signature verification and there is no unauthorized modification during installation process. |
| **O.ScrCommunication** | The TOE connects to update server and portal server by using of the minimum secure version of TLS (TLS 1.2) to prevent MITM attacks and intercept the messages. |
| **O.InptVerification** | The TOE verifies the input sent on local area network to listen TCP ports for preventing injection attacks and malicious inputs. |
| **O.UserAuth** | The TOE verifies the users before they access the TV settings. The TOE blocks the user for the next 30 minutes after 5 failure attempts are occurred. |
| **O.ScrBoot** | The TOE verifies the integrity of OS before it is launched by digital signature verification and there is no unauthorized modification during initializing process. |
| **O.DataDeletion** | The TOE allows user to delete personal data. |
| **O.Outages** | The TOE ensures that the TOE maintains expected operations of all capabilities even after the event of failures/outages. |

## **Security Objectives for Operational Environment**

|  |  |
| --- | --- |
| **Identifier** | **Objective Statements** |
| **OE.UserAuth** | Users are responsible for protection of PIN-code. The PIN-code will not be stored in the operational environment in an exposed way, thus it can’t be accessed by any third party. |
| **OE.ScrCommunicationChannel** | A secure communication channel is provided for communication between the Smart TV and the VESTEL servers by using of the minimum secure version of TLS (TLS 1.2). |
| **OE.ProductUniqueID** | Smart TVs must have unique IDs to manage them securely. This ID is used to identify the product uniquely in VESTEL servers. |
| **OE.ScrPrivateKey** | All private keys for sign process of software update image and profile update file are stored securely. |
| **OE.Port** | Unnecessary local network services and network ports are closed. |
| **OE.MobileApp** | All third party applications and Smart Center are up-to-date with no vulnerabilities. |
| **OE.Protocol** | All application protocols used in Local Network Services are up-to-date with no vulnerabilities. |
| **OE.ScrBoot** | All credentials such as signature value, keys related to Secure Boot Operation are stored in secure area. |

## **Security Objectives Rationale**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **THREATS** | | | | | | | | | | | | **OSP** | **ASSUMPTIONS** | | | | | | |
| T.UnverifiedUptImg | T.ModifyUptImg | T.UnverifiedPrfUpt | T.ModifyPrfUpt | T.MITM | T.ModifyInpt | T.Unauth | T.UnautBrtFrc | T.FakeUrl | T.ModifyOS | T.Outages | T.OwnershipTransfer | P.UptStrategy | A.ScrUptSrvr | A.ScrPrtlSrvr | A.SignTool | A.MobileApp | A.Ports | A.User | A.Protocol |
| **SECURITY OBJECTIVES FOR TOE** | O.SWUptImgVerification | √ | √ |  |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |
| O.SWUptImgProtection |  | √ |  |  | √ |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |
| O.PrflUptFileVerification |  |  | √ | √ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| O.ScrCommunication |  |  |  |  | √ |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |  |
| O.InptVerification |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| O.UserAuth |  |  |  |  |  |  | √ | √ |  |  |  |  |  |  |  |  |  |  |  |  |
| O.DataDeletion |  |  |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |
| O.Outages |  |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |
| O.ScrBoot |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |
| **SECURITY OBJ. FOR OP. ENVIRONMENT** | OE.UserAuth |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |  | √ |  |
| OE.ScrCommunicationChannel |  |  |  |  | √ |  |  |  |  |  |  |  |  | √ | √ |  |  |  |  |  |
| OE.ProductUniqueID |  |  |  |  |  |  |  |  |  |  |  |  |  | √ | √ |  |  |  |  |  |
| OE.ScrPrivateKey | √ |  | √ |  |  |  |  |  |  |  |  |  | √ |  |  | √ |  |  |  |  |
| OE.Port |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | √ |  |  |
| OE.MobileApp |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | √ |  |  |  |
| OE.Protocol |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | √ |
| OE.ScrBoot |  |  |  |  |  |  |  |  |  | √ |  |  |  |  |  |  |  |  |  |  |

**O.SWUptImgVerification:**

This security objective ensures that only the authenticated OTA package is downloaded to the product via digital signature verification by the TOE. This security objective enables preventing the threats T.UnverifiedUptImg and T.ModifyUptImg. It also addresses P.UptStrategy since the secure firmware update procedure is given in “Software Update Strategy” document.

**O.SWUptImgProtection**

This security objective addresses the threat T.ModifyUptImg and T.MITM by preventing unauthorized access such as illegal copying of product firmware source codes, etc. by encrypting files of the OTA package downloaded on the product. As it also addresses P.UptStrategy since the secure firmware update procedure is given in “Software Update Strategy” document.

**O.PrflUptFileVerification:**

This security objective ensures that only the authenticated profile file is downloaded to the product via digital signature verification by the TOE. This security objective enables preventing the threat T.UnverifiedPrfUpt. It also addresses T.ModifyPrfUpt by preventing unauthorized use such as illegal copying of product firmware source codes, etc. by encrypting files of the profile file downloaded on the product.

**O.ScrCommunication:**

This security objective addresses the threats T.MITM and T.FakeURL since it prevents manipulation of encryption keys by connecting to update and portal servers with usage of the minimum secure version of TLS.

**O.InptVerification:**

This security objective addresses the threat T.ModifyInpt since it prevents injection attacks and malicious inputs by verifying the input sent on local area network to listen open TCP ports.

**O.UserAuth:**

This security objective addresses the threat T.Unauth by verifying the users before they access the TV settings. It also addresses the threat T.UnautBrtFrc by blocking the user for the next 30 minutes after 5 failure attempts are occurred.

**O.ScrBoot:**

This security objective addresses the threat T.ModifyOS by verifying the integrity of OS during the launching process and preventing the modified OS launch.

**O.Outages:**

This security objective addresses the threat T.Outages by maintaining expected operations of all capabilities after the event of failures/outages.

**O.DataDeletion**

This security objective addresses the threat T.OwnershipTransfer by allowing user to delete personal data via factory reset option.

**OE.UserAuth:**

This security objective for operational environment addresses the assumption A.User since users are responsible for the protection of PIN-code and it is assumed that users protect it. In addition, it addresses the threat T.Unauth by verifying the users before they access the TV settings.

**OE.ScrCommunicationChannel:**

This security objective for operational environment addresses the assumption A.ScrUptSrvr and A.ScrPrtlSrvr since it provides a secure communication between the Smart TV and the VESTEL servers by using of the minimum secure version of TLS (TLS 1.2). The security objective also addresses threat T.MITM as it prevents man in the middle attack by secure communication.

**OE.ProductUniqueID:**

This security objective for operational environment addresses the assumption A.ScrUptSrvr and A.ScrPrtlSrvr since Smart TVs have unique IDs in order to manage them securely and identify the product uniquely in VESTEL servers.

**OE.ScrPrivateKey:**

This security objective for operational environment addresses the threats T.UnverifiedUptImg and T.UnverifiedPrfUpt since all private keys for sign process of software update image and profile update file are stored securely. It also addresses the assumption A.SignTool by storing the private keys securely. Moreover, this security objective is covered under “Software Update Strategy” that is identified as P.UptStrategy.

**OE.Port:**

This security objective for operational environment addresses the assumption A.Ports since unnecessary local network services and network ports are closed.

**OE.MobileApp:**

This security objective for operational environment addresses the assumption A.MobileApp since all third party applications and Smart Center are up-to-date with no vulnerabilities.

**OE.Protocol:**

This security objective for operational environment addresses the assumption A.Protocol since all application protocols used in Local Network Services are up-to-date with no vulnerabilities.

**OE.ScrBoot:**

This security objective for operational environment addresses the threat T.ModifyOS since the objective provides verification of cryptographic integrity.

# **EXTENDED COMPONENT DEFINITION**

## **Extended Family FPT\_SCB – TSF initialisation**

### Family behavior

To define the security functional requirements of the TOE an additional family (FPT\_SCB) of the Class FPT (Protection of the TSF) is introduced here. This family describes the functional requirements for the initialization of the TSF by a dedicated function of the TOE that ensures the integrity of OS before the OS launch.

### Component levelling

**FPT\_SCB: TSF initialisation**

**1**

FPT\_SCB.1 TSF initialisation, requires that an integrity check of the boot image is performed prior to the first operational usage after a power-on.

### Management: FPT\_ SCB.1

There are no management activities foreseen.

### Audit: FPT\_ SCB.1

There are no auditing activities foreseen.

The family TSF Initialization (FPT\_SCB) is specified as follows.

### FPT\_SCB.1 TSF Initialisation

|  |  |
| --- | --- |
| Hierarchical to: | No other components. |
| Dependencies: | No other components. |
| **FPT\_SCB.1.1** | **The TSF shall provide secure initialization function that brings it into a secure operational state at** **[assignment:** *list of TOE states***]** **by verification of [assignment:** *list of firmware, software, or data***] [selection:** *integrity, authenticity, unicity***].** |
| **FPT\_SCB.1.2** | **The TSF initialization function is verified by [assignment:** *type of cryptographic keys***] [assignment:** *list of properties***].** |
| **FPT\_SCB.1.3** | **The TSF shall provide** **[assignment:** *list of TOE capabilities***]** |
| **FPT\_SCB.1.4** | **The TSF shall perform [assignment:** *type of cryptographic key access***] in accordance with a specified cryptographic key access method [assignment:** *cryptographic key access method***] that meets the following: [assignment:** *list of standards***].** |
| **FPT\_SCB.1.5** | **The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE either successfully completes initialization or is halted.** |
| **FPT\_SCB.1.6** | **The TOE initialization function shall not be able to arbitrarily interact with the TSF after TOE initialization completes.** |

# **SECURITY REQUIREMENTS**

**Overview**

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

• Assignment: The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment].**

• Selection: The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows ***[selection].***

• Refinement: The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for additions, and strike-through, for deletions.

• Iteration: The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP\_IFF.1 (a) and FDP\_IFF.1 (b). Each letter represents a security functions where:

* OTA Firmware Update is (a),
* Profile File Update is (b),
* Local Network Service is (c),
* Secure Communication is (d) and
* User Authentication and Operations is (e).
* Secure Boot Operation (f).

Another usage of iteration is as follows FCS\_COP.1 (1) and FCS\_COP.1 (2). In this case, numbers represent the method that is used to correspond the SFRs such as RSA, AES, and Decryption etc.

## **Security Functional Requirements**

This section specifies the security functional requirements for the TOE. It organizes the SFRs by the CC classes.

Table 5 Description of Security Function Policies

|  |  |
| --- | --- |
| **Security Function Policies (SFPs)** | **Description** |
| Smart TV flow control | This flow control policy corresponding with FDP\_IFC.1 (a), FDP\_IFF.1 (a) and FMT\_MSA.3 defines control mechanism between client and local network services on Smart TV. |
| Access control | This flow control policy corresponding with FDP\_ACF.1 , FDP\_ACC.1 defines user access policy to Smart TV settings features. |
| VESTEL Cloud flow control | This flow control policy corresponding with OTA Firmware Update related SFRs defines access policy between TOE and VESTEL Clouds. |
| Profile file update access control | This flow control policy corresponding with FMT\_MOF.1 defines access policy for profile update file download. |

Table 6 Description of Security Function Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement Class** | **Requirement Identifier** | | **Requirement Title** |
| FTP: Trusted Paths/Channels | | FTP\_TRP.1 (a) | Trusted Path |
| FTP\_TRP.1 (d) | Trusted Path |
| FDP: User Data Protection | | FDP\_ACC.1 (e) | Subset Access Control |
| FDP\_ACC.1 (a-f) | Subset Access Control |
| FDP\_ACF.1 (a-f) | Security attribute based access control |
| FDP\_ACF.1 (e) | Security attribute based access control |
| FDP\_ETC.2 (a) | Export of User Data with Security Attributes |
| FDP\_IFC.1 (a) | Subset Information Flow Control |
| FDP\_IFC.1 (c) | Subset Information Flow Control |
| FDP\_IFC.1 (d) | Subset Information Flow Control |
| FDP\_IFF.1 (a) | Simple Security Attributes |
| FDP\_IFF.1 (c) | Simple Security Attributes |
| FDP\_IFF.1 (d) | Simple Security Attributes |
| FDP\_ITC.2 (a-b) | Import of User Data with Security Attributes |
| FDP\_ROL.1 | Basic Rollback |
| FDP\_UCT.1 (a) | Basic data exchange confidentiality |
| FDP\_UCT.1 (d) | Basic data exchange confidentiality |
| FDP\_UIT.1 (a) | Data exchange integrity |
| FMT: Security Management | | FMT\_MOF.1 (b) | Management of Security Functions |
| FMT\_MSA.1 (e) | Management of Security Attributes |
| FMT\_MSA.1 (d) | Management of Security Attributes |
| FMT\_MSA.3 (a-c) | Static Attribute Initialization |
| FMT\_MSA.3 (e) | Static Attribute Initialization |
| FMT\_MSA.3 (d) | Static Attribute Initialization |
| FMT\_SMF.1 (b-c) | Specification of Management Functions |
| FMT\_SMF.1 (e) | Specification of Management Functions |
| FMT\_SMF.1 (d) | Specification of Management Functions |
| FMT\_SMR.1(c) | Security Roles |
| FMT\_SMR.1(e) | Security Roles |
| FMT\_SMR.1 (b) | Security Roles |
| FMT\_SMR.1 (d) | Security Roles |
| FCS: Cryptographic Support | | FCS\_COP.1(a.1) | Cryptographic Operation / RSA |
| FCS\_COP.1(a.2) | Cryptographic Operation / AES |
| FCS\_COP.1(a.3) | Cryptographic Operation / HASH |
| FCS\_COP.1(b.1) | Cryptographic Operation / RSA |
| FCS\_COP.1(b.2) | Cryptographic Operation / HASH |
| FCS\_CKM.3 (a.1) | Cryptographic Key Management / Decryption |
| FCS\_CKM.3 (a-f.2) | Cryptographic Key Management / Signature Verification OTA |
| FCS\_CKM.3 (b.2) | Cryptographic Key Management / Signature Verification  Profile |
| FIA: Identification and Authentication | | FIA\_ATD.1 (e) | User attribute definition |
| FIA\_AFL.1 (e) | Authentication Failure |
| FIA\_UAU.1 (e) | User Authentication |
| FIA\_UID.1 (e) | User Identification |
| FIA\_UID.1 (c) | User Identification |
| FIA\_UID.1 (b) | User Identification |
| FPT: Protection of the TSF | | FPT\_FLS.2 (c) | Fail Secure |
| FPT\_SCB.1 (f) | Secure Boot |
| FRU: Resource Utitisation | | FRU\_FLT.2 (c) | Fault Tolerance |

### Cryptographic Support (FCS)

#### FCS\_CKM Cryptographic Key Management

|  |  |
| --- | --- |
| **FCS\_CKM.3 (a.1) Cryptographic key access / Decryption – OTA Firmware Update** | |
| 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\_CKM.3.1 | The TSF shall perform **[cryptographic key escrow]** in accordance with a specified cryptographic key access method **[internal secure storage read]** that meets the following : **[None].** |

|  |  |
| --- | --- |
| **FCS\_CKM.3 (a-f.2) Cryptographic key access / Signature Verification - OTA Firmware Update / Secure Boot Operation** | |
| 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\_CKM.3.1 | The TSF shall perform **[escrow]** in accordance with a specified cryptographic key access method **[internal secure storage read]** that meets the following: **[None].** |

|  |  |
| --- | --- |
| **FCS\_CKM.3 (b.2) Cryptographic key access / Signature Verification – Profile File Update** | |
| 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\_CKM.3.1 | The TSF shall perform **[archive]** in accordance with a specified cryptographic key access method **[internal secure storage read]** that meets the following: **[None].** |

#### FCS\_COP Cryptographic Operation

|  |  |
| --- | --- |
| **FCS\_COP.1 (a-f.1) Cryptographic Operation / RSA – OTA Firmware Update / Secure Boot Operation** | |
| 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 **[signature verification]** in accordance with a specified cryptographic algorithm **[RSA PKCS v2.1 ]** and cryptographic key sizes **[2048]** that meet the following: **[RFC 3447].** |

|  |  |
| --- | --- |
| **FCS\_COP.1 (a.2) Cryptographic Operation / AES – OTA Firmware Update** | |
| 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 **[Encryption AND Decryption of OTA firmware update image]** in accordance with a specified cryptographic algorithm **[AES-CBC]** and cryptographic key sizes **[256]** that meet the following: **[FIPS 197]** |

|  |  |
| --- | --- |
| **FCS\_COP.1 (a.3) Cryptographic Operation / HASH – OTA Firmware Update** | |
| 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 **[Hash value generation of OTA firmware update image]** in accordance with a specified cryptographic algorithm **[SHA-256]** and cryptographic key sizes **[None]** that meet the following: **[FIPS 180-4].** |

|  |  |
| --- | --- |
| **FCS\_COP.1 (b.1) Cryptographic Operation / RSA – Profile File Update** | |
| 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 **[Verification of the signature for profile file update image]** in accordance with a specified cryptographic algorithm **[RSA PKCS v2.1]** and cryptographic key sizes **[4096]** that meet the following: **[RFC 3447].** |

|  |  |
| --- | --- |
| **FCS\_COP.1 (b.2) Cryptographic Operation / HASH – Profile File Update** | |
| 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 **[Hash value generation of Profile file update image]** in accordance with a specified cryptographic algorithm **[SHA-256]** and cryptographic key sizes **[None]** that meet the following: **[FIPS 180-4].** |

### User Data Protection (FDP)

#### FDP\_ACC Access Control Policy

|  |  |
| --- | --- |
| **FDP\_ACC.1 (e) Subset Access Control – User Authentication and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_ACF.1 Security attribute based access control |
| FDP\_ACC.1.1 | The TSF shall enforce the **[Access control SFP]** on **[Subject: end-user, Object: PIN-code, Operation: Authentication].** |

|  |  |
| --- | --- |
| **FDP\_ACC.1 (a-f) Subset Access Control – OTA Firmware Update / Secure Boot Operation** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_ACF.1 Security attribute based access control |
| FDP\_ACC.1.1 | The TSF shall enforce the **[Access control SFP]** on **[Subject: signature verification function of the TOE, Operation: signature verification, Object: integrity].** |

#### FDP\_ACF Access Control Functions

|  |  |
| --- | --- |
| **FDP\_ACF.1 (a-f) Security attribute based access control – OTA Firmware Update / Secure Boot Operation** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_ACC.1 Subset access control  FMT\_MSA.3 Static attribute initialization |
| FDP\_ACF.1.1 | The TSF shall enforce the **[Access control SFP, VESTEL Cloud Flow Control SFP]** to objects based on the following: **[Subject: signature verification function of the TOE, Objects: OTA Firmware Update image; Boot image, Security attributes: digital signatures and hash values].** |
| FDP\_ACF.1.2 | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[When the integrity of the object is verified, then access is granted on the image].** |
| FDP\_ACF.1.3 | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[None].** |
| FDP\_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None].** |

|  |  |
| --- | --- |
| **FDP\_ACF.1 (e) Security attribute based access control – User Authentication and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_ACC.1 Subset access control  FMT\_MSA.3 Static attribute initialization |
| FDP\_ACF.1.1 | The TSF shall enforce the **[Access control SFP]** to objects based on the following: **[Subject: User, Object: Settings, Security attribute: PIN-code digits].** |
| FDP\_ACF.1.2 | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[When the user requests to access Smart TV Settings for making adjustment, Smart TV forces the user to enter a PIN-code that is determined on first-time installation of Smart TV. If Smart TV verifies the user PIN-code, the user is granted access].** |
| FDP\_ACF.1.3 | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[None].** |
| FDP\_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None].** |

#### FDP\_ETC Export from the TOE

|  |  |
| --- | --- |
| **FDP\_ETC.2 (a) Export of User Data with Security Attributes – OTA Firmware Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control] |
| FDP\_ETC.2.1 | The TSF shall enforce the **[VESTEL Cloud Flow Control SFP]** when exporting user data, controlled under the SFP(s), outside of the TOE. |
| FDP\_ETC.2.2 | The TSF shall export the user data with the user data's associated security attributes. |
| FDP\_ETC.2.3 | The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data. |
| FDP\_ETC.2.4 | The TSF shall enforce the following rules when user data is exported from the TOE: **[None].** |

#### FDP\_IFC Information Flow Control Policy

|  |  |
| --- | --- |
| **FDP\_IFC.1 (c) Subset information flow control / Local Network Service** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_IFF.1 Simple security attributes |
| FDP\_IFC.1.1 | The TSF shall enforce the **[Smart TV flow control SFP]** on **[Subject: Network Local Services, Information: Network Ports Operation: Send/Receive].** |

|  |  |
| --- | --- |
| **FDP\_IFC.1 (a) Subset information flow control / OTA Firmware Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_IFF.1 Simple security attributes |
| FDP\_IFC.1.1 | The TSF shall enforce the **[VESTEL Cloud flow control SFP]** on **[Subject: VESTEL Cloud and Smart TV, Information: OTA firmware update image, Operation: Send].** |

|  |  |
| --- | --- |
| **FDP\_IFC.1 (d) Subset information flow control / Secure Communication** | |
| Hierarchical to: | No other components. |
| Dependencies: | FDP\_IFF.1 Simple security attributes |
| FDP\_IFC.1.1 | The TSF shall enforce the **[VESTEL Cloud flow control SFP]** on **[Subject: VESTEL Portal Server and Smart TV, Information: encrypted messages, Operation: Send/Receive].** |

#### FDP\_IFF Information Flow Control Functions

|  |  |
| --- | --- |
| **FDP\_IFF.1 (c) Simple security attributes / Local Network Services** | |
| 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 **[Smart TV flow control SFP]** based on the following types of subject and information security attributes: **[Subject: Network Local Services , Information: Network Ports, Security attribute: Input whitelist** |
| 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: **[TOE verifies inputs by checking of white listing command before the permission is given].** |
| 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: **[None].** |
| FDP\_IFF.1.5 | The TSF shall explicitly deny an information flow based on the following rules: **[checking of white-list].** |

|  |  |
| --- | --- |
| **FDP\_IFF.1 (a) Simple security attributes / OTA Firmware Update** | |
| 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 **[VESTEL Cloud flow control SFP and Smart TV flow control SFP]** based on the following types of subject and information security attributes: **[Subject:signature verification function of the TOE, Information: OTA firmware update image, security attributes: digital signatures and hash values].** |
| 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: **[TOE verifies inputs by checking the integrity and authenticity of the OTA Firmware Update image].** |
| 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: **[None].** |
| FDP\_IFF.1.5 | The TSF shall explicitly deny an information flow based on the following rules: **[None].** |

|  |  |
| --- | --- |
| **FDP\_IFF.1 (d) Simple security attributes / Secure Communication** | |
| 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 **[VESTEL Cloud flow control SFP and Smart TV flow control SFP]** based on the following types of subject and information security attributes: **[Subject: VESTEL Cloud and Smart TV, Information: Message, Security attribute: Encrypted message.]** |
| 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: **[TOE verifies inputs by checking the confidentiality of messages between cloud and Smart TV].** |
| FDP\_IFF.1.3 | The TSF shall enforce the **[Encryption].** |
| FDP\_IFF.1.4 | The TSF shall explicitly authorize an information flow based on the following rules: **[None].** |
| FDP\_IFF.1.5 | The TSF shall explicitly deny an information flow based on the following rules: **[None].** |

#### FDP\_ITC Import of User Data with Security Attributes

|  |  |
| --- | --- |
| **FDP\_ITC.2 (a-b) Import of user data with security attributes - OTA Firmware Update / Profile File Uptdate** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control]  [FTP\_ITC.1 Inter-TSF trusted channel, or  FTP\_TRP.1 Trusted path]  FPT\_TDC.1 Inter-TSF basic TSF data consistency |
| FDP\_ITC.2.1 | The TSF shall enforce the **[VESTEL Cloud Flow Control SFP]** when importing user data, controlled under the SFP, from outside of the TOE. |
| FDP\_ITC.2.2 | The TSF shall use the security attributes associated with the imported user data. |
| FDP\_ITC.2.3 | The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. |
| FDP\_ITC.2.4 | The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. |
| FDP\_ITC.2.5 | The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[None].** |

#### FDP\_ROL Rollback

|  |  |
| --- | --- |
| **FDP\_ROL.1 Basic rollback** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control] |
| FDP\_ROL.1.1 | The TSF shall enforce **[Access control SFP]** to permit the rollback of the **[return to factory settings state]** on the **[TOE].** |
| FDP\_ROL.1.2 | The TSF shall permit operations to be rolled back within the **[specific settings and data deletion].** |

#### FDP\_UCT Inter-TSF User Data Confidentiality Transfer Protection

|  |  |
| --- | --- |
| **FDP\_UCT.1 (a) Basic data exchange confidentiality - OTA Firmware Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FTP\_ITC.1 Inter-TSF trusted channel, or  FTP\_TRP.1 Trusted path]  [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control] |
| FDP\_UCT.1.1 | The TSF shall enforce the **[VESTEL Cloud information flow control SFP]** to ***[selection: transmit***] user data in a manner protected from unauthorized disclosure. |

|  |  |
| --- | --- |
| **FDP\_UCT.1 (d) Basic data exchange confidentiality - Secure Communication** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FTP\_ITC.1 Inter-TSF trusted channel, or  FTP\_TRP.1 Trusted path]  [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control] |
| FDP\_UCT.1.1 | The TSF shall enforce the **[VESTEL Portal Cloud information flow control SFP]** to ***[transmit, receive***] user data in a manner protected from unauthorized disclosure. |

#### FDP\_UIT Inter-TSF User Data Integrity Transfer Protection

|  |  |
| --- | --- |
| **FDP\_UIT.1 (a) Data exchange integrity - OTA Firmware Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | [FDP\_ACC.1 Subset access control, or  FDP\_IFC.1 Subset information flow control]  [FTP\_ITC.1 Inter-TSF trusted channel, or  FTP\_TRP.1 Trusted path] |
| FDP\_UIT.1.1 | The TSF shall enforce the **[VESTEL Cloud information flow control SFP]** to ***[receive]*** user data in a manner protected from ***[modification, insertion]*** errors. |
| FDP\_UIT.1.2 | The TSF shall be able to determine on receipt of user data, whether ***[modification, insertion]*** has occurred. |

### Identification and Authentication (FIA)

#### FIA\_AFL Authentication Failures

|  |  |
| --- | --- |
| **FIA\_AFL.1 (e) Authentication failure handling – User Authentication** **and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UAU.1 Timing of authentication |
| FIA\_AFL.1.1 | The TSF shall detect when ***[5]*** unsuccessful authentication attempts occur related to **[user authentication].** |
| FIA\_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall **[blocking for 30 minutes].** |

#### FIA\_ATD User Attribute Definition

|  |  |
| --- | --- |
| **FIA\_ATD.1 (e) User attribute definition – User Authentication** **and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA\_ATD.1.1 | The TSF shall maintain the following list of security attributes belonging to individual users: **[user rights, number of PIN-code digits.]** |

#### FIA\_UAU User Authentication

|  |  |
| --- | --- |
| **FIA\_UAU.1 (e) Timing of authentication – User Authentication** **and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FIA\_UAU.1.1 | The TSF shall allow **[General usage of Smart TV]** on behalf of the user to be performed before the user is authenticated. |
| FIA\_UAU.1.2 | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. |

#### FIA\_UID User Identification

|  |  |
| --- | --- |
| **FIA\_UID.1 (e) Timing of identification – User Authentication** **and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA\_UID.1.1 | The TSF shall allow **[General usage of Smart TV**] on behalf of the user to be performed before the user is identified. |
| FIA\_UID.1.2 | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

|  |  |
| --- | --- |
| **FIA\_UID.1 (c) Timing of identification – Local Network Services** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA\_UID.1.1 | The TSF shall allow **[usage of Smart TV via mobile application**] on behalf of the user to be performed before the user is identified. |
| FIA\_UID.1.2 | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

|  |  |
| --- | --- |
| **FIA\_UID.1 (b) Timing of identification – Profile Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA\_UID.1.1 | The TSF shall allow **[General settings modification of Smart TV**] on behalf of the user to be performed before the user is identified. |
| FIA\_UID.1.2 | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

### Security Management (FMT)

#### FMT\_MOF Management of Functions

|  |  |
| --- | --- |
| **FMT\_MOF.1 (b) Management of Security Functions - Profile File Update** | |
| 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 ***[enable/disable the behaviour of]*** the functions **[connectivity options, value-added services, test and debug options, storage services, under-pinning services]** to **[the authorised identified roles].** |

#### FMT\_MSA Management of Security Attributes

|  |  |
| --- | --- |
| **FMT\_MSA.1 (e) Management of Security Attributes – User Authentication** **and Operations** | |
| 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 **[Access control SFP]** to restrict the ability to ***[selection: change\_default, modify, [None]]*** the security attributes **[PIN-code]** to **[end-user].** |

|  |  |
| --- | --- |
| **FMT\_MSA.1 (d) Management of Security Attributes – Secure Communication** | |
| 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 **[Vestel Cloud access control SFP]** to restrict the ability to ***[selection: change\_default, modify, [None]]*** the security attributes **[Encryption credentials]** to **[Smart TV].** |

|  |  |
| --- | --- |
| **FMT\_MSA.3 (a-c) Static Attribute Initialization – Local Network Services/OTA Firmware Update** | |
| 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 **[Smart TV flow control *SFP*]** to provide ***[Restrictive]*** default values for security attributes that are used to enforce the SFP. |
| FMT\_MSA.3.2 | The TSF shall allow the **[*None*]** to specify alternative initial values to override the default values when an object or information is created. |

|  |  |
| --- | --- |
| **FMT\_MSA.3 (e) Static Attribute Initialization – User Authentication** **and Operations** | |
| 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 **[End-user access control SFP]** to provide ***[Restrictive]*** default values for security attributes that are used to enforce the SFP. |
| FMT\_MSA.3.2 | The TSF shall allow the **[*None*]** to specify alternative initial values to override the default values when an object or information is created. |

|  |  |
| --- | --- |
| **FMT\_MSA.3 (d) Static Attribute Initialization – Secure Communication** | |
| 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 **[VESTEL Cloud flow control SFP]** to provide ***[Restrictive]*** default values for security attributes that are used to enforce the SFP. |
| FMT\_MSA.3.2 | The TSF shall allow the **[*None*]** to specify alternative initial values to override the default values when an object or information is created. |

#### FMT\_SMR Security Management Roles

|  |  |
| --- | --- |
| **FMT\_SMR.1 (c) Security roles / Local Network Services** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FMT\_SMR.1.1 | The TSF shall maintain the roles **[Application user.]** |
| FMT\_SMR.1.2 | The TSF shall be able to associate users with roles. |

|  |  |
| --- | --- |
| **FMT\_SMR.1 (e) Security roles / User Authentication and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FMT\_SMR.1.1 | The TSF shall maintain the roles **[End-user].** |
| FMT\_SMR.1.2 | The TSF shall be able to associate users with roles. |

|  |  |
| --- | --- |
| **FMT\_SMR.1 (b) Security roles / Profile File Updates** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FMT\_SMR.1.1 | The TSF shall maintain the roles **[the authorised identified roles, third party services].** |
| FMT\_SMR.1.2 | The TSF shall be able to associate users with roles. |

|  |  |
| --- | --- |
| **FMT\_SMR.1 (d) Security roles / Secure Communication** | |
| Hierarchical to: | No other components. |
| Dependencies: | FIA\_UID.1 Timing of identification |
| FMT\_SMR.1.1 | The TSF shall maintain the roles **[Smart TV trust manager].** |
| FMT\_SMR.1.2 | The TSF shall be able to associate users with roles. |

#### FMT\_SMF Specification of Management Functions

|  |  |
| --- | --- |
| **FMT\_SMF.1 (b-c)Specification of Management Functions – Local Network Ser./Profile File Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FMT\_SMF.1.1 | The TSF shall be capable of performing the following management functions: **[PIN-code configuration, third party services enable/disable operation].** |

|  |  |
| --- | --- |
| **FMT\_SMF.1 (e) Specification of Management Functions – User Authentication** **and Operations** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FMT\_SMF.1.1 | The TSF shall be capable of performing the following management functions: **[input white list configuration].** |

|  |  |
| --- | --- |
| **FMT\_SMF.1 (d) Specification of Management Functions – Secure Communication** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FMT\_SMF.1.1 | The TSF shall be capable of performing the following management functions: **[Establish of encrypted communication].** |

### Protection of the TSF (FPT)

#### FPT\_FLS Fail Secure

|  |  |
| --- | --- |
| **FPT\_FLS.1 (c) Failure with preservation of secure state – Local Network Services** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT\_FLS.1.1 | The TSF shall preserve a secure state when the following types of failures occur: **[power failures, network failures].** |
| NOTE 1 | Power failure means in case of a power outage, the power recovery Smart TV will be initialized without any security leakage. |
| NOTE 2 | Network failure means that Smart TV runs without any security leakage under network issues such as connection lost. |

#### FPT\_SCB TSF Initialisation

|  |  |
| --- | --- |
| **FPT\_SCB.1 (f) Secure Boot** | |
| Hierarchical to: | No other components. |
| Dependencies: | No other components. |
| FPT\_SCB.1.1 | The TSF shall provide secure initialization function that brings it into a secure operational state at **[power-on]** by verification of **[OS] [*integrity*] .** |
| FPT\_SCB.1.2 | The TSF initialization function is verified by **[public keys]** **[stored encrypted and verified before used]**. |
| FPT\_SCB.1.3 | The TSF shall provide **[the integrity of the storage root of trust, the version of the firmware to prevent downgrade to previous versions]**. |
| FPT\_SCB.1.4 | The TSF shall perform **[escrow]** in accordance with a specified cryptographic key access method **[internal secure storage read]** that meets the following: **[None].** |
| FPT\_SCB.1.5 | The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE either successfully completes initialization or is halted. |
| FPT\_SCB.1.6 | The TOE initialization function shall not be able to arbitrarily interact with the TSF after TOE initialization completes. |

### Resource Utilisation (FRU)

#### FRU\_FLT Fault Tolerance

|  |  |
| --- | --- |
| **FRU\_FLT.2 (c) Limited Fault Tolerance – Local Network Services** | |
| Hierarchical to: | FRU\_FLT.1 Degraded fault tolerance |
| Dependencies: | FPT\_FLS.1 Failure with preservation of secure state |
| FRU\_FLT.2.1 | The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **[power failures, network failures]**. |

### Trusted Path/Channels (FTP)

#### FTP\_TRP Trusted Path

|  |  |
| --- | --- |
| **FTP\_TRP.1 (a) Trusted path / OTA Firmware Update** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FTP\_TRP.1.1 | The TSF shall provide a communication path between itself and ***[remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[modification, disclosure].*** |
| FTP\_TRP.1.2 | The TSF shall permit ***[the TSF, remote users]*** to initiate communication via the trusted path. |
| FTP\_TRP.1.3 | The TSF shall require the use of the trusted path for ***[OTA firmware update image].*** |

|  |  |
| --- | --- |
| **FTP\_TRP.1 (d) Trusted path - Secure Communication** | |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FTP\_TRP.1.1 | The TSF shall provide a communication path between itself and ***[remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[modification, disclosure].*** |
| FTP\_TRP.1.2 | The TSF shall permit ***[the TSF, remote users]*** to initiate communication via the trusted path. |
| FTP\_TRP.1.3 | FTP\_TRP.1.3 The TSF shall require the use of the trusted path for ***[Secure Communication].*** |

## **Security Assurance Requirements**

|  |  |
| --- | --- |
| **Assurance Class** | **Assurance Components** |
| ADV: Development | ADV\_ARC.1 Security architecture description |
| ADV\_FSP.2 Security-enforcing functional specification |
| ADV\_TDS.1 Basic design |
| AGD: Guidance documents | AGD\_OPE.1 Operational user guidance |
| AGD\_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC\_CMC.2 Use of a CM system |
| ALC\_CMS.2 Parts of the TOE CM coverage |
| ALC\_DEL.1 Delivery procedures |
| ASE: Security Target evaluation | ASE\_CCL.1 Conformance claims |
| ASE\_ECD.1 Extended components definition |
| ASE\_INT.1 ST introduction |
| ASE\_OBJ.2 Security objectives |
| ASE\_REQ.2 Derived security requirements |
| ASE\_SPD.1 Security problem definition |
| ASE\_TSS.1 TOE summary specification |
| ATE: Tests | ATE\_COV.1 Evidence of coverage |
| ATE\_FUN.1 Functional testing |
| ATE\_IND.2 Independent testing - sample |
| AVA: Vulnerability Assessment | AVA\_VAN.2 Vulnerability analysis |

## **Security Requirements Rationale**

In the section, the security function requirements are represented according to the security function letter match given below.

* OTA Firmware Update is (a),
* Profile File Update is (b),
* Local Network Service is (c),
* Secure Communication is (d),
* User Authentication and Operations is (e) and
* Secure Boot Operation (f).

### SFR Dependency

|  |  |  |  |
| --- | --- | --- | --- |
| **NO** | **SFR** | **Dependency** | **Dependency Met?** |
| **1** | FCS\_CKM.3 (a.1) | FDP\_ITC.1  or  FDP\_ITC.2  or  FCS\_CKM.1  FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **2** | FCS\_CKM.3 (a-f.2) | FDP\_ITC.1  or  FDP\_ITC.2  or  FCS\_CKM.1  FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **3** | FCS\_CKM.3 (b.2) | FDP\_ITC.1  or  FDP\_ITC.2  or  FCS\_CKM.1  FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **4** | FCS\_COP.1 (a-f.1) | --FDP\_ITC.1  or  --FDP\_ITC.2  or  --FCS\_CKM.1  --FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **5** | FCS\_COP.1 (a.2) | --FDP\_ITC.1  or  --FDP\_ITC.2  or  --FCS\_CKM.1  --FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **6** | FCS\_COP.1 (a.3) | --FDP\_ITC.1  or  --FDP\_ITC.2  or  --FCS\_CKM.1  --FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **7** | FCS\_COP.1 (b.1) | --FDP\_ITC.1  or  --FDP\_ITC.2  or  --FCS\_CKM.1  --FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **8** | FCS\_COP.1 (b.2) | --FDP\_ITC.1  or  --FDP\_ITC.2  or  --FCS\_CKM.1  --FCS\_CKM.4 | --FDP\_ITC.2 (a-b)  N/A. There is no cryptographic key destruction since the key is kept securely during the life cycle of the device. |
| **9** | FDP\_ACC.1 (e) | --FDP\_ACF.1 | --FDP\_ACF.1 (e) |
| **10** | FDP\_ACC.1 (a-f) | --FDP\_ACF.1 | --FDP\_ACF.1 (a-f) |
| **11** | FDP\_ACF.1 (e) | --FDP\_ACC.1  --FMT\_MSA.3 | --FDP\_ACC.1 (e)  --FMT\_MSA.3 (e) |
| **12** | FDP\_ACF.1 (a-f) | --FDP\_ACC.1  --FMT\_MSA.3 | --FDP\_ACC.1 (a-f)  --FMT\_MSA.3 (a-c) |
| **13** | FDP\_ETC.2 (a) | --FDP\_ACC.1  --FDP\_IFC.1 | --FDP\_ACC.1 (a-f)  --FDP\_IFC.1 (a) |
| **14** | FDP\_IFC.1 (a) | --FDP\_IFF.1 | --FDP\_IFF.1 (a) |
| **15** | FDP\_IFC.1 (c) | --FDP\_IFF.1 | --FDP\_IFF.1 (c) |
| **16** | FDP\_IFC.1 (d) | --FDP\_IFF.1 | --FDP\_IFF.1 (d) |
| **17** | FDP\_IFF.1 (a) | --FDP\_IFC.1  --FMT\_MSA.3 | --FDP\_IFC.1 (a)  -- FMT\_MSA.3 (a-c) |
| **18** | FDP\_IFF.1 (c) | --FDP\_IFC.1  --FMT\_MSA.3 | --FDP\_IFC.1 (c)  --FMT\_MSA.3 (c) |
| **19** | --FDP\_IFF.1 (d) | --FDP\_IFC.1  --FMT\_MSA.3 | --FDP\_IFC.1 (d)  --FMT\_MSA.3 (d) |
| **20** | FDP\_ITC.2 (a-b) | --FDP\_ACC.1  or  --FDP\_IFC.1  --FTP\_ITC.1  or  --FTP\_TRP.1  --FPT\_TDC.1 | --FDP\_ACC.1 (a-f)  --FDP\_IFC.1 (a)  --FTP\_TRP.1 (a)  N/A. There is no data sharing between TOE and another trusted IT product. |
| **21** | FDP\_ROL.1 | --FDP\_ACC.1  or  --FDP\_IFC.1 | N/A. There is no information flow to be controlled or any user role involved with the rollback operation. |
| **22** | FDP\_UCT.1 (a) | --FTP\_ITC.1  or  --FTP\_TRP.1  --FDP\_ACC.1  or  --FDP\_IFC.1 | --FTP\_TRP.1 (a)  --FDP\_ACC.1 (a-f)    --FDP\_IFC.1 (a) |
| **23** | FDP\_UCT.1 (d) | --FTP\_ITC.1  or  --FTP\_TRP.1  --FDP\_ACC.1  or  --FDP\_IFC.1 | --FTP\_TRP.1 (d)  --FDP\_IFC.1 (d) |
| **24** | FDP\_UIT.1 (a) | FDP\_ACC.1  or  FDP\_IFC.1  FTP\_ITC.1  or  FTP\_TRP.1 | --FDP\_ACC.1 (a-f)  --FDP\_IFC.1 (a)  --FTP\_TRP.1 (a) |
| **25** | FIA\_AFL.1 (e) | --FIA\_UAU.1 | --FIA\_UAU.1 (e) |
| **26** | FIA\_ATD.1 (e) | N/A | N/A |
| **27** | FIA\_UAU.1 (e) | --FIA\_UID.1 | --FIA\_UID.1 (e) |
| **28** | FIA\_UID.1 (e) | N/A | N/A |
| **29** | FIA\_UID.1 (c) | N/A | N/A |
| **30** | FIA\_UID.1 (b) | N/A | N/A |
| **31** | FMT\_MOF.1 (b) | --FMT\_SMR.1  --FMT\_SMF.1 | --FMT\_SMR.1 (c)  --FMT\_SMF.1 (b-c) |
| **32** | FMT\_MSA.1 (e) | --FDP\_ACC.1  or  --FDP\_IFC.1  --FMT\_SMR.1  --FMT\_SMF.1 | --FDP\_ACC.1 (e)  --FMT\_SMR.1 (e)  --FMT\_SMF.1 (e) |
| **33** | FMT\_MSA.1 (d) | --FDP\_ACC.1  or  --FDP\_IFC.1  --FMT\_SMR.1  --FMT\_SMF.1 | --FDP\_IFC.1 (d)  --FMT\_SMR.1 (d)  --FMT\_SMF.1 (d) |
| **34** | FMT\_MSA.3 (a-c) | --FMT\_MSA.1  --FMT\_SMR.1 | N/A. There is no management of security attributes.  --FMT\_SMR.1 (c) |
| **35** | FMT\_MSA.3 (e) | --FMT\_MSA.1  --FMT\_SMR.1 | --FMT\_MSA.1 (e)  --FMT\_SMR.1 (e) |
| **36** | --FMT\_MSA.3 (d) | --FMT\_MSA.1  --FMT\_SMR.1 | --FMT\_MSA.1 (d)  --FMT\_SMR.1 (d) |
| **37** | FMT\_SMR.1 (c) | --FIA\_UID.1 | --FIA\_UID.1 (c) |
| **38** | FMT\_SMR.1 (e) | --FIA\_UID.1 | --FIA\_UID.1 (e) |
| **39** | FMT\_SMR.1 (b) | --FIA\_UID.1 | --FIA\_UID.1 (b) |
| **40** | FMT\_SMR.1 (d) | --FIA\_UID.1 | N/A. There is no communication before secure communication is established. |
| **41** | FMT\_SMF.1 (b-c) | N/A | N/A |
| **42** | FMT\_SMF.1 (e) | N/A | N/A |
| **43** | FMT\_SMF.1 (d) | N/A | N/A |
| **44** | FPT\_FLS.1 (c) | N/A | N/A |
| **45** | FPT\_SCB.1 (f) | N/A | N/A |
| **46** | FRU\_FLT.2 (c) | --FPT\_FLS.1 | --FPT\_FLS.1 (c) |
| **47** | FTP\_TRP.1 (a) | N/A | N/A |
| **48** | FTP\_TRP.1 (d) | N/A | N/A |

### SFR - Objective Rationale

Rationale of security functional requirements demonstrates in the following table. Each TOE security objective has at least one security functional requirement corresponding to it. Each TOE security functional requirement corresponds back to at least one TOE security objectives.

Table 7 Security Functional Requirements’ Mapping

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Security Objectives** | | | | | | | | |
| O.SWUptImgVerification | O.SWUptImgProtection | O.PrflUptFileVerification | O.ScrCommunication | O.InptVerification | O.UserAuth | O.DataDeletion | O.Outages | O.ScrBoot |
| **Security Functional Requirements** | FCS\_CKM.3 (a.1) |  | √ |  |  |  |  |  |  |  |
| FCS\_CKM.3 (a-f.2) | √ |  |  |  |  |  |  |  | √ |
| FCS\_CKM.3 (b.2) |  |  | √ |  |  |  |  |  |  |
| FCS\_COP.1 (a-f.1) | √ |  |  |  |  |  |  |  | √ |
| FCS\_COP.1 (a.2) |  | √ |  |  |  |  |  |  |  |
| FCS\_COP.1 (a.3) | √ |  |  |  |  |  |  |  |  |
| FCS\_COP.1 (b.1) |  |  | √ |  |  |  |  |  |  |
| FCS\_COP.1 (b.2) |  |  | √ |  |  |  |  |  |  |
| FDP\_ACC.1 (e) |  |  |  |  |  | √ |  |  |  |
| FDP\_ACC.1 (a-f) | √ |  |  |  |  |  |  |  | √ |
| FDP\_ACF.1 (a-f) | √ |  |  |  |  |  |  |  | √ |
| FDP\_ACF.1 (e) |  |  |  |  |  | √ |  |  |  |
| FDP\_ETC.2 (a) |  | √ |  |  |  |  |  |  |  |
| FDP\_IFC.1 (c) |  |  |  |  | √ |  |  |  |  |
| FDP\_IFC.1 (a) |  | √ |  |  |  |  |  |  |  |
| FDP\_IFC.1 (d) |  |  |  | √ |  |  |  |  |  |
| FDP\_IFF.1 (a) |  | √ |  |  |  |  |  |  |  |
| FDP\_IFF.1 (c) |  |  |  |  | √ |  |  |  |  |
| FDP\_IFF.1 (d) |  |  |  | √ |  |  |  |  |  |
| FDP\_ITC.2 (a-b) |  | √ | √ |  |  |  |  |  |  |
| FDP\_ROL.1 |  |  |  |  |  |  | √ |  |  |
| FDP\_UCT.1 (a) |  | √ |  |  |  |  |  |  |  |
| FDP\_UCT.1 (d) |  |  |  | √ |  |  |  |  |  |
| FDP\_UIT.1 (a) | √ |  |  |  |  |  |  |  |  |
| FIA\_AFL.1 (e) |  |  |  |  |  | √ |  |  |  |
| FIA\_ATD.1 (e) |  |  |  |  |  | √ |  |  |  |
| FIA\_UAU.1 (e) |  |  |  |  |  | √ |  |  |  |
| FIA\_UID.1 (e) |  |  |  |  |  | √ |  |  |  |
| FIA\_UID.1 (c) |  |  |  |  | √ |  |  |  |  |
| FIA\_UID.1 (b) |  |  | √ |  |  |  |  |  |  |
| FMT\_MOF.1 (b) |  |  | √ |  |  |  |  |  |  |
| FMT\_MSA.1 (e) |  |  |  |  |  | √ |  |  |  |
| FMT\_MSA.1 (d) |  |  |  | √ |  |  |  |  |  |
| FMT\_MSA.3 (a-c) | √ |  |  |  | √ |  |  |  |  |
| FMT\_MSA.3 (e) |  |  |  |  |  | √ |  |  |  |
| FMT\_MSA.3 (d) |  |  |  | √ |  |  |  |  |  |
| FMT\_SMR.1 (c) |  |  |  |  | √ |  |  |  |  |
| FMT\_SMR.1 (e) |  |  |  |  |  | √ |  |  |  |
| FMT\_SMR.1 (b) |  |  | √ |  |  |  |  |  |  |
| FMT\_SMR.1 (d) |  |  |  | √ |  |  |  |  |  |
| FMT\_SMF.1 (b-c) |  | √ | √ |  | √ |  |  |  |  |
| FMT\_SMF.1 (e) |  |  |  |  |  | √ |  |  |  |
| FMT\_SMF.1 (d) |  |  |  | √ |  |  |  |  |  |
| FPT\_FLS.2 (c) |  |  |  |  |  |  |  | √ |  |
| FPT\_SCB.1 (f) |  |  |  |  |  |  |  |  | √ |
| FRU\_FLT.2 (c) |  |  |  |  |  |  |  | √ |  |
| FTP\_TRP.1 (a) |  | √ |  |  |  |  |  |  |  |
| FTP\_TRP.1 (d) |  |  |  | √ |  |  |  |  |  |

Table 8 Security Functional Requirements / Security Objectives Rationale

|  |  |  |
| --- | --- | --- |
| **Security Objective** | **Mapped SFRs** | **Rationale** |
| O.SWUptImgVerification | FCS\_CKM.3 (a-f.2) | The requirement helps meet the objective by performing signature verification of OTA firmware update image. |
| FCS\_COP.1 (a-f.1) | The requirement helps meet the objective by generating and verifying the signature for OTA firmware update image in accordance with RSA. |
| FCS\_COP.1 (a.3) | The requirement helps meet the objective by generating Hash value of OTA firmware update image in accordance with SHA-2. |
| FDP\_UIT.1 (a) | The requirement addresses the objective by modification and insertion of the user data transmitted. |
| FMT\_MSA.3 (a-c) | The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP. |
| FDP\_ACC.1 (a-f) | The requirement helps meet the objective by identifying the objects and users subjected to the access control policy. |
| FDP\_ACF.1 (a-f) | The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy. |
| O.SWUptImgProtection | FCS\_CKM.3 (a.1) | The requirement helps meet the objective by performing decryption process of OTA firmware update image. |
| FCS\_COP.1 (a.2) | The requirement helps meet the objective by performing encryption and decryption of OTA firmware update image in accordance with AES. |
| FDP\_ETC.2 (a) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP in order to export user data outside of the TOE. |
| FDP\_IFC.1 (a) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP during OTA firmware update. |
| FDP\_IFF.1 (a) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP during OTA firmware update. |
| FDP\_ITC.2 (a-b) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP in order to import user data outside of the TOE. |
| FDP\_UCT.1 (a) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP in order to transmit user data in a manner protected from unauthorized disclosure. |
| FMT\_SMF.1 (b-c) | The requirement helps meet the objective by specifying the management functions of the TOE. |
| FTP\_TRP.1 (a) | The requirement helps meet the objective by protecting the traffic transmitted from disclosure and modification. |
| O.PrflUptFileVerification | FCS\_COP.1 (b.1) | The requirement helps meet the objective by generating and verifying the signature for Profile file update image in accordance with RSA. |
| FCS\_COP.1 (b.2) | The requirement helps meet the objective by generating Hash value of Profile file update image in accordance with SHA-2. |
| FCS\_CKM.3 (b.2) | The requirement helps meet the objective by performing signature verification of profile update file |
| FDP\_ITC.2 (a-b) | The requirement helps meet the objective by enforcing VESTEL Cloud Flow Control SFP in order to import user data outside of the TOE. |
| FIA\_UID.1 (b) | The requirement helps meet the objective by allowing the General settings modification of Smart TVbefore the user is identified. It also helps meet the objective by identifying the users before any TSF mediated actions. |
| FMT\_MOF.1 (b) | The requirement helps meet the objective by allowing the authorised users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable. |
| FMT\_SMF.1 (b-c) | The requirement helps meet the objective by specifying the management functions of the TOE. |
| FMT\_SMR.1 (b) | The requirement helps meet the objective by maintaining the authorised identified roles and third party services. |
| O.ScrCommunication | FTP\_TRP.1 (d) | The requirement helps meet the objective by protecting the traffic transmitted from disclosure and modification. |
| FDP\_IFC.1 (d) | The requirement helps meet the objective by enforcing VESTEL Cloud flow control SFP during sending and receiving encrypted messages. |
| FDP\_IFF.1 (d) | The requirement helps meet the objective by verifying inputs by checking the confidentiality of messages send and receive by cloud and Smart TV. |
| FDP\_UCT.1 (d) | The requirement helps meet the objective by enforcing VESTEL Portal Cloud Flow Control SFP in order to transmit and receive user data in a manner protected from unauthorized disclosure. |
| FMT\_MSA.3 (d) | The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP. |
| FMT\_MSA.1 (d) | The requirement helps meet the objective by allowing the authorized users (roles) to manage the specified security attributes. |
| FMT\_SMR.1 (d) | The requirement helps meet the objective by maintaining and managing Smart TV trust manager role. |
| FMT\_SMF.1 (d) | The requirement helps meet the objective by specifying the management functions of the TOE. |
| O.InptVerification | FDP\_IFF.1 (c) | The requirement helps meet the objective by verifying inputs with checking of white listing before the input is processed. |
| FIA\_UID.1 (c) | The requirement helps meet the objective by allowing the usage of Smart TV via mobile application before the user is identified. It also helps meet the objective by identifying the users before any TSF mediated actions. |
| FMT\_MSA.3 (a-c) | The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP. |
| FMT\_SMR.1 (c) | The requirement helps meet the objective by maintaining End-user role and manages multiple user roles. |
| FMT\_SMF.1 (b-c) | The requirement helps meet the objective by specifying the management functions of the TOE. |
| FDP\_IFC.1 (c) | The requirement helps meet the objective by enforcing Smart TV Flow Control SFP during sending and receiving Network Local Services and Network Ports. |
| O.UserAuth | FDP\_ACC.1 (e) | The requirement helps meet the objective by identifying the objects and users subjected to the access control policy. |
| FDP\_ACF.1 (e) | The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy. |
| FIA\_AFL.1 (e) | The requirement helps meet the objective by handling of authentication failure during PIN-code verification. |
| FIA\_ATD.1 (e) | The requirement helps meet the objective by maintaining a security attribute (PIN-code) that belongs to individual users. |
| FIA\_UAU.1 (e) | The requirement helps meet the objective by allowing the general usage of Smart TV before the user is authenticated. It also helps meet the objective by authenticating the users before any TSF mediated actions. |
| FIA\_UID.1 (e) | The requirement helps meet the objective by allowing the general usage of Smart TV before the user is identified. It also helps meet the objective by identifying the users before any TSF mediated actions. |
| FMT\_MSA.1 (e) | The requirement helps meet the objective by allowing the authorized users (roles) to manage the specified security attributes. |
| FMT\_MSA.3 (e) | The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP. |
| FMT\_SMR.1 (e) | The requirement helps meet the objective by maintaining End-user role and manages multiple user roles. |
| FMT\_SMF.1 (e) | The requirement helps meet the objective by specifying the management functions of the TOE. |
| O.DataDeletion | - | - |
| FDP\_ROL.1 | The requirement helps meet the objective by providing user specific data deletion option by factory reset mechanism. |
| O.Outages | FPT\_FLS.1 (c) | The requirement helps meet the objective by preserving a secure state in the face of the identified failures. |
| FRU\_FLT.2 (c) | The requirement helps meet the objective by ensuring the operation of all the TOE's capabilities in case of identified failures occur. |
| O.ScrBoot | FPT\_SCB.1 (f) | The requirement helps meet the objective by providing Secure OS initialization function. |
| FCS\_CKM.3 (a-f.2) | The requirement helps meet the objective by performing signature verification of boot image. |
| FCS\_COP.1 (a-f.1) | The requirement helps meet the objective by generating and verifying the signature for boot image in accordance with RSA. |
| FDP\_ACC.1 (a-f) | The requirement helps meet the objective by identifying the objects and users subjected to the access control policy. |
| FDP\_ACF.1 (a-f) | The requirement meets the objective by ensuring the TOE only allows access to objects based on the defined access control policy. |

### SAR Rationale

The chosen assurance level is appropriate with the threats defined for the environment. The threats that were chosen are consistent with attacker of low attack motivation, therefore EAL2 was chosen for this ST.

# **TOE SUMMARY SPECIFICATION**

This section summarizes security functions provided by TOE in term of how they fulfill the related SFR’s. The TOE security functions divided into “OTA Firmware Update”, “Profile File Update”, “Local Network Services”, “Secure Communication”, “User Authentication and Operations” and “Secure Boot Operation”.

## **OTA Firmware Update**

Smart TVs connect to update server for checking of the update image uploaded periodically. If there is a new signed and encrypted update image uploaded on the server, TOE download that image over secure communication protected by using of minimum secure version of TLS (TLS 1.2). After downloading encrypted software update image, TOE ensures the integrity of the image by verification of digital signature, and then decrypt the image. After completed of these processes, authorized software update image is installed on smart TVs.

Functional Requirement Satisfied: FCS\_CKM.3 (a.1), FCS\_CKM.3 (a-f.2), FCS\_COP.1 (a-f.1), FCS\_COP.1 (a.2), FCS\_COP.1 (a.3), FDP\_ACC.1 (a-f), FDP\_ACF.1 (a-f), FDP\_ETC.2 (a), FDP\_IFC.1 (a), FDP\_IFF.1 (a), FDP\_ITC.2(a-b), FDP\_UCT.1 (a), FDP\_UIT.1 (a), FMT\_MSA.3 (a-c) and FTP\_TRP.1 (a)

## **Profile File Update**

Smart TV has service settings that allows changing physical and software features such as debug port enable/disable and connectivity features. A USB memory that includes signed profile file is plugged on smart TVs, TOE download the signed profile file over USB by trigger of USB operation option on smart TV settings. After downloading profile update file, TOE checks the integrity of the file by verification of digital signature. After completed of these processes, authorized profile update image is installed on smart TVs.

Functional Requirement Satisfied: FCS\_COP.1 (b.1), FCS\_COP.1 (b.2), FCS\_CKM.3 (b.2), FDP\_ITC.2 (a-b), FIA\_UID.1 (b), FMT\_MOF.1 (b), FMT\_SMR.1 (b) and FMT\_SMF.1 (b-c)

## **Local Network Services**

Local Network Services allow to pair Smart TV and mobile devices such as smartphone or tablet, connected to the same local network for enabling second-screen (Smart TV) applications to discover and launch first-screen (mobile devices) applications on first-screen. Herewith, the feature blocks unauthorized access, prevents a malicious input and injection attacks, provides availability for that the connection between Smart TV and third party applications (Netflix, YouTube etc.) or native Smart TV control purposed mobile application (Smart Center) is established to share screen between devices, control Smart TV on mobile application instead of remote controller. In addition, the TOE is protected against security leakages in case of any outages such as, power cut or network issues.

Functional Requirement Satisfied: FDP\_IFC.1 (c), FDP\_IFF.1 (c), FMT\_MSA.3 (a-c), FMT\_SMF.1 (b-c), FMT\_SMR.1 (c), FRU\_FLT.2 (c) and FPT\_FLS.1 (c)

## **Secure Communication**

Smart TVs provide an application portal such as application store, that user can select an application to open. Unlike the Android or iOS, there is no installation of application here. When user selects application icon, Smart TV connects to VESTEL Portal Server to get application URL and open it on browser. Herewith the connection between Smart TVs and VESTEL Portal Server is secured by minimum secure version of TLS (TLS 1.2) against the attacks for modification URLs or direct user to malicious webpages.

Functional Requirement Satisfied: FDP\_IFC.1 (d), FDP\_IFF.1 (d), FDP\_UCT.1 (d),FMT\_MSA.3 (d), FMT\_MSA.1 (d), FMT\_SMR.1 (d), FMT\_SMF.1 (d) and FTP\_TRP.1 (d)

## **User Authentication and Operations**

TOE provides a user authentication and verification mechanisms based on a PIN-code determined by users during the first time installation of Smart TV. Before making of modification on Settings, Wi-Fi Settings, Connected Services etc. user should authenticate to the Smart TV for prevention of unauthenticated user. Also, the feature prevents brute-force attacks by blocking the attempts for 30 minutes after 5 failure attempts. Moreover, the TOE provides user specific data deletion option including PIN-code by factory reset mechanism.

Functional Requirement Satisfied: FDP\_ACC.1 (e), FDP\_ACF.1 (e), FDP\_ROL.1, FIA\_AFL.1 (e), FIA\_ATD.1 (e), FIA\_UAU.1 (e), FIA\_UID.1 (e), FMT\_MSA.1 (e), FMT\_MSA.3 (e), FMT\_SMR.1 (e) and FMT\_SMF.1 (e)

## **Secure Boot Operation**

TOE provides security measure against risks about that the device OS has been modified in an unauthorized way. To provide this, the integrity of boot loader, OS kernel, file systems, etc. is verified by using of digital signature verification method during system launches.

Functional Requirement Satisfied: FPT\_SCB.1(f), FCS\_CKM.3(a-f.2), FDP\_ACC.1(a-f), FDP\_ACF.1(a-f), FCS\_COP.1(a-f.3)