Certification Report

EAL2 Evaluation of

VESTEL A.Ş.

VESTEL SMART TV COMMON FIRMWARE V1.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-89

TABLE OF CONTENTS

BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI
CCCS CERTIFICATION REPORT

Document Information

Date of Issue	**10/10/2023**
Approval Date	**13/10/2023**
Certification Report Number	**21.0.03/23-006**
Sponsor and Developer	**VESTEL A.Ş.**
Evaluation Facility	**TÜBİTAK BİLGEM OKTEM**
TOE/ PP Name*	**VESTEL Smart TV Common Firmware v1.0**
Pages	**23**

Prepared by ***Common Criteria Inspection Expert***	**Merve Hatice KARATAŞ**
Common Criteria Inspection Expert	**Göktuğ İLISU**
Common Criteria Candidate Inspection Expert	**Almıla Beyza KARAKAPICI**
Reviewer (Approver)	**Mehmet Kürşad ÜNAL**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	**04/10/2023**	**All**	**First Release**

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for VESTEL Smart TV Common Firmware v1.0 whose evaluation was completed on August 14th 2023 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.6 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including *EAL2*. The current list of signatory nations and approved certification schemes can be found on:
http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

Developer of the IT product: Vestel A.Ş.

Evaluated IT product: Vestel Smart TV Common Firmware

IT Product Version: 1.0

Name of IT Security Evaluation Facility: TÜBİTAK BİLGEM OKTEM

Completion date of evaluation: 14/08/2023

Assurance Package: EAL 2

1.1. Brief Description

Vestel Smart TV Common Firmware v1.0 (hereinafter TOE) is an IoT device security solution which provides security functions to implement secure OTA 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 TOE provides secure OTA firmware update feature to the device Smart TV users. The user easily updates the device firmware by following the procedure demonstrated on the mobile application. During the OTA firmware update process, download and install phases are protected by several cryptographic processes.

Also, 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. Therefore, an attacker or unauthorized person cannot change physical and software features.

1.2. Major Basic Security and Functional Attributes

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. 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 3. 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 (mobiledevices) 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

1.3. Threats

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.

- **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.

1.4. Organizational Security Policies (OSPs)

- **P.UptStrategy:** The secure firmware update procedure is given in "Software Update Strategy V1.0" document.

1.5. Assumptions

- **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.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-89
TOE Name and Version	VESTEL Smart TV Common Firmware V1.0
Security Target Title	VESTEL Smart TV Common Firmware V1.0 Security Target
Security Target Version	1.6
Security Target Date	06/06/2023
Assurance Level	EAL 2
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, 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 Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor and Developer	Vestel A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy

- **P.UptStrategy:** The secure firmware update procedure is given in "Software Update Strategy V1.0" document.

2.3 Assumptions and Clarification of Scope

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.

2.4 Architectural Information

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

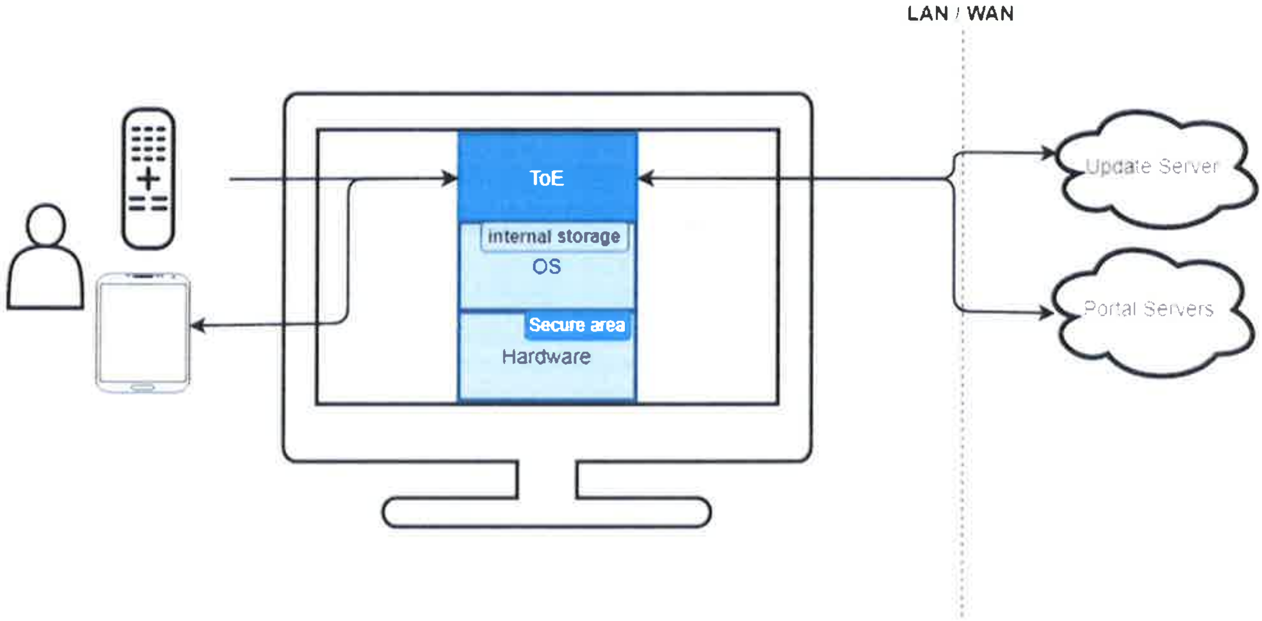

Figure 1 External Entities of the TOE Operational Environment

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 the secure version of TLS (TLS 1.2 or 1.3).

Smart TV contains two different secure storage areas. One of them is hardware secure area that stores the keys related to secure boot operation. When OS is launched, secure boot operation verifies that OS is the authorized OS, with the keys in the secure area. Other is the internal storage in file system of OS. This storage contains the keys that are used for integrity verification of SW update image and profile file update.

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 documents are provided to the user during the delivery. Documents:

- Smart TV User Guidance v11
- VESTEL SMART TV COMMON FIRMWARE V1.0 Operational User Guidance & Preparative Procedures v1.3

2.5 Documentation

Document Name	Version	Release Date
VESTEL SMART TV COMMON FIRMWARE V1.0 Security Target	V1.6	06/06/2023
VESTEL SMART TV USER GUİDANCE	v011	29/12/2021

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred compeletely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families and the evaluation evidences has been established. The evaluation results are available at the final Evaluation Technical Report (ETR) of Vestel Smart Tv Common Firmware v1.0 It is concluded that the TOE supports EAL 2. There exist 19 assurance families which are all evaluated with the methods detailed in the ETR.

- **Developer Testing:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE design documentation which includes TSF subsystems and its iteractions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 18 functional tests in total.

- **Evaluator Testing:** Evaluator has conducted 18 developer tests. Additionally, evaluator has prepared 11 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.

Test ID	Test	TSFI	SFR
BT_01	OTA Software Upgrade Operations Test	Update Server	FCS_CKM.3, FCS_COP.1 (a.1, f.1), FCS_COP.1 (a.2, f.3), FCS_COP.1 (a.3, b.1, f.2), FDP_ETC.2, FDP_IFC.1 (a, d, f), FDP_IFF.1 (a, f), FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FIA_UID.1 (a, b, f), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f), FTP_TRP.1
BT_02	Feature Alteration with Profile File Update Test	USB Stick, Remote Controller	FCS_CKM.3, FCS_COP.1 (a.3, b.1, f.2), FCS_COP.1 (b.2), FDP_ACC.1 (b), FDP_ACF.1 (b), FDP_ITC.2, FIA_UID.1 (a, b, f),

			FMT_MOF.1, FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f)
BT_03	Third Party App Usage Test	Mobile Application	FDP_IFC.1 (c), FDP_IFF.1 (c), FIA_UID.1 (c), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (c), FMT_SMF.1 (a, b, c, f)
BT_04	VESTEL Smart Center App Usage Test	Mobile Application	FDP_IFC.1 (c), FDP_IFF.1 (c), FIA_UID.1 (c), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (c), FMT_SMF.1 (a, b, c, f)
BT_05	Menu Lock Test	Remote Controller	FDP_ACC.1 (e), FDP_ACF.1 (e), FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UID.1 (e), FIA_SOS.1, FMT_MSA.1 (e), FMT_MSA.3, FMT_SMR.1 (e), FMT_SMF.1 (e)

BT_06	Different Server IP Test	Update Server, Portal Server	FDP_IFC.1 (a, d, f), FDP_IFF.1 (d), FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (d), FMT_SMF.1 (d), FTP_TRP.1
BT_07	Firmware Upgrade without Connection Test	Update Server	FCS_CKM.3, FCS_COP.1 (a.1, f.1), FCS_COP.1 (a.2, f.3), FCS_COP.1 (a.3, b.1, f.2), FDP_ETC.2, FDP_IFC.1 (a, d, f), FDP_IFF.1 (a, f), FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FIA_UID.1 (a, b, f), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f), FTP_TRP.1
BT_08	Service Menu Test	Update Server, Remote Controller	FCS_CKM.3, FCS_COP.1 (a.1, f.1), FCS_COP.1 (a.2, f.3), FCS_COP.1 (a.3, b.1, f.2), FDP_ETC.2,

			FDP_IFC.1 (a, d, f), FDP_IFF.1 (a, f), FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FIA_UID.1 (a, b, f), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f), FTP_TRP.1
BT_09	USB Operations Test	Remote Controller, USB Stick	FCS_CKM.3, FCS_COP.1 (a.1, f.1), FCS_COP.1 (a.2, f.3), FCS_COP.1 (a.3, b.1, f.2), FDP_ETC.2, FDP_IFC.1 (a, d, f), FDP_IFF.1 (a, f), FDP_ITC.2, FDP_UCT.1, FDP_UIT.1, FIA_UID.1 (a, b, f), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f), FTP_TRP.1
BT_10	Application Input Validation Test	Mobile Application, Remote Controller	FDP_IFC.1 (c), FDP_IFF.1 (c), FIA_UID.1 (c),

			FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (c), FMT_SMF.1 (a, b, c, f)
BT_11	Factory Reset Interruption Test	Remote Controller	FCS_COP.1 (a.1, f.1), FCS_COP.1 (a.2, f.3), FCS_COP.1 (a.3, b.1, f.2), FDP_IFC.1 (a, d, f), FDP_IFF.1 (a, f), FDP_ITC.2, FDP_SDI.1, FIA_UID.1 (a, b, f), FMT_MSA.1 (a, d, b, c, f), FMT_MSA.3, FMT_SMR.1 (a, b, f), FMT_SMF.1 (a, b, c, f), FPT_SCB.1

Table 2: *Independent Tests*

- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 7 penetration tests have been conducted. TOE proved that it is resistant to "Attacker with Basic Attack Potential".

2.7 Evaluated Configuration

Evaluated TOE configuration is composed of:

- Vestel Smart TV Firmware v1.0

Also as consistent with the minimum Hardware/ Software/ OS requirements for the TOE, the test environment presented at the ETR is composed of software and hardware.

Hardware	Software
TP-Link WN722N USB WiFi Adapter	Kali Linux 2023.1
File v5.41	Wireshark v4.0.1
	Suricata IDS v6.0.8
	NMAP v7.93
	Smart Center v6.0230.19 Android Application
	Smart Center v7.0236.29 iOS Application
	Hping3 3.0.0-alpha 2

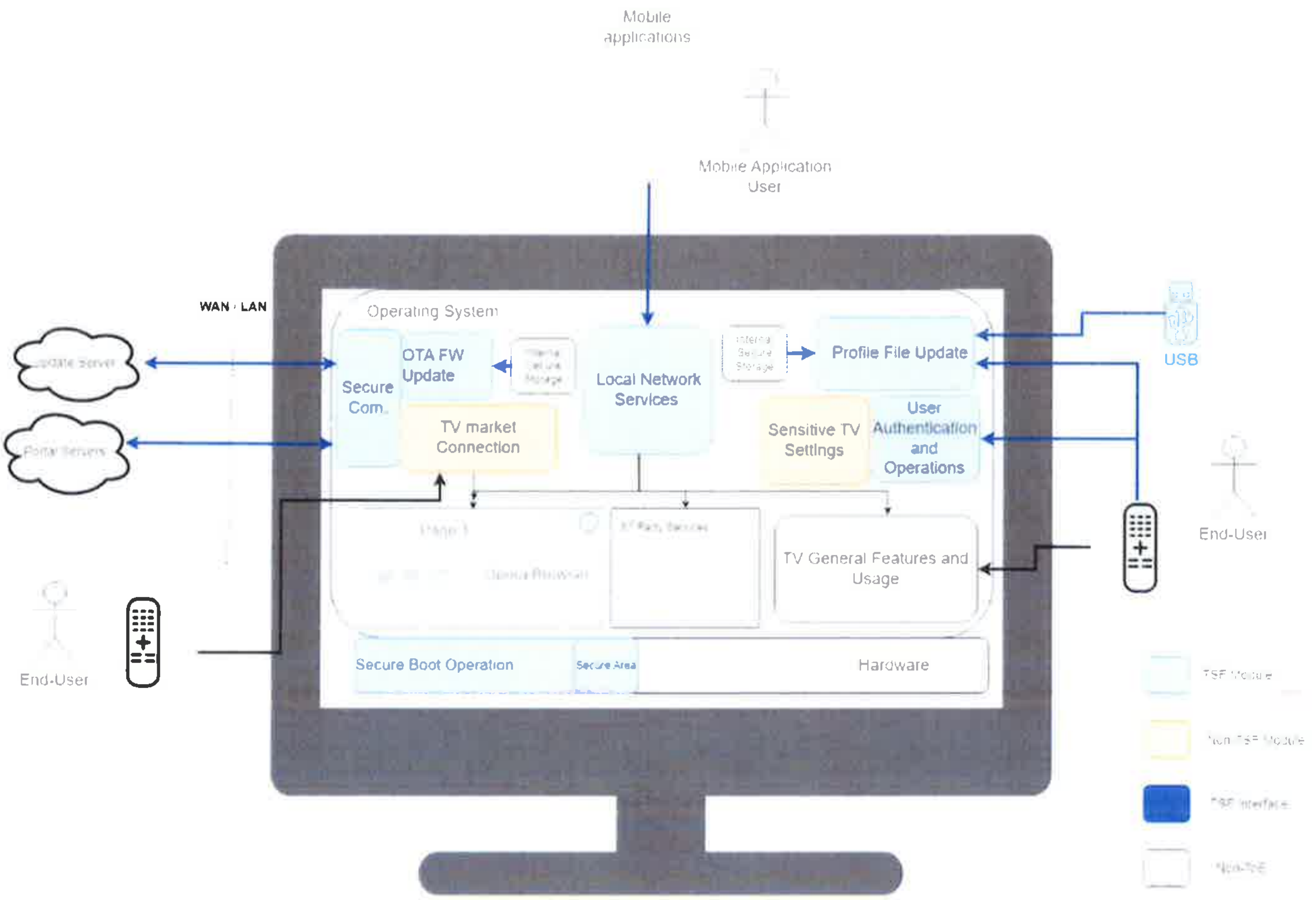

***Table 3:** Software and Hardware Requirements of Test Environment*

2.8 Results of the Evaluation

The table below provides a complete list of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 2 (EAL 2) components as specified in Part 3 of the Common Criteria.

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.2	Complete functional specification	PASS
	ADV_TDS.1	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS

Class Heading	Class Family	Description	Result
ALC: Lifecycle Support	ALC_CMC.2	Production support, acceptance procedures and automation	PASS
	ALC_CMS.2	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.1	Analysis of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.2	Focused vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:

Title: Vestel Smart Tv Firmware v1.0 Security Target

Version: v1.6

Date of Document: June 6, 2023

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

BİLGEM: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

CKM: Cryptographic Key Management

COP: Cryptographic Operation

EAL: Evaluation Assurance Level

FTP: Function of Trusted Path

IFC: Information Flow Control

IoT: Internet of Things

ITC: Inter TSF Confidentiality

MSA: Management of Security Attributes

OKTEM: Ortak Kriterler Test Merkezi

OSP: Organisational Security Policy

OTA: Over the Air

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

SHA: Secure Hash Algorithm

SMF: Specification of Management Functions

ST: Security Target

TLS: Transport Layer Security

TOE: Target of Evaluation

TDC: TSF Data Consistency

TSF: TOE Security Functionality

TSFI: TSF Interface

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

[3] DTR 90 TR 02 of Vestel Smart TV v1.0, Rel. Date: Agust 14, 2023

[4] Vestel Smart TV Firmware v1.0 Security Target, Version 1.6,
Rel. Date: June 6, 2023.

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: Vestel Smart Tv Firmware v1.0

TOE Hash (SHA256):

Modules	SHA-256
VESTEL Smart TV Common Firmware V1.0)	BA54FEF8B2566239A0D2BACCD418CDF86FA05B762921AFADDA790146237AEBF2

6.2 TEST ENVIRONMENT

	Test Software/ Hardware Name	Purpose of Use	Analysis
1	Kali Linux 2023.1	It is used to perform test.	It is used to perform test.
2	TP-Link WN722N USB WiFi Adapter	Wireless access provider adapter	Wireless access provider adapter
3	Wireshark v4.0.1	It is used to analyze and examine incoming packets	Packet analysis application
4	Suricata IDS v6.0.8	It is used to display connections made to the wireless port.	Attack detection application
5	NMAP v7.93	It is used to scan the network to find open TCP ports.	Network exploration and scanning application.

6	Smart Center v6.0230.19 Android Appliction	It will be used for communication and control with TOE.	Application based on Android platform
	Smart Center v6.0236.29 ios Application	It will be used for communication and control with TOE.	Application based on ios platform
7	Hping3 3.0.0-alpha 2	Network is used for TCP/IP packet sending.	Network TCP/IP packet sending tool