Certification Report

EAL2 Evaluation of

ARÇELİK A.Ş.

ARCELIK WI-FI IoT CONNECTIVITY SOLUTION v1.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-88

TABLE OF CONTENTS

Document Information

Date of Issue	**23/06/2023**
Approval Date	**23/06/2023**
Certification Report Number	**21.0.03/23-005**
Sponsor and Developer	**Arçelik A.Ş.**
Evaluation Facility	**TÜBİTAK BİLGEM OKTEM**
TOE/ PP Name*	**Arcelik Wi-Fi IoT Connectivity Solution v1.0**
Pages	**21**

Prepared by *Common Criteria Inspection Expert*	**Merve Hatice KARATAŞ**
Common Criteria Inspection Expert	**Göktuğ İLISU**
Common Criteria Candidate Inspection Expert	**Barış UÇAR**
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	**23/06/2023**	**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 Arcelik Wi-Fi IoT Connectivity Solution v1.0 whose evaluation was completed on March 24th 2023 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 0.15 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: Arçelik A.Ş.

Evaluated IT product: Arcelik Wi-Fi IoT Connectivity Solution

IT Product Version: 1.0

Name of IT Security Evaluation Facility: TÜBİTAK BİLGEM OKTEM

Completion date of evaluation: 24/03/2023

Assurance Package: EAL 2

1.1. Brief Description

Arcelik Wi-Fi IoT Connectivity Solution v1.0 (hereinafter TOE) is an IoT device security solution which provides security functions to implement secure OTA firmware download of Arcelik Wi-Fi IoT Devices (hereinafter IoT Device and/or Arcelik IoT Device) connectivity and control boards and secure OTA installation of connectivity board together with secure log storage of Arcelik IoT Devices.

The TOE provides secure OTA firmware update feature to the device 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, the device periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the device and so on. The Secure Log Storage feature provides the log data to be stored securely inside and outside (to Arcelik Cloud Server) of the product.

TOE is an Arcelik IoT Devices Security Solution that provides security functions in the form of library by being embedded on Arcelik IoT Devices electronic board.

1.2. Major Basic Security and Functional Attributes

- ✓ **Secure OTA Firmware Download:** This function blocks the installation of unauthorized firmware by using digital signature verification. The digital signature process for the firmware takes place in the Arcelik Cloud server and this enables only the firmware that are downloaded from the Arcelik Cloud server to be installable on the IoT device.
- ✓ **Secure OTA Firmware Installation:** The new OTA images downloaded on the Arcelik IoT device is stored in the external flash of connectivity board. If the OTA image is for connectivity board TOE verifies and the installation process starts. If the OTA image is for control board, firmware image is

transferred from connectivity board to control board via UART or SPI (Refrigerators have SPI, other IoT devices have UART) line chunk by chunk. The control board is responsible for validating integrity of the image. After OTA image is validated by control board it is installed and replaces the existing firmware.

- ✓ **Secure Log Storage:** The Arcelik IoT Devices periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the appliance and so on. The Secure Log Storage function provides the log data to be stored and transmitted securely inside and outside (to Arcelik Cloud Server) of the product. The logged data is generated by different control boards of the IoT device. Generated log data is imported from control board to TOE. The log data is stored in TOEs external flash until sent to Cloud Server. The Secure Log Storage Function uses UART or SPI (Refrigerators have SPI, other IoT devices have UART) connection between control board and connectivity board. TOE has two different firmware in which one of them for appliances have UART connection and the one for appliances have SPI connection.

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.UnverifiedOtaDownload:** Attacker could gain unauthorized access to the TOE data by bypassing the verification requirements and download OTA package to the TOE.
- **T.ModifyingOtaImage:** Attacker may install a malicious OTA image by intercepting OTA image installation process which is sent over the network and modifying the OTA image data.
- **T.StealModifyUsageLogData:** Attacker may steal or modify the usage log data as it is sent outside of the chip or to the Cloud Server.
- **T.UnauthorizedKeyAccess:** Attacker may try to access to the cryptographic keys which are used in authentication, encryption/decryption, and verification functions of TOE.
- **T.FirmwareCopyrightInfringement:** Attackers may copy the firmware contents like source codes and assets illegally and infringe product firmware copyrights.

1.4. Organizational Security Policies (OSPs)

- **P.FirmwareUpdateFileGenerationStorage:** For ensuring the secure firmware update procedure, the firmware update image file must be generated and stored securely. The firmware update image file which is digitally signed using ECDSA algorithm is downloaded by TOE over secure TLS tunnel, so that it is protected while being transferred via network. The signed firmware update image file is stored in Arcelik Cloud Server. All firmware update images shall be signed for the target appliance, it shall not be possible for an incorrectly signed image to execute, for example firmware signed for a different target appliance. When the OTA request come from end-user, the TOE step into the process and provide Secure Firmware OTA to the products.
- **P.CloudSecureKeyManagement:** The private key, which is used for authentication process of Arcelik Cloud Server and connected product, is generated by Arcelik based on the ECC standard, and stored securely on the Arcelik Cloud Server. The generation, storage, access control, and destruction of the cryptographic keys, which are managed from the Arcelik Cloud Server are performed securely in accordance with Arcelik regulations and policies.

1.5. Assumptions

- **A.SecureCloudServer:** For secure operation of TOE, The Arcelik Cloud Server which exists in the operating environment is operated securely.
- **A.ProductUniqueIDRegistration:** For secure management of each product, a unique identification is supported by Arcelik to each product while they are producing in the production lines.
- **A.ProductDisassemblyAuthorization:** The user of the Arcelik IoT Device has not got authorization for disassemble the product and access the TOE physically.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-88
TOE Name and Version	Arcelik Wi-Fi IoT Connectivity Solution v1.0
Security Target Title	Arcelik Wi-Fi IoT Connectivity Solution v1.0 Security Target
Security Target Version	0.15
Security Target Date	29/12/2022
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	Arçelik A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy

- **P.FirmwareUpdateFileGenerationStorage:** For ensuring the secure firmware update procedure, the firmware update image file must be generated and stored securely. The firmware update image file which is digitally signed using ECDSA algorithm is downloaded by TOE over secure TLS tunnel, so that it is protected while being transferred via network. The signed firmware update image file is stored in Arcelik Cloud Server. All firmware update images shall be signed for the target appliance, it shall not be possible for an incorrectly signed image to execute, for example firmware signed for a different target appliance. When the OTA request come from end-user, the TOE step into the process and provide Secure Firmware OTA to the products.
- **P.CloudSecureKeyManagement:** The private key, which is used for authentication process of Arcelik Cloud Server and connected product, is generated by Arcelik based on the ECC standard, and stored securely on the Arcelik Cloud Server. The generation, storage, access control, and destruction of the cryptographic keys, which are managed from the Arcelik Cloud Server are performed securely in accordance with Arcelik regulations and policies.

2.3 Assumptions and Clarification of Scope

- **A.SecureCloudServer:** For secure operation of TOE, The Arcelik Cloud Server which exists in the operating environment is operated securely.

- **A.ProductUniqueIDRegistration:** For secure management of each product, a unique identification is supported by Arcelik to each product while they are producing in the production lines.
- **A.ProductDisassemblyAuthorization:** The user of the Arcelik IoT Device has not got authorization for disassemble the product and access the TOE physically.

2.4 Architectural Information

The physical scope of TOE includes software elements that are used for securing the implementing securely usage log OTA firmware update and storage. The structure of the TOE can be found in Figure 1 below and identifies its components. Only authenticated and properly encrypted firmware images are downloaded and installed to the product electronic boards. The usage log data is always stored encrypted inside the product. Also, the usage log data sent from product to server is encrypted using a secure authenticated communication channel.

The TOE is a firmware element: connectivity board microcontroller firmware in binary format (*.bin). The firmware can be updated with a new version in any time whenever it is needed (to add a connectivity feature or solve a problem or vulnerability) in connectivity board by using secure OTA method. Arcelik TOE does not have a firmware configuration depends on the product configuration. Firmware solution is adaptable to any Arcelik product (dishwasher, air conditioner, washing machine, etc..). On the other hand, there are two types of communication methods are mainly used between TOE and CB (control board). These are UART (Universal Asynchronous Receiver Transmitter) and SPI (Serial Peripheral Interface). Firmware solution have two types depends on the communication methods between TOE and CB:

- Safir_batch_v3.10.23 (TOE [UART] – ESP32 FW)
- Safir_batch_v2.10.17 (TOE [SPI] – ESP32 FW)

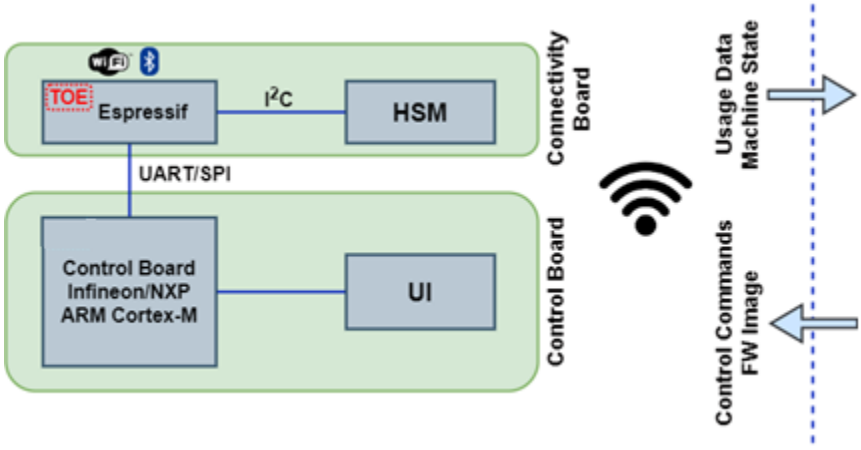

Figure 1: *Infrastructure of TOE*

The TOE operates in electronic board of IoT Device. The device user must use the Arcelik HomeWhiz mobile application for utilizing connectivity features of IoT device and activating the TOE. In addition to requiring services from the environment to achieve its main goal, the environment (Arcelik Cloud Server) also maintains a secure posture so that the application cannot be compromised by factors out of the TSF Scope of Control. Table 1 identifies the hardware required by TOE.

Category		Specifications
Connectivity Board	MPU	Dual-core Xtensa LX6 MCU with 448KB of RAM for booting, 520KB SRAM, and 4MB of external flash

Table 1: *Hardware Required by TOE*

The external entities of the TOE operational environment can be divided into three group: Arcelik Cloud Server, mobile device (mobile application) and the appliance user. Figure 2 shows the external entities of the TOE operational environment.

✓ **Arcelik Cloud Server**

Arcelik Cloud Server is implemented by Arcelik and running on AWS EC2 machines. It communicates with the mobile device and Arcelik IoT Device via secure MQTT. It carries out an application layer TLS handshake with both sides and transmits the messages as encrypted with that TLS session to make sure these messages are secured. Moreover, the usage data and machine state information are also encrypted with that TLS session and sent from the appliance to the cloud server.

✓ **Mobile Device**

HomeWhiz mobile application runs on the mobile device. This application reads the machine state data from the cloud and sends user control commands to the cloud as required. The command to start the firmware update process is also issued from this device. As mentioned before, the connection between the mobile device and Arcelik cloud server is encrypted.

✓ **Appliance User**

This refers to the user who uses an Arcelik IoT Device, connects it to the Arcelik Cloud Server using mobile application running on a mobile device. If necessary, upgrades the firmware of the appliance to take advantage of a variety of new features the appliance can provide. The users do not directly call the TOE but install new firmware to appliance and use mobile applications using IoT device functions.

✓ **Control Board**

Control board is the board that has a firmware run appliance with the required features in defined states and it is different from appliance to appliance. Control board communicates with the connectivity board via UART or SPI interface. Control board generates user data collected from the internal sensors of the appliance and sends them to the TOE periodically or at the end of each operation cycle.

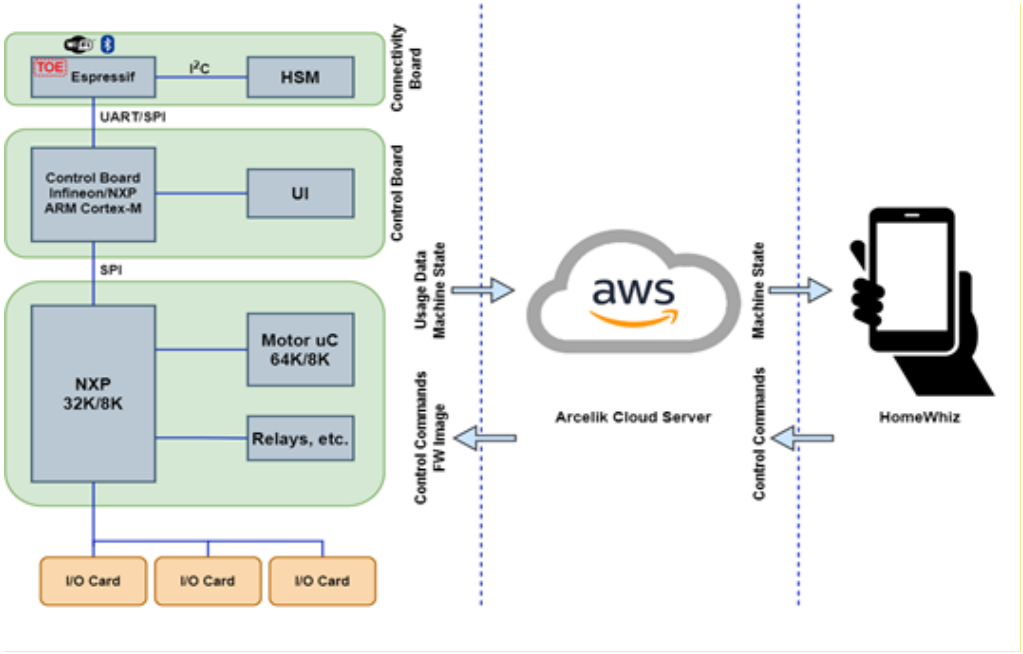

Figure 2: *External Entities of the TOE Operational Environment*

2.5 Documentation

Document Name	Version	Release Date
Arcelik Wi-Fi IoT Connectivity Solution v1.0 Security Target	v0.15	29/12/2022
Arcelik Wi-Fi IoT Connectivity Solution v1.0 Guidance and Preparative Procedures Document	v0.5	05/01/2023

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 Arcelik Wi-Fi IoT Connectivity

Solution 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 9 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 9 developer tests. Additionally, evaluator has prepared 4 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	SF	SFR
BT_01	OTA Download/ Install Interface Test	OTA Download, OTA Install	Secure OTA Firmware Download, Secure OTA Firmware Installation	FCS_CKM.3 FCS_CKM.4 FCS_COP.1 FDP_IFC.1 – HSM FDP_IFF.1 – HSM FDP_ITC.2 FMT_MSA.1 – HSM FMT_MSA.3 – HSM FMT_SMF.1 FPT_TDC.1 FPT_ITC.1 – HSM FPT_ITC.1 – CLOUD FTP_ITC.1 – HSM FTP_TRP.1 FPT_ITI.1
BT_02	Signup Test with Wrong Wi-Fi Password	OTA Install	Secure OTA Firmware Download, Secure OTA Firmware Installation	FCS_CKM.3 FCS_CKM.4 FCS_COP.1 FDP_IFC.1 – HSM

				FDP_IFF.1 – HSM FDP_ITC.2 FMT_MSA.1 – HSM FMT_MSA.3 – HSM FMT_SMF.1 FPT_TDC.1 FPT_ITC.1 – HSM FPT_ITC.1 – CLOUD FTP_ITC.1 – HSM FTP_TRP.1
BT_03	Power Failure Test During Update	OTA Install, Diagnostic Data	Secure OTA Firmware Download, Secure OTA Firmware Installation Secure Log Storage	FAU_STG.1 FCS_CKM.3 FCS_CKM.4 FCS_COP.1 FDP_ETC.2 FDP_IFC.1 – CLOUD FDP_IFC.1 – HSM FDP_IFC.1 – CB FDP_IFF.1 – CLOUD FDP_IFF.1 – CB FDP_ITC.1 FDP_ITC.2 FDP_UIT.1 FMT_MSA.1 – CLOUD FMT_MSA.1 – HSM FMT_MSA.1 – CB FMT_MSA.3 – CLOUD FMT_MSA.3 – HSM FMT_MSA.3 – CB FMT_SMF.1

				FPT_TDC.1 FPT_ITC.1 – HSM FTP_ITC.1 – HSM FTP_ITC.1 – CB FTP_TRP.1
BT_04	Control Test of Server Connection Addresses	OTA Download	Secure OTA Firmware Download, Secure OTA Firmware Installation	FCS_CKM.3 FCS_CKM.4 FCS_COP.1 FDP_IFC.1 – HSM FDP_IFF.1 – HSM FDP_ITC.2 FMT_MSA.1 – HSM FMT_MSA.3 – HSM FMT_SMF.1 FPT_TDC.1 FPT_ITC.1 – HSM FPT_ITC.1 – CLOUD FTP_ITC.1 – HSM FTP_TRP.1

Table 2: *Independent Tests*

- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 4 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:

- Arcelik Wi-Fi IoT Connectivity Solution 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
DUT: The Device Under Test (including the TOE)	Windows 10 64-bit
5V energy source to power the DUT	Firmware Test Package v0.1 (provided by Arcelik)
ESP-Prog USB-TTL adaptor to transfer device logs to the PC (Logging Device)	Tera Term v4.106
Custom cable to connect the Logging Device to TOE	esptool.exe v4.4
An Android mobile phone with HomeWhiz application installed	HomeWhiz v2.8.0.5 for Android
A Wi-Fi modem with active internet connection	
A desktop or laptop PC with at least 8GB RAM and 2GB free disk space	

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

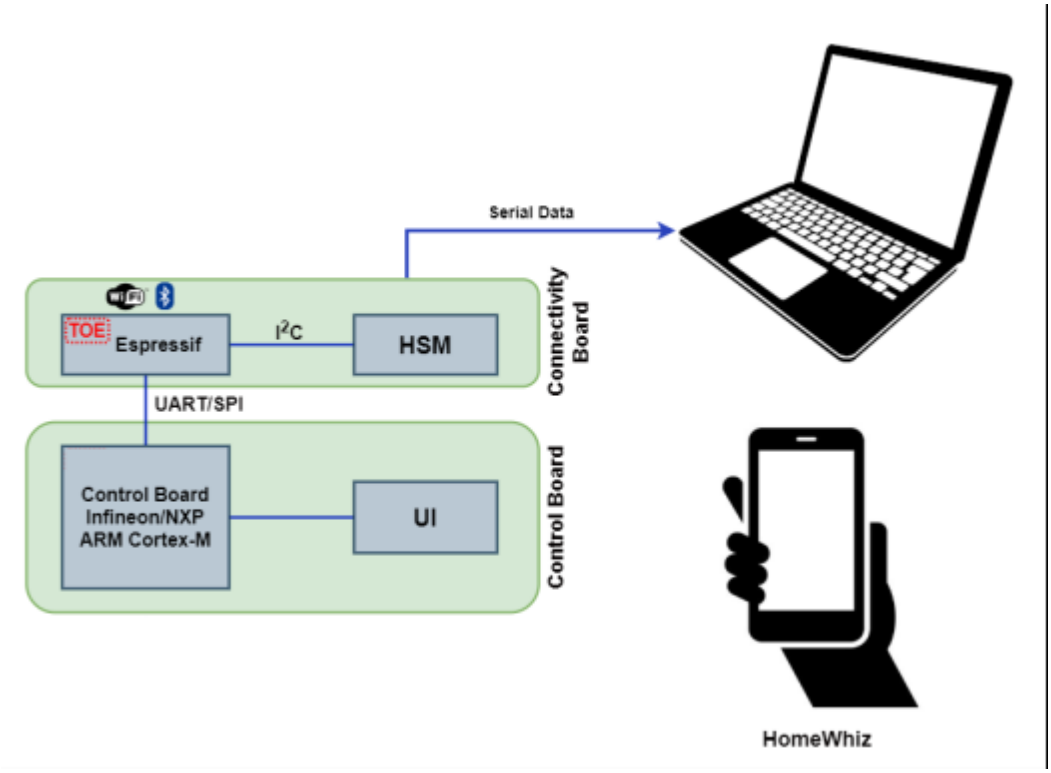

Figure 3: *TOE Test Topology*

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
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: Arcelik Wi-Fi IoT Connectivity Solution v1.0 Security Target

Version: v0.15

Date of Document: December 29, 2022

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

AWS EC2: Amazon Web Services Elastic Compute Cloud

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

ECDSA: Elliptic Curve Digital Signature Algorithm

FAU: Function of Audit

FTP: Function of Trusted Path

STG: Storage

HSM: Hardware Security Module

IFC: Information Flow Control

IoT: Internet of Things

ITC: Inter TSF Confidentiality

ITCD: Information Technologies Test and Certification Department

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

UART: Universal Asynchronous Receiver Transmitter

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 87 TR 01 of Arcelik W-Fi IoT Connectivity Solution v1.0, Rel. Date: March 24, 2023

[4] Arcelik W-Fi IoT Connectivity Solution v1.0 Security Target, Version 0.15, Rel. Date: December 29, 2022.

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: Arcelik W-Fi IoT Connectivity Solution v1.0

TOE Hash (SHA256):

Modules	**SHA-256**
Safir_batch_v3.10.23 (TOE [UART] – ESP32 FW)	F8807AE09DD3BDB873CC90F125513C6FC54F03EEA10623DCE89480D64B4158C3
Safir_batch_v2.10.17 (TOE [SPI] – ESP32 FW)	AD443B681CC8C181B4CBFFE02D4398AE001A70A4EF47001AC1974716FDF57AEA

6.2 TEST ENVIRONMENT

	Test Software/ Hardware Name	**Purpose of Use**	**Analysis**
1	esptool.exe v4.4	Software installation to TOE and reading of memory parts	Application for programming ESP device family and sending commands
2	HomeWhiz v2.8.0.5 (Android)	Communication with TOE and necessary corporations	Application based on Android platform
3	HomeWhiz v3.1.13 (ios)	Communication with TOE and necessary corporations	Application based on ios platform
4	PuTTy v0.78	Serial communication with TOE and log monitoring	Serial communication monitoring application
5	Suricata IDS v6.0.8	Viewing connections to the wireless hotspot	Attack detection application
6	Samsung Galaxy Tab S2 Android 7.0	Running the HomeWhiz application	Tablet with Android operating system and providing Wi-Fi connection
7	ESP-Prog USB-TTL adapter	Serial communication via USB	USB-TTL converter adapter