	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015		
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05



# Certification Report

**EAL 2 Evaluation of**

**ARÇELİK A.Ş**

**Embedded Firmware Security Solution of Connectivity Features V1.0  
for Arçelik Bluetooth IoT Devices**


issued by

**Turkish Standards Institution  
Common Criteria Certification Scheme**

*Certificate Number: 21.0.03/TSE-CCCS-58*

*C.S.* *AK*

**Bu dokümanın güncelliği, elektronik ortamda TSE Doküman Yönetim Sisteminden takip edilmelidir.**

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

## TABLE OF CONTENTS



<b>TABLE OF CONTENTS .....</b>	<b>2</b>
DOCUMENT INFORMATION.....	3
DOCUMENT CHANGE LOG.....	3
DISCLAIMER.....	4
FOREWORD.....	5
RECOGNITION OF THE CERTIFICATE.....	6
<b>1 - EXECUTIVE SUMMARY.....</b>	<b>7</b>
1.1 TOE Overview.....	7
1.2 Threats .....	8
<b>2 - CERTIFICATION RESULTS.....</b>	<b>8</b>
2.1 Identification of Target of Evaluation .....	8
2.2 Security Policy.....	8
2.3 Assumptions and Clarification of Scope .....	9
2.4 Architectural Information .....	9
2.4.1 Logical Scope .....	9
2.4.2 Physical Scope.....	10
2.5 Documentation.....	11
2.6 IT Product Testing.....	11
2.7 Evaluated Configuration.....	11
2.8 Results of the Evaluation .....	12
2.9 Evaluator Comments / Recommendations.....	13
<b>3 - SECURITY TARGET .....</b>	<b>14</b>
<b>4 - BIBLIOGRAPHY .....</b>	<b>14</b>

C.Ş. 

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
		Yayın Tarihi	30/07/2015		
	<b>CCCS CERTIFICATION REPORT</b>	Revizyon Tarihi	29/04/2016	No	05

### DOCUMENT INFORMATION

Date of Issue	April 15 <sup>th</sup> , 2019
Approval Date	April 15 <sup>th</sup> , 2019
Certification Report Number	21.0.03/19-004
Sponsor and Developer	Arçelik A.Ş.
Evaluation Facility	Beam Technology Test Center
TOE	Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices
Pages	14


Prepared by	Cem ERDİVAN Common Criteria Inspection Expert	
Reviewed by	İbrahim Halil KIRMIZI Common Criteria Technical Responsible (Software Product Group)	

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

### DOCUMENT CHANGE LOG

Release	Date	Pages Affected	Remarks/Change Reference
1.0	April 16 <sup>th</sup> , 2019	All	First Release


C. E. 

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
		<b>Yayın Tarihi</b>	30/07/2015		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05

## DISCLAIMER

*This certification report and the IT product 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.*

c.e. 

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015		
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05

## 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 Beam Technology Testing Facility, 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 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 Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices whose evaluation was completed on February 21<sup>th</sup>, 2019 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 0.9 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](http://bilisim.tse.org.tr) portal and the Common Criteria Portal (the official web site of the Common Criteria Project).*

C. S. 


	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
		<b>Yayın Tarihi</b>	30/07/2015		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05

### **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>.*

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

## 1 - EXECUTIVE SUMMARY

### 1.1 TOE Overview

Embedded Firmware Security Solution of Connectivity Features v1.0 for Arçelik Bluetooth IoT Devices is an IoT device security solution which provides security functions to implement secure OTA firmware update of Arçelik IoT Devices mainboard and secure log storage of Arçelik 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 the download and install phases are protected by several cryptographic processes which are stated below.

Also, the device periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the device etc. The Secure Log Storage feature provides the log data to be stored and transmitted securely inside and outside (to Arçelik Cloud Server) of the product.

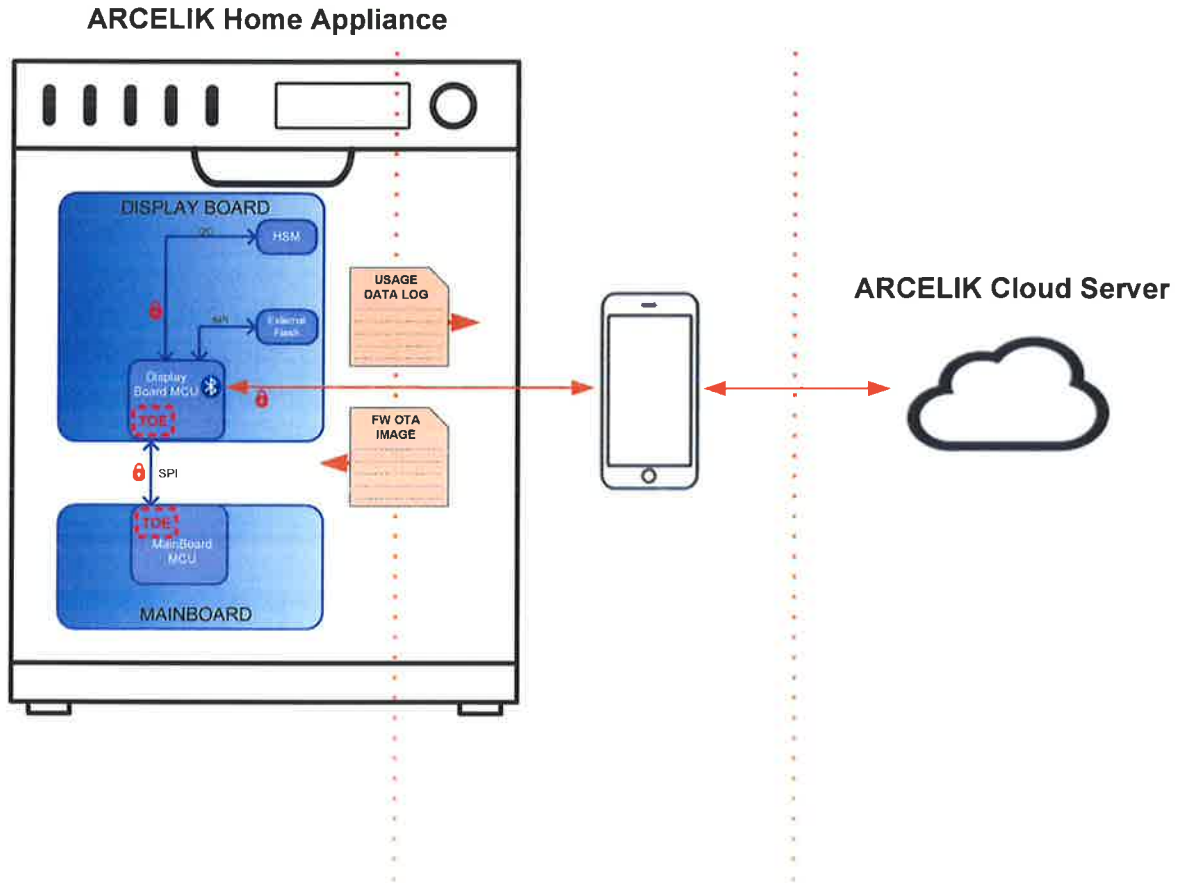


Figure 1 – External Entities of the TOE Operational Environment

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015		
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05

## 1.2 Threats

Threats are defined in Section 3.1 of Security Target Document v0.9.

## 2 - CERTIFICATION RESULTS

### 2.1 Identification of Target of Evaluation


<i>Certificate Number</i>	21.0.03/TSE-CCCS-58
<i>TOE Name and Version</i>	Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices
<i>Security Target Title</i>	Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices Security Target
<i>Security Target Version</i>	V0.9
<i>Security Target Date</i>	December 25 <sup>th</sup> , 2018
<i>Assurance Level</i>	EAL2
<i>Criteria</i>	<ul style="list-style-type: none"> <li>• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017</li> <li>• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017</li> <li>• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017</li> </ul>
<i>Methodology</i>	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
<i>Protection Profile Conformance</i>	None
<i>Common Criteria Conformance</i>	<ul style="list-style-type: none"> <li>• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017</li> <li>• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant</li> <li>• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant</li> </ul>
<i>Sponsor and Developer</i>	Arçelik A.Ş.
<i>Evaluation Facility</i>	Beam Technology Test Center
<i>Certification Scheme</i>	TSE CCCS

### 2.2 Security Policy

The TOE's purpose and key security features are as follows:

c. 2  
M



	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

- 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 Arçelik Cloud server and this enables only the firmware that are downloaded from the Arçelik Cloud server to be installable on the IoT device.

- Secure OTA Firmware Installation of Mainboard

The new mainboard firmware downloaded on the Arçelik IoT device is encrypted and stored in the external flash of display board. The TOE decrypts and verifies the mainboard firmware image. After the verification is successfully completed, the installation process starts. The mainboard firmware image is securely transferred from display board to mainboard via encrypted SPI line chunk by chunk. The mainboard microcontroller decrypts each OTA image chunks and the mainboard's bootloader programs its own flash accordingly. The firmware update of mainboard finished after all required packages arrived in mainboard.

- Secure Log Storage

The Arçelik IoT Devices periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the appliance etc. The Secure Log Storage function provides the log data to be stored and transmitted securely inside and outside (to Arçelik Cloud Server) of the product. The logged data are generated by mainboard. The log data are stored in display board's external flash until sent to Cloud Server. The Secure Log Storage Function uses the same secure SPI connection between DB and MB as stated in Secure OTA Firmware Installation phase. The communication between DB\_MCU and external flash is also secure.

## 2.3 Assumptions and Clarification of Scope

Please refer to Security Target Document v0.9 Section 3.2 for OSPs and Section 3.3 for Assumptions.


## 2.4 Architectural Information

### 2.4.1 Logical Scope

- Secure OTA Firmware Download

When a user connects a mobile device to Arçelik IoT Device via BLE, initially the firmware versions of the appliance and the latest firmware version published to Arçelik Cloud for respective appliance polled by the mobile device. After the comparison of firmware versions, the download request generated if needed.

The new OTA firmware update image is placed on Arçelik Cloud Server. The image on Cloud Server is signed and encrypted. Before the download process starts, the Appliance to Arçelik Cloud authentication and digital signature verification must be fulfilled. Appliance to Arçelik Cloud

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
		Yayın Tarihi	30/07/2015		
	<b>CCCS CERTIFICATION REPORT</b>	Revizyon Tarihi	29/04/2016	No	05

authentication is established using TLS 1.2 protocol and digital signature material downloaded through TLS channel from Cloud Server to Appliance. After successful completion of authentication and verification processes, OTA firmware update image starts download from Cloud Server to Appliance. This means that apart from authenticated and verified OTA firmware update images download process are blocked by TOE.

- **Secure OTA Firmware Installation of Mainboard**

The downloaded OTA firmware image on the Arçelik IoT Device is encrypted and stored in display board. Before passing to installation phase, the display board must implement verification and decryption to OTA image. The verification and decryption keys which was downloaded through TLS channel are used for fulfilling this step.

After verifying and decrypting the OTA image, the sending and installation process starts.

The DB transfers the OTA image through secure channel between DB and MB. The secure channel implemented by encryption and decryption of OTA image packages using DB-MB communication encryption key. After that the mainboard microcontroller gets the OTA package securely, the mainboard's bootloader programs its own flash accordingly. The firmware update of mainboard finished after all required packages arrived in mainboard.

- **Secure Log Storage**


The Arçelik IoT Device periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the appliance etc. The Secure Log Storage function provides that the log data is stored and transmitted securely. The logged data are generated by mainboard, sent to display board and then sent to Cloud Server if all security conditions are fulfilled. The Secure Log Storage Function uses the same secure channels between DB-MB and Appliance-Cloud Server which is implemented in OTA download and installation phases. The log data is stored in DB until the connection occurs. If there is a secure connection between appliance and Cloud Server, the log data is sent over this channel.

## 2.4.2 Physical Scope

The physical scope of TOE includes software elements that are used for securing the OTA firmware update and implementing securely usage log storage. A figure of the TOE can be found in below (Figure 2) and identifies its components. Only authenticated and properly encrypted firmware images downloaded and installed to the product electronic boards. The usage log data is always stored and transferred encrypted inside the product. Also, the usage log data sent from product to server encrypted by using a secure authenticated communication channel.

The TOE has two firmware elements. Those are display board microcontroller firmware and mainboard microcontroller firmware. Those firmware's are installed to the electronic boards in the factory during the serial production phase of IoT devices. Upon completion of the production, the IoT device delivered and set up to the user's property by Arçelik Service Technician. Also, the Arçelik User Guide is delivered to the user during the delivery.

C. E. M.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

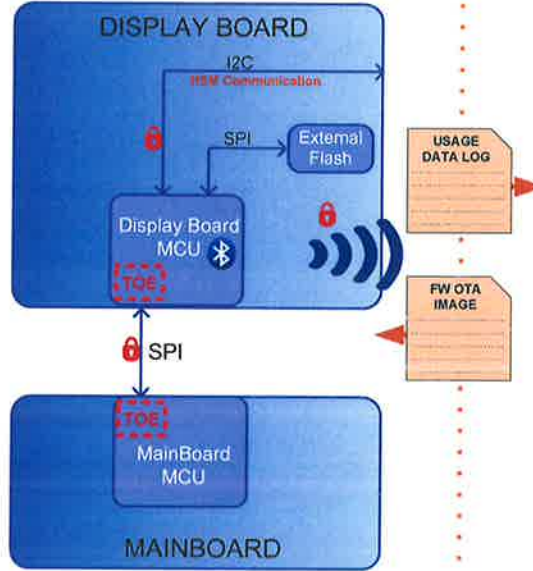


Figure 2 - Infrastructure of TOE

## 2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:


Document Name	Version	Release Date
Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices Security Target	v0.9	December 25 <sup>th</sup> , 2018
User Manual	v0.2	October 10 <sup>th</sup> , 2018

## 2.6 IT Product Testing

- **Developer Testing:** All TOE security behaviors have been tested by developer. Developer has conducted 11 functional tests in total, including negative-tests.
- **Evaluator Testing:** Evaluator has conducted all 11 developer tests. Since the scope of TOE is limited, no additional (independent) functional tests have been devised. TOE has passed all 11 functional tests to demonstrate that its security functions work as it is defined in the ST.
- **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 “Attackers with Basic Attack Potential”.

## 2.7 Evaluated Configuration

TOE Configuration:

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01		
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015		
		Revizyon Tarihi	29/04/2016	No	05

Embedded Firmware Security Solution of Connectivity Features v1.0 for Arçelik Bluetooth IoT Devices


### Required Non-TOE Hardware/Software Configuration:

Category		Specifications
Display Board	MPU	48-MHz ARM Cortex-M0 256KB Flash 32KB SRAM
	Bluetooth	BLE 4.2
	Flash Memory	2MB SPI Flash
	HSM	ECC508
Mainboard	MPU	48-MHz ARM Cortex-M0+ 128KB Flash 16KB RAM
Communication Interface	Mainboard MPU - Display MPU	SPI
	Display MPU - Flash Memory	SPI
	Display MPU - HSM	I2C
Mobile App/Device	HomeWhiz	Requires BLE4.2 or later mobile device Requires Android 5.0/iOS 9 or later mobile device

## 2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL2) and the security target evaluation) is summarized in the following table:

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.2	Security-enforcing functional specification	PASS
	ADV_TDS.1	Basic design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system	PASS
	ALC_CMS.2	Parts of the TOE 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


	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01		
		<b>Yayın Tarihi</b>	30/07/2015		
	<b>CCCS CERTIFICATION REPORT</b>	<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>	05

<b>Class Heading</b>	<b>Class Family</b>	<b>Description</b>	<b>Result</b>
ATE: Tests	ATE_COV.1	Evidence of coverage	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis	PASS

## 2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices” product, result of the evaluation, or the ETR.

c. e. m

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

### **3 - SECURITY TARGET**

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

**Title:** Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices Security Target

**Version:** v0.9

**Date of Document:** December 25<sup>th</sup>, 2018

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 - 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] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016
- [4] ETR v1.2 of Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices, Rel. Date: February 21<sup>st</sup>, 2019
- [5] Embedded Firmware Security Solution of Connectivity Features V1.0 for Arçelik Bluetooth IoT Devices Security Target, Version 0.9, Rel. Date: December 25<sup>th</sup>, 2018

c. < 