Arcelik Wi-Fi IoT Connectivity Solution v1.0

SECURITY TARGET v0.15

ARÇELİK A.Ş.

Document History

Version	Author	Date	Description
0.1	Çağatay BÜYÜKTOPÇU	07.09.2021	First Draft
0.2	Hamed MOHAMMADI	14.09.2021	TOE architecture fixed. Cryptography algorithm changed.
0.3	Serkan DEMİR	07.10.2021	Comments and clarification requests (24.09.2021) are cleared and/or commented.
0.4	Serkan DEMİR	11.11.2021	Comments and clarification requests (08.10.2021) are cleared and/or commented.
0.5	Serkan DEMİR	03.12.2021	Comments and clarification requests (08.11.2021) are cleared and/or commented.
0.6	Serkan DEMİR	14.01.2022	Comments and clarification requests (15.12.2021) are cleared and/or commented.
0.7	Serkan DEMİR	27.01.2022	Comments and clarification requests (27.01.2022) are cleared and/or commented.
0.8	Serkan DEMİR	21.02.2022	Comments and clarification requests (10.02.2022) are cleared and/or commented.
0.9	Serkan DEMİR	25.02.2022	Comments and clarification requests (21.02.2022) are cleared and/or commented.
0.10	Serkan DEMİR	22.04.2022	Change requests (according to meeting held on 19.04.2022) are cleared.
0.11	Serkan DEMİR	25.04.2022	Change requests (according to meeting held on 25.04.2022) are cleared.
0.12	Serkan DEMİR	17.12.2022	Scope changes are applied to the document.
0.13	Serkan DEMİR	22.12.2022	Requests in report (23.12.2022) are cleared.
0.14	Serkan DEMİR	28.12.2022	Requests in report (27.12.2022) are cleared.
0.15	Serkan DEMİR	29.12.2022	SFR - Objective Rationale table is updated.

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

1.1 ABBREVIATED TERMS

Abbreviations which are widely used in this document listed as below:

CK : Common Key

KT : Key Transfer

ECC : Elliptic Curve Cryptography

ECDH : Elliptic Curve Diffie-Hellman

ECDSA : Elliptic Curve Digital Signature Algorithm

HSM : Hardware Security Module

OTA : Over-The-Air

UART : Universal Asynchronous Receiver Transmitter

SPI : Serial Peripheral Interface

TLS : Transport Layer Security

AES : Advanced Encryption Standard

EAL : Evaluation Assurance Level

CC : Common Criteria

PP : Protection Profile

TOE : Target of Evaluation

SFR : Security Function Requirements

SFP : Security Function Policy

TSF : TOE Security Functions

TSP : TOE Security Policy

SHA : Secure Hash Algorithm

PSK : Pre – Shared Key

AWS EC2 : Amazon Web Server Elastic Compute Cloud

CRC : Cyclic Redundancy Check

1.2 ST & TOE REFERENCE

This section provides information to refer to the Security Target (ST) and Target of Evaluation (TOE) as in the following Table. The ST is identified by ST Title (including the TOE identification) and ST Version. The TOE is identified by TOE Title and the TOE Version.

ST Title	Arcelik Wi-Fi IoT Connectivity Solution v1.0 Security Target
ST Version & Date	v0.15 – 29.12.2022
TOE Title	Arcelik Wi-Fi IoT Connectivity Solution v1.0
TOE Version	v1.0
Assurance Level	EAL2
CC Identification	▪ Common Criteria Part 1 Version 3.1 Revision 5 ▪ Common Criteria Part 2 Version 3.1 Revision 5 ▪ Common Criteria Part 3 Version 3.1 Revision 5

Table 1 : ST and TOE References

1.3 TOE OVERVIEW

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.

1.3.1 TOE USAGE AND SECURITY FEATURE

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 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.

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

- ✓ 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.

1.3.2 TOE TYPE

TOE is an embedded firmware that consists of "Secure OTA Download", "Secure OTA Installation" and "Secure Usage Log Storage" security features. TOE has two different firmware in which one of them for appliances have UART connection and the one for appliances have SPI connection.

1.3.3 REQUIRED NON-TOE HARDWARE/SOFTWARE/FIRMWARE

Table 2 identifies required non-TOE hardware and software components.

Category		Specifications
Control Board	Control Board MPU	Depends on the appliance, there are different type of control boards have their own firmware.
	UI	There are different type of UI electronic boards depends on the projects & devices.
Connectivity Board	HSM	ECC508
Communication Interface	Control MCU - Connectivity MPU	UART/SPI
	Connectivity MPU - Flash Memory	SPI
	Connectivity MPU - HSM	I2C
Mobile App/Device	HomeWhiz	Requires BLE4.2 or later mobile device Requires Android 5.0/iOS 9 or later mobile device
Motor Board	Motor MCU	Renesas 64k Flash / 8k RAM
I/O Board	I/O Board	There are different type of I/O boards depends on the projects & devices.

Table 2 : Required Non-TOE Hardware & Software

1.3.4 TOE OPERATIONAL ENVIRONMENT

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 1 shows the external entities of the TOE operational environment.

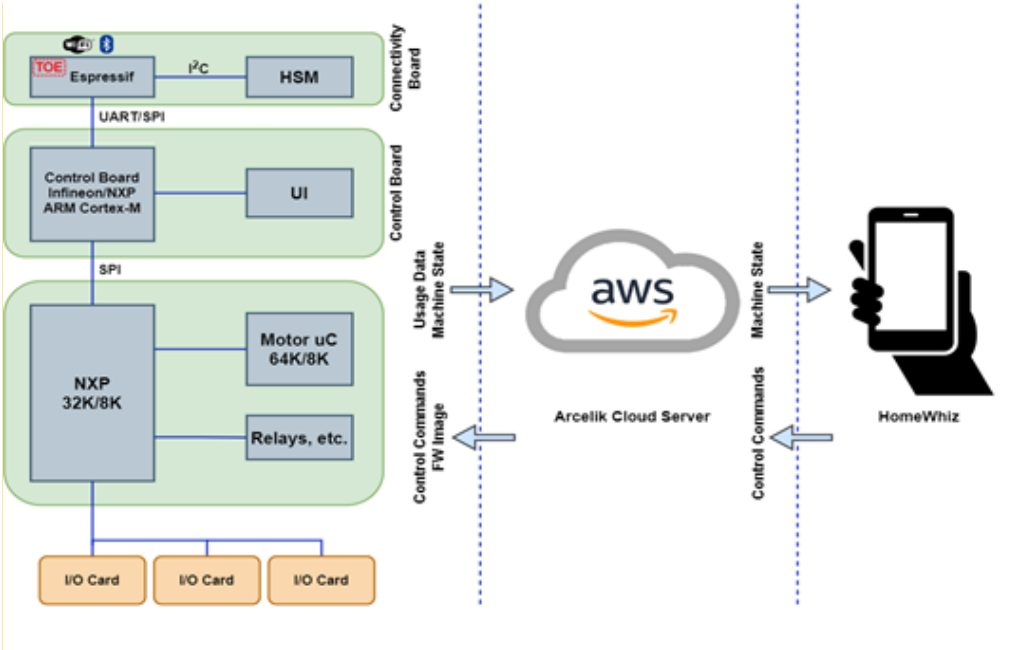

Figure 1 : External Entities of the TOE Operational Environment

✓ 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.

1.4 TOE DESCRIPTION

This section describes the TOE's scope in terms of physical and logical scope of the TOE to describe the environment in which the TOE can be operated.

1.4.1 PHYSICAL SCOPE OF TOE

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 2 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)

The IoT device is delivered to the user and set up by only Arcelik Service Technicians. In addition, Device User Guide is delivered to the user during delivery and it can be downloaded from product web page. [an example user guide is referenced as #5]

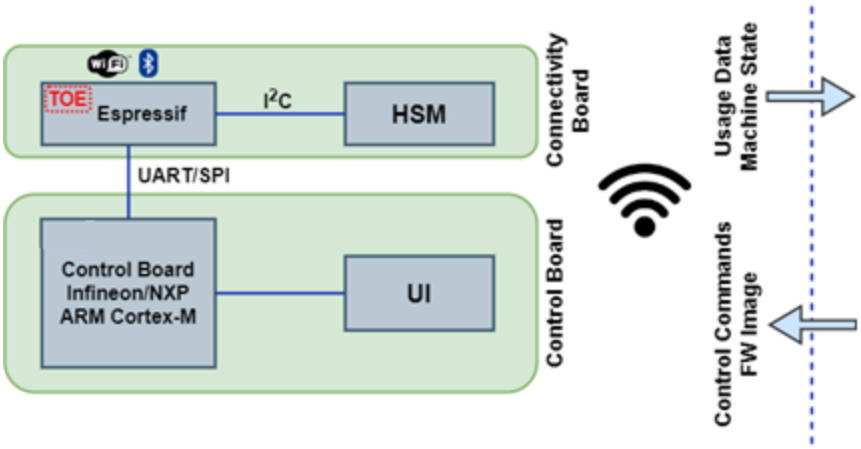

Figure 2 : Infrastructure of TOE

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 3 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 3 : Hardware Required by TOE

1.4.2 LOGICAL SCOPE OF TOE

The logical scope of the TOE is described through the security functionality as follows.

- ✓ Secure OTA Firmware Download

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

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

Server to Appliance. This means that download process is blocked by TOE if the OTA firmware update image is not authenticated and verified.

- ✓ Secure OTA Firmware Installation

  The downloaded OTA firmware image on the Arcelik IoT Device is encrypted and stored in connectivity board. The image is signed with Arcelik private key and only images with valid signature will be allowed to run. The validation is done by using connectivity board secure boot mechanism.

  If the OTA image is for connectivity board, connectivity board's bootloader directly gets the OTA packages from external flash and programs itself. If the OTA image is for other control boards rather than connectivity board, it is sent to the related board and validation is done under the responsibility of that board.

- ✓ Secure Log Storage

  The Arcelik IoT Device periodically logs usage data like diagnosis, customer detailed usage, electrical and sensor data of the appliance and so on. [These generated logs are imported from control board to TOE]. The Secure Log Storage function provides that the log data is stored securely. The logged data are generated by control board, and stored in the connectivity board's external flash and then sent to Cloud Server if all security conditions are fulfilled. The Secure Log Storage Function uses the same secure channels between Appliance-Cloud Server which is implemented in OTA download and installation phases. The log data is stored in connectivity board's external flash until the connection occurs. If there is a secure connection between appliance and Cloud Server, the log data is sent over this channel.

2 CONFORMANCE CLAIMS

2.1 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, Revision 5, April 2017, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 5, April 2017, [2], *Conformant*
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 5, April 2017, [3], *Conformant*

2.2 PP CLAIM

This ST does not claim conformance to any protection profile.

2.3 PACKAGE CLAIM

Evaluation Assurance Level is EAL2-conformant.

2.4 CONFORMANCE RATIONALE

No conformance rationale is necessary for this evaluation since this ST does not claim conformance to a Protection Profile.

3 SECURITY PROBLEM DEFINITION

This chapter defines the threats, OSPs (Organizational Security Policies) and assumptions which are intended to be addressed by the TOE and its operational environment.

The assets covered in the Connected Product are as follows.

- OTA Firmware image of connectivity board.
- Usage log data (lifetime, detailed usage, electrical, sensor data, etc.)
- TOE data (device control and monitoring data i.e. device operational state, program data, current working conditions, settings data, etc.)
- Cryptographic keys

3.1 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.

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.

3.2 ORGANIZATIONAL SECURITY POLICY

The organizational security policies are described below.

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.

3.3 ASSUMPTIONS

The assumptions are described in below.

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.

4 SECURITY OBJECTIVES

This Security Target classifies security objectives into 2 groups: security objectives for the TOE and security objectives for the operational environment. The security objectives for the TOE are those that are directly handled by the TOE, and the security objectives for the operational environment are those that must be addressed through the technical and procedural measures which are supported by the operational environment for the TOE to provide security functionality.

4.1 SECURITY OBJECTIVES FOR TOE

The security objectives for the TOE are described in below.

O.OtaPackageVerification

The TOE verifies that the OTA firmware package to be installed on the product is an authorized package through digital signature verification and there is no unauthorized modification during downloading process.

O.OtaPackageContentsProtection

The TOE stores content files of downloaded OTA package in an encrypted form on the product, and before the OTA package is installed, the TOE verifies its integrity and decrypts the encrypted OTA package content files.

O.LogDataProtection

Log data is generated in control board during the operation cycle of the appliance. The TOE imports user log data and stores it encrypted and when it's needed to transfer the log data inside the product, it transferred through secured channels.

O.CryptographicKeyManagement

TOE makes cryptographic key management through HSM using secure channel.

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

OE.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.

OE.FirmwareUpdateFileGenerationStorage

After shipment of connected products, the product firmware which includes the TOE is updated through mobile app (HomeWhiz) via OTA by end-user. The firmware update file (product firmware image) is digitally signed using ECDSA algorithm, stored in Arcelik Cloud Server. When the OTA request come from end-user, the TOE step into the process and provide Secure Firmware OTA to the products.

OE.SecureCloudServer

Arcelik Cloud Server which exists in the operating environment meets core security and compliance requirements, such as data locality, protection, and confidentiality.

OE.ProductUniqueIDRegistration

Arcelik must assign unique ID's to each product to manage them securely. This ID used to identify the product uniquely in Arcelik Cloud Server.

OE.ProductDisassemblyAuthorization

The user of the Arcelik IoT Device hasn't got authorization for disassemble the product and access the electronic boards (TOE) physically. This information is given to the user in user manual of appliance.

OE.CryptographicKeyProtection

All private cryptographic keys are stored in secure storage hardware element (HSM). The HSM prevents unauthorized physical access to the private keys stored in its slots.

4.3 SECURITY OBJECTIVE RATIONALE

The security objectives rationale demonstrates the following:

- Each threat, organizational security policies, and assumption is addressed by at least one security objective.

- Each security objective addresses at least one threat, organizational security policies, or assumption.

The following table demonstrates that all security objectives trace back to the threats, OSPs and assumptions in the security problem definition.

		THREATS					OSPs		ASSUMPTIONS		
		T.UnverifiedOtaDownload	T.ModifyingOtaImage	T.StealModifyUsageLogData	T.UnauthorizedKeyAccess	T.FirmwareCopyrightInfringement	P.FirmwareUpdateFileGenerationStorage	P.CloudSecureKeyManagement	A.SecureCloudServer	A.ProductUniqueIDRegistration	A.ProductDisassemblyAuthorization
SECURITY OBJECTIVES FOR TOE	O.OtaPackageVerification	X									
	O.OtaPackageContentsProtection		X			X					
	O.CryptographicKeyManagement				X						
	O.LogDataProtection			X							
SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT	OE.CloudSecureKeyManagement							X			
	OE.FirmwareUpdateFileGenerationStorage						X				
	OE.SecureCloudServer								X		
	OE.CryptographicKeyProtection				X						
	OE.ProductUniqueIDRegistration									X	
	OE.ProductDisassemblyAuthorization										X

Table 4 : Security Objective Rationale

O.OtaPackageVerification

This security objective ensures that only the authenticated OTA package for connectivity board firmware downloaded to the product via digital signature verification by the TOE. This security objective enables preventing the threat T.UnverifiedOtaDownload. For the OTA packages of other than the connectivity board (e.g. control board), image digital signature verification responsibility is on the board which owns the firmware.

O.OtaPackageContentsProtection

This security objective addresses the threat T.FirmwareCopyrightInfringement by preventing unauthorized use 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 T.ModifyingOtaImage by checking the integrity of the downloaded OTA package. By means of this, corrupted or modified OTA packages detected.

O.CryptographicKeyManagement

This security objective addresses the threat T.UnauthorizedKeyAccess in such that all private cryptographic keys can only be read by encrypted way.

O.LogDataProtection

This security objective enables preventing the threat T.StealModifyUsageLogData by storing the user log data encrypted and when its needed to transfer, it transfers encrypted data through secured channels.

OE.CloudSecureKeyManagement

This security objective for operational environment executes OSP (organization security policy), P.CloudSecureKeyManagement by performing following. 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 keys used for encrypting OTA firmware package is generated based on the AES (FIPS 197) standard by Arcelik Cloud Server 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.

OE.FirmwareUpdateFileGenerationStorage

This security objective for operational environment executes organizational security policy, P.FirmwareUpdateFileGenerationStorage by executing the following. After shipment of connected products, the product firmware which includes the TOE is updated through mobile app (HomeWhiz) via OTA by end-user. The firmware update file (product firmware image) is encrypted using AES (FIPS 197) cryptography algorithm and digitally signed using ECDSA algorithm, stored in Arcelik Cloud Server. When the OTA request come from end-user, the TOE step into the process and provide Secure Firmware OTA to the products.

OE.SecureCloudServer

This security objective for operational environment supports the assumption A.SecureCloudServer by executing the following. For secure operation of the TOE, Arcelik Cloud Server which exists in the operating environment is operated securely.

OE.ProductUniqueIDRegistration

This security objective for operational environment supports the assumption A.ProductUniqueIDRegistration by executing the following. Arcelik must assign unique ID's to each product to manage them securely. This ID used to identify the product uniquely in Arcelik Cloud Server.

OE.ProductDisassemblyAuthorization

This security objective for operational environment supports the assumption A.ProductDisassemblyAuthorization by executing the following. The user of the Arcelik IoT Device hasn't got authorization for disassemble the product and access the electronic boards (TOE) physically. This information is given to the user in user manual of appliance.

OE.CryptographicKeyProtection

This security objective addresses the threat T.UnauthorizedKeyAccess by stored all private cryptographic keys in HSM. Unauthorized physical and open text access to the private keys blocked by means of HSM.

5 EXTENDED COMPONENT DEFINITION

This Security Target does not include any extended component.

6 SECURITY REQUIREMENTS

SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 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 that are 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 ***italic and 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 *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 an identifier at the end of the component identifier as follows FDP_IFC.1 – IDENTIFIER

List of SFPs

Following table lists SFPs which are used in this document.

SFP	Brief Explanation
Cloud Flow Control SFP	Collected data transfer between device and Arcelik Cloud Servers via TLS 1.2 connections securely.
HSM Flow Control SFP	TOE and HSM communicate with each other over secure I^2C channel and transfer cryptographic keys. Device data collected from main board and display board is encrypted via HSM keys and stored at the ESP32 flash as encrypted.
CB Flow Control SFP	TOE and Control Board communicate with each other over SPI or UART channel and user log data generated in control board is transferred to the TOE. Communication's data verification is done by CRC error-detecting code.

Table 5 : Security Functional Policies

6.1 SECURITY FUNCTIONAL REQUIREMENTS (SFR)

This section specifies the security functional requirements for the TOE. It organizes the SFRs by the CC Part 2 classes.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage
FCS: Cryptographic Support	FCS_CKM.3: Cryptographic Key Access
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1: Cryptographic Operation
FDP: User Data Protection	FDP_ETC.2: Export of User Data with Security Attributes
	FDP_IFC.1 – CLOUD: Subset Information Flow Control
	FDP_IFC.1 – HSM: Subset Information Flow Control
	FDP_IFC.1 – CB: Subset Information Flow Control
	FDP_IFF.1 – CLOUD: Simple Security Attributes
	FDP_IFF.1 – HSM: Simple Security Attributes
	FDP_IFF.1 – CB: Simple Security Attributes
	FDP_ITC.1: Import of User Data Without Security Attributes
	FDP_ITC.2 – HSM: Import of User Data with Security Attributes
	FDP_UIT.1: Data Exchange Integrity
FMT: Security Management	FMT_MSA.1 – CLOUD: Management of Security Attributes
	FMT_MSA.1 – HSM: Management of Security Attributes
	FMT_MSA.1 – CB: Management of Security Attributes
	FMT_MSA.3 – CLOUD: Static Attribute Initialization
	FMT_MSA.3 – HSM: Static Attribute Initialization
	FMT_MSA.3 – CB: Static Attribute Initialization
	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_TDC.1: Inter-TSF Basic TSF Data Consistency
	FPT_ITC.1 – CLOUD: Inter-TSF Confidentiality During Transmission
	FPT_ITC.1 – HSM: Inter-TSF Confidentiality During Transmission
	FPT_ITI.1: Inter – TSF Detection of Modification
FTP: Trusted Paths/Channels	FTP_ITC.1 - HSM: Inter-TSF Trusted Channel
	FTP_ITC.1 - CB: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

Tablo 6 : Security Functional Requirements

6.1.1 Security Audit (FAU)

FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*detect*] unauthorized modifications to the stored audit records in the audit trail

6.1.2 Cryptographic Support (FCS)

FCS_CKM.3 Cryptographic Key Access

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 **[*accessing HSM keys*]** that meets the following: **[*None]***.

Application Note:

Cryptographic keys are stored inside the HSM chip and after booting keys are used for data encryption. The keys required for cryptographic process like encryption, decryption and authentication are transferred from HSM to RAM by using CK when they are necessary. CK is initially stored in internal flash and used for reaching HSM transport key and HSM authentication key. CK is removed from internal flash once HSM keys are accessed. Memory for HSM keys in RAM area are dynamically allocated. After usage of the HSM keys from RAM, they are removed.

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[*Recycling the MEMORY, i.e. Erasing and Rewriting to the Same Location of MEMORY*]** that meets the following: **[*None*]**.

Application Note:

Recycling the MEMORY is erasing and rewriting the same location of MEMORY. It is done via filling this location with value of **0x00**.

FCS_COP.1 Cryptographic 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 **[*Symmetric Key Encryption / Decryption*]** in accordance with a specified cryptographic algorithm **[*AES (in CBC mode)*]** and cryptographic key sizes **[*256bits*]** that meet the following: **[*FIPS 197]***.

Application Note:

Device data (device sensor data, customer device usage data and customer preferences) collected from main board and control board is transferred into the TOE. Transferred data is encrypted via HSM keys and stored at the ESP32 flash as encrypted. When Arcelik Cloud Services are available for ESP32, encrypted data stored in the flash is decrypted via HSM keys and sent to Arcelik Cloud Servers over TLS 1.2 secure channel. Control Board OTA image is also stored in connectivity board's flash as encrypted. Encrypted image is sent to the control board chunk by chunk.

6.1.3 User Data Protection (FDP)

FDP_ETC.2 Export of User Data with Security Attributes

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 **[*Cloud Flow Control SFP*]** when exporting user data, controlled under the SFP(s), outside of the TOE.

Application Note:

Device transfers collected data via TLS 1.2 connections securely to the Arcelik Cloud Servers. TLS 1.2 confirms integrity, authenticity, and confidentiality of the data.

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.1 - CLOUD Subset Information Flow Control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [***Cloud Flow Control SFP***] on [***Subject: Connectivity Board, Information: Stored Usage Log Operation: Send***].

FDP_IFC.1 - HSM **Subset Information Flow Control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[*HSM Flow Control SFP*]** on **[*Subject: Connectivity Board, Information:***

- ***Cryptographic Keys Operation: Receive,***
- ***Certificates: Receive].***

FDP_IFC.1 – CB **Subset Information Flow Control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [***CB Flow Control SFP***] on [***Subject: Connectivity Board, Information: Log Data: Receive***]

FDP_IFF.1 - CLOUD **Simple Security Attributes**

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the **[*Cloud Flow Control SFP*]** based on the following types of subject and information security attributes:

[*Subject: Connectivity Board, Information: Stored Usage Log,*

Subject security attribute: None, Information security attribute: Security Session Existence].

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: **[*TSF shall permit Connectivity Board to send Stored Usage Log via Wi-fi Data Communication to Cloud, if Security Session exists*]**.

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 - HSM Simple Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the **[*HSM Flow Control SFP*]** based on the following types of subject and information security attributes:

**[*Subject: Connectivity Board, Information: Cryptographic Keys (except Authorization Key and Transport Key), Certificates*

Subject security attribute: Certificate signature, Information security attribute: Key size].

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: **[*TSF shall permit Connectivity Board to receive cryptographic keys from HSM, if the Authorization Key is verified*]**.

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*]**.

Application Note:

AUTH and TRSPT keys are imported from HSM at the beginning (when the device first time energized) by using CK and saved into the flash. Therefore, they are not part of the cryptographic keys mentioned in HSM Flow Control SFP.

FDP_IFF.1 – CB Simple Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the **[*CB Flow Control SFP*]** based on the following types of subject and information security attributes:

[*Subject: Connectivity Board, Information: Log Data,*

***Subject security attribute: Log Data CRC code, Information security attribute: Log Data size*]**.

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: **[*TSF shall permit Connectivity Board to receive user log data from Control Board, if there exist a new log data waiting to be transferred on the control board*]**.

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_ITC.1 Import of User Data Without Security Attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [***CB Flow Control SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***none***].

FDP_ITC.2 Import of User Data with Security Attributes

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 **[*HSM 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_UIT.1 Data exchange integrity

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 **[*CB Flow Control SFP*]** to [*receive*] data packages in a manner protected from [*modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [*modification, deletion, insertion*] has occurred.

Application Note:

Data package integrity between TOE and CB communication is provided by CRC checksum control. CRC is calculated as summation of every byte after start word which is 0xAA.

6.1.4 Security Management (FMT)

FMT_MSA.1 - CLOUD Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[*Cloud Flow Control SFP*]** to restrict the ability to **[***modify, delete, [**change**]***]** the security attributes **[*user data, telemetry data*]** to **[*none*]**.

FMT_MSA.1 - HSM Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[*HSM Flow Control SFP*]** to restrict the ability to **[***modify, delete, [**change, decrypt**]***]** the security attributes **[*device data*]** to **[*none*]**.

FMT_MSA.1 – CB Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[*CB Flow Control SFP*]** to restrict the ability to **[***modify, delete, [**change, decrypt**]***] the security attributes **[*device data*]** to **[*none*]**.

FMT_MSA.3 - CLOUD Static Attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[*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_MSA.3 - HSM Static Attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[*HSM 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 – CB Static Attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **[*CB 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_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[*management of security attributes*]**.

6.1.5 Protection of the TSF (FPT)

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [***cryptographic key, certificates, OTA image***] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [***Cloud Flow Control SFP, HSM Flow Control SFP***] when interpreting the TSF data from another trusted IT product.

FPT_ITC.1 – HSM Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

FPT_ITC.1 – CLOUD Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Application Note:

TSF shall permit Connectivity Board to receive OTA Image via Wi-fi Data Communication from Cloud if signature of FW OTA Image is verified successfully.

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [***OTA image signature control***].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [***keep the existing firmware, do not install the newcoming OTA image and delete the failed OTA image***] if modifications are detected.

6.1.6 Trusted Path/Channels (FTP)

FTP_ITC.1 - HSM Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[*TOE – HSM communication***].

FTP_ITC.1 - CB Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[*TOE – CB communication*]**.

FTP_TRP.1 Trusted path

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 [***Secure OTA Firmware Download and Secure Log Sending with secure channel TLS to Cloud***].

6.2 SECURITY ASSURANCE REQUIREMENTS (SAR)

The TOE meets the security assurance requirements for EAL2. The following table is the summary for the 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

Tablo 7 : Security Assurance Requirements

6.3 SECURITY REQUIREMENTS RATIONALE

Security Requirements Rationale demonstrates that the described security requirements are suitable to satisfy security objectives and, as a result, appropriate to address security problems.

6.3.1 SFR RATIONALE

SFR Dependency Rationale

The table below shows dependencies of security functional requirements.

No	SFR	Dependency	Dependency Met?
1	FAU_STG.1	FAU_GEN.1	FAU_GEN.1 is not fulfilled since user data logs are generated in the environment (control board) and they are imported from environment into TOE after checking message CRC code control.
2	FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2 FCS_CKM.4
3	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.2
4	FCS_COP.1	[FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2 FCS_CKM.4
5	FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1 - CLOUD
6	FDP_IFC.1 - CLOUD	FDP_IFF.1	FDP_IFF.1 - CLOUD
7	FDP_IFC.1 - HSM	FDP_IFF.1	FDP_IFF.1 - HSM
8	FDP_IFC.1 - CB	FDP_IFF.1	FDP_IFF.1 - CB
9	FDP_IFF.1 - CLOUD	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 - CLOUD FMT_MSA.3 - CLOUD

10	FDP_IFF.1 - HSM	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 - HSM FMT_MSA.3 - HSM
11	FDP_IFF.1 - CB	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 - CB FMT_MSA.3 - CB
12	FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_IFC.1 – CB FMT_MSA.3 - CB
13	FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_IFC.1 - HSM FTP_ITC.1 - HSM FPT_TDC.1
14	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	 FDP_IFC.1 – CB FTP_ITC.1 - CB
15	FMT_MSA.1 - CLOUD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 – CLOUD FMT_SMF.1 Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1
16	FMT_MSA.1 - HSM	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 – HSM FMT_SMF.1 Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1
17	FMT_MSA.1 - CB	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 – CB FMT_SMF.1 Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1

18	FMT_MSA.3 - CLOUD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 – CLOUD Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1
19	FMT_MSA.3 - HSM	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 – HSM Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1
20	FMT_MSA.3 - CB	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 – CB Because of the information flow controls which used in TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of SFR FMT_SMR.1
21	FMT_SMF.1	-	-
22	FPT_TDC.1	-	-
23	FPT_ITC.1 – CLOUD	-	-
24	FPT_ITC.1 – HSM	-	-
25	FPT_ITI.1	-	-
26	FTP_ITC.1 – HSM	-	-
27	FTP_ITC.1 – CB	-	-
28	FTP_TRP.1	-	-

Tablo 8 : SFR Dependency Table

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.

	Security Objectives			
	O.OtaPackage Verification	O.OtaPackage Contents Protection	O.LogData Protection	O.Cryptographic KeyManagement
FAU_STG.1			X	
FCS_CKM.3				X
FCS_CKM.4				X
FCS_COP.1		X	X	X
FDP_ETC.2			X	
FDP_IFC.1 - CLOUD			X	
FDP_IFC.1 - HSM		X	X	X
FDP_IFC.1 - CB			X	
FDP_IFF.1 - CLOUD			X	
FDP_IFF.1 - HSM		X	X	X
FDP_IFF.1 - CB			X	
FDP_ITC.1			X	
FDP_ITC.2			X	X
FDP_UIT.1			X	
FMT_MSA.1 - CLOUD			X	
FMT_MSA.1 - HSM			X	X
FMT_MSA.1 - CB			X	
FMT_MSA.3 - CLOUD			X	
FMT_MSA.3 - HSM		X	X	X
FMT_MSA.3 - CB			X	
FMT_SMF.1		X	X	X
FPT_TDC.1			X	X
FPT_ITC.1 - CLOUD	X			
FPT_ITC.1 - HSM			X	X
FPT_ITI.1	X			
FTP_ITC.1 - HSM			X	X
FTP_ITC.1 - CB			X	
FTP_TRP.1	X	X	X	

Tablo 9 : SFR - Objective Rationale Table

O.OtaPackageVerification

Verification of OTA packages are done by public key which are stored in TOE's e-Fuse storage area. This corresponds with FPT_ITC.1 – CLOUD. OTA image integrity is consistently checked by FPT_TDC.1. OTA image signature control and verification is done via FPT_ITI.1. The TLS trusted path which is established between Cloud server and TOE meets by *FTP_TRP.1.*

O.OtaPackageContentsProtection

Content protection of the OTA image is done via FCS_COP.1 as it is described in the application note. OTA image for the control board is encrypted by keys in TOE which are imported from the HSM and corresponds to *FDP_IFC.1 – HSM* and *FDP_IFF.1 – HSM*. Encrypted image is stored in connectivity board's flash. The TLS trusted path which is established between Cloud server and TOE meets by *FTP_TRP.1.*

O.LogDataProtection

The device Log Data is created in control board and connectivity board imports the generated user log data. Subset information flow control between CB and TOE correspond with *FDP_IFC.1 - CB.* The CB Flow Control SFP corresponds with *FDP_IFF.1 - CB.* After the Log data is transferred to connectivity Board, the connectivity Board's microcontroller transfers it to External Flash for storage purpose if there is no valid internet connection. Connectivity Board's microcontroller encrypts the log data with FCS_COP.1 using the Flash Encryption Key before sending it to its external flash corresponds with *FDP_IFF.1 – HSM*. The Flash Encryption Key is accessed from HSM and used for encrypting/decrypting the Log Data using Flash Encryption Key before transferring to External Flash. Subset information flow control between Cloud and TOE correspond with *FDP_IFC.1 - CLOUD.* The Cloud Flow Control SFP corresponds with *FDP_IFF.1 - CLOUD. FDP_ETC.2* helps the objective by exporting Log Data with security attributes from TOE to Cloud Server. Log data integrity between CB and TOE is based on CRC code check of messages and corresponds to *FDP_UIT.1*.

O.CryptographicKeyManagement

The TOE uses several cryptographic keys and certificates for ensuring the security objectives. Due to secure storage of those cryptographic keys and certificates an HSM module exists in the system. During the initialization phase of TOE, a secure I^2C communication channel is established between HSM and connectivity board's microcontroller (TOE). The trusted I^2C channel between TOE to HSM represented by *FTP_ITC.1 - HSM*. The bus between TOE to HSM is encrypted using the Trsprt Key by FCS_COP.1. The Common Key is used for accessing the Trsprt Key. *FCS_CKM.3* helps the objective by accessing the HSM keys Trsprt Key and Auth Key.

The Common Key is removed from the MEMORY after reaching the Trsprt and Auth keys. Importing cryptographic keys and certificates from HSM to TOE is provided by *FDP_ITC.2.* The HSM Flow Control SFP corresponds with *FDP_IFF.1 - HSM.* Subset information flow control between HSM and TOE correspond with *FDP_IFC.1 - HSM.*

6.3.2 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.

7 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 "secure OTA firmware download", "secure OTA firmware Installation of connectivity and control board" and "Secure Log Storage".

7.1 Secure OTA Firmware Download

When a user connects a mobile device to Arcelik IoT Device via Wi-fi, initially the firmware versions of the appliance and the latest firmware version published to Arcelik Cloud Server for respective appliance polled by the mobile device. After the comparison of firmware versions, the download process starts if needed. Appliance to Arcelik Cloud Server authentication is established using TLS 1.2 protocol. Each TLS connection is established using a unique session key which are produced by HSM. In order to use TLS connection device private key inside the HSM should be authorized. Authorization is done using AUTH_KEY and TRNSP_KEY that are read from HSM by using CK. These keys are unique keys per device. The new OTA firmware update image is placed on Arcelik Cloud Server. The image on Cloud Server is signed using ECDSA. After downloading OTA image HSM verifies the signature of OTA.

Functional Requirement Satisfied: *FCS_CKM.3, 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.*

7.2 Secure OTA Firmware Installation of Connectivity Board

The new connectivity board's firmware image downloaded on the Arcelik IoT Device is stored in the external flash of connectivity board. To verify the downloaded OTA image, the connectivity board controls the signature of the OTA image. The connectivity board's secure boot calculates the hash of the image and uses the ECDSA public key stored in e-Fuse area of the connectivity board MCU to verify the signature. After the verification is successfully completed, the new OTA image is selected as a valid firmware and replaces the existing firmware.

Functional Requirement Satisfied: *FDP_IFF.1 - HSM, FPT_TDC.1, FPT_ITI.1.*

7.3 Secure Log Storage

The Arcelik IoT Device 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 that the log data is stored and is transmitted securely. The logged data are generated by control board. Log data is imported by the connectivity board. A format of log data is only known by Arcelik. It also includes CRC which can be used to detect modification to user data. The Secure Log Storage function uses secure channels that are already established between the components of appliance and Cloud Server. The log data is stored until the connection occurs. If there is a secure connection between appliance and Cloud Server, the log data is sent over this channel. The Secure Log Storage Function uses the same UART or SPI connection between control board and connectivity board. (There are two different connectivity board firmware to support either SPI connection or UART connection. For an appliance, only one of them is active in connectivity board depending on the connection used between TOE and control board.) Then control board transfers the log data to connectivity board's MCU. Connectivity board's MCU writes them into external flash by using flash encryption key if there is no active internet connection. In this process, key that is used to encrypt the log data is read from HSM. This reading process is an encrypted read process. In this process, another key is used which is named transport key. This key is used in encryption of the link between HSM and connectivity board. Every encrypted read operation uses this key. Transport key is read from HSM via Common Key and once required keys are escrowed, CK is destroyed. When the connectivity board's sending process starts, connectivity board reads the encrypted log data, decrypts it, and sends it over the TLS to the Cloud Server.

Functional Requirement Satisfied: *FAU_STG.1, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FDP_ETC.2, FDP_IFC.1 – HSM, FDP_IFC.1 – CB, FDP_IFC.1 - CLOUD, FDP_IFF.1 - CLOUD, FDP_IFF.1 - HSM, 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_ITC.1 – HSM, FTP_ITC.1 – HSM, FTP_ITC.1 – CB, FTP_TRP.1.*

8 REFERENCES

[1] FIPS 186 – 3 Digital Signature Standard (DSS)

https://csrc.nist.gov/csrc/media/publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf

[2] FIPS 197 Advanced Encryption Standard (AES)

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[3] Hardware Security Module (HSM)

https://csrc.nist.gov/glossary/term/hardware_security_module_hsm

[4] Arcelik web site

https://www.arcelikglobal.com/tr/

[5] Product Information

Product Type : Refrigerator

Product Model Name : 670560 EI

Production Date : 2020

User Manual Name : “7298220286_202011181550183_User Manual - File (Long)tr_TR”

User Manual Download Link : https://www.beko.com.tr/no-frost-buzdolabi/670561-ei-buzdolabi