INVISHIELD

Security Target

v1.0

05/02/2025

Created by

Version control

Version	Comment	Date
0.1	Initial draft version	06/03/2023
0.2	Minor changes in sections 1.1, 2.3 and 4. Changes according TOE functionalities in sections 2.1 and 3.1. Requirements of section 5 have been updated.	09/10/2023
0.3	Section 4.3 modified according to new security problem definition. Requirements of section 5.6 modified according to new TOE security functionalities.	13/12/2023
0.4	General changes throughout the document according to new security implementations from the manufacturer to the TOE.	07/05/2024
0.5	Minor changes in section 4.1. Requirements of sections 5.5 and 5.6 updated according to manufacturer comments.	14/05/2024
0.6	Changes in section 4.1 according to the use case in the operational environment. Minor changes in section 3.1.	31/05/2024
0.7	Changes in section 4.1 according to assumptions of the security problem definition. Section 2.3 updated according to TOE required considerations. TOE version and manuals have been updated.	17/06/2024
0.8	Section 2.2 updated according to last user manual version. TOE mobile application updated to its last version in section 1.1. Section 2.3 updated according to required TOE considerations.	04/09/2024
0.9	Minor changes in sections 2.1, 2.2, 2.3 and 3.1 according to manufacturer modifications in TOE manuals.	26/11/2024
1.0	Minor changes in section 1.1 and user manuals declared in section 2.2.	05/02/2025

Table of contents

1 Introduction

This document is the Security Target for **INVISHIELD**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Sponsor, TOE and evaluation information

Applicant data	AMLO Sistemas de Seguridad SL
Developer data	AMLO Sistemas de Seguridad SL
Contact information of developer	Paseo de Independencia Nº5 Principal Izquierda 50001, Zaragoza Lorenzo Dieste Burguete lorenzo@invishield.io
TOE name	INVISHIELD
TOE version	Hardware device with firmware v01.00.007(HW 3.0) Mobile application v1.0.17 (DCB804D561773409E99CDE939AC8824F6401E2949F9A7DDF2363F633DD1D1352 – SHA256)
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE secure use, installation and configuration guides*
Taxonomy according to CNN-STIC-140	N/A

1.2 Methodology and evaluation criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE description

2.1 TOE Functional description

The TOE is composed of two elements; the first known as TOE hardware device, and the second is the TOE mobile application.

The appliance (Figure 1) is a hardware USB 3.0 and Gigabit Ethernet switch configurable via Bluetooth with an upgradeable and signed firmware. The firmware is updated when connected via Bluetooth (BLE v4.2) to the mobile device running the TOE Invishield mobile application and stores the instructions that the TOE hardware device can execute. This is a physical device with no MAC addresses on its interfaces which core functionality is provided by hardware.

Figure 1. TOE hardware device

The TOE mobile application is the software which provides an interface where the user can perform the management of the hardware device via commands.

This hardware device has several connections and LED indicators as described in Table 1 and Table 2:

Port	Type	Description
DCin	Input	Power supply (5VDC 10W)
RST	Button	Bluetooth Activation and Reset
USBin	Input	USB 3.0 input port
USBout1	Output	Configurable USB 3.0 port
USBout2	Output	Configurable USB 3.0 port
ETHin	Input	Gigabit Ethernet input port
ETHout1	Output	Configurable Gigabit Ethernet port
ETHout2	Output	Configurable Gigabit Ethernet port

Table 1. TOE physical connections

LED	Description
DCin	Device powered on
Status	BLE enabled or disabled
Status (Flashes 3s)	Device reset
USBout1	USB output enabled or disabled
USBout2	USB output enabled or disabled
ETHout1	Ethernet port enabled or disabled
ETHout2	Ethernet port enabled or disabled

Table 2. TOE LED indicators

The TOE hardware device has one USB and one Ethernet input and two outputs for each of them (two USBs and two Ethernets) which can be activated independently. Only one of the USB outputs can be activated at the same time. The outputs can be activated and deactivated on days and times determined by the configuration, through schedules and rules.

Configuration about schedules and rules is done by using the Invishield mobile application. The TOE hardware device receives the configuration through commands via Bluetooth generated by the TOE mobile application.

The architecture of the TOE hardware device is depicted below:

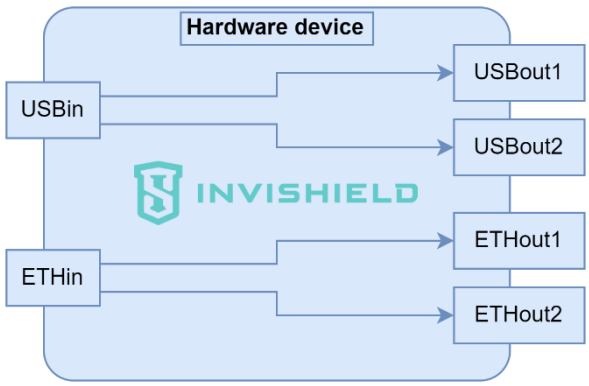

Figure 2. TOE hardware device architecture

The main capabilities of the TOE are the following:

- **Schedules management**. A schedule consists of a series of rules. The TOE hardware device applies the schedule stored in the memory and new schedules are received through a command via Bluetooth, generated by the TOE mobile application. The rules of a schedule define the date and time when an output interface is enabled or disabled. Schedules can be uploaded to the TOE hardware device or retrieved from it.
- **Rules management**. Rules allow to change the status of an output at a specific day and time. A rule is assigned to a single output. The TOE only allows one of the USB outputs to be active at a time. In case the configuration rules overlap the USB activations, it is not allowed to define that configuration for schedules.
- **Product configuration**. The TOE hardware device allows to receive configurations through commands sent over a single communication channel via Bluetooth, allowing the following actions:
    - Date and time synchronization.
    - Schedule management.
    - Management of the states of the outputs.
    - Firmware upgrades.

The TOE provides the following security functionalities:

- **SF. Audit**. The TOE generates audit information according to the events generated and behaviour detected during its execution.
- **SF. Trusted administration**. The TOE allows the user to perform the management functionalities locally and remotely through the TOE mobile application.

- **SF. Trusted Installation and Updates**. The TOE can be updated securely to address security issues detected by the manufacturer.
- **SF. Cryptography**. The TOE supports secure cryptographic mechanisms composed by algorithms accepted by the CCN-STIC-807 guide.
- **SF. Bluetooth Communication Channel**. The TOE hardware device provides Bluetooth (BLE v4.2) communication to exchange information with the mobile device running the TOE mobile application, such as schedules and rules.
- **SF. Trusted Flow Control**. The TOE provides secure flow control capabilities managed by schedules previously defined by the user and do not share information between interfaces. Moreover, both TOE components protect the transmitted commands.

2.2 Identification of the TOE secure use, installation and configuration guides

The following table lists the documents and user's guides necessary to carry out the configuration of the TOE properly:

Document's type	Document's name	Document's version (update-history-date)
PDF	Invishield: User manual	1.0.10

2.3 TOE usage description

The following considerations, referred in the documentation of section *2.2: Identification of the TOE secure use, installation and configuration guides*, must be taken into account previously to achieve the evaluated configuration:

- The manufacturer provides directly to the customer with both TOE mobile application and TOE hardware device. To install the TOE mobile application according to the considerations of the evaluated configuration, it is necessary to **follow the user guidelines and ensure that the integrity of the downloaded application file is assured** by following the steps in the subsection on integrity verification in "*Instalación de aplicación vía APK*".

- By default, the BLE connection is disabled, so the first step is to enable the Bluetooth connection in the hardware device, as defined in the "*Encender Bluetooth dispositivo*" section of the user manual. For the TOE to perform the security functionalities, the Bluetooth channel doesn't need to be active on the TOE hardware device, but it is necessary to have it active to send the configuration to the TOE hardware device from the TOE mobile application.

- The second step is to connect the TOE hardware device with the application, as defined in the "*Puesta en marcha de Invishield*" section of the user manual, using the pairing PIN described in this section. When the authorized user, via the mobile device with the TOE mobile application, pairs with the TOE hardware device, the status LED will change indicating that the TOE hardware device has been paired with a mobile device via Bluetooth.

    - For the first time using the TOE mobile application, when clicking on the "*Buscar Dispositivos*" button a message appears indicating that, since Android v6.0, the location permission must be granted to the TOE mobile application. Accept this message and open the Android settings to allow this permission for the TOE mobile application.

- After pairing the TOE hardware device with the authorized user's mobile, to use the TOE mobile application, the authorized user must use the default PIN for a first-time access, defined in the "*Puesta en marcha de Invishield*". Then, the authorized user must change the default PIN as defined in the *"Cambiar el código PIN"* section of the user manual with a length of 6-digit numbers. First, the authorized user must introduce the actual PIN (default one) to change it.

- The TOE hardware device will be saved in the known devices list of the TOE mobile application, so the devices search will not be necessary for future connections.

- To create, modify or delete an existent schedule, the authorized user must follow the steps defined in "*Programas*" section.

    - To create a schedule, the authorized user must select the "*Programas*" option and then click on "*Nuevo programa*". The schedules are composed by a group of rules, and these rules define the status of any output of the TOE hardware device at a given date and time. For the configuration of new rules, view the created ones, modify or delete them, the authorized user must follow the steps defined in the subsections "Reglas", "*Añadir nuevas reglas*" and "*Ver reglas*" of this section.

    - In this part of the configuration, it is important to note that the TOE hardware device only allows one of the USB outputs to be active at a time. In case the configuration rules overlap the USB activations, the application displays warnings that there is a

conflict, and if the authorized user doesn´t change the configuration, the TOE hardware device will only activate the USBout1 port.

- When all of these previous steps are configured, the authorized user must configure the TOE hardware device to apply the schedule defined and synchronize data time.
    - To do this last function, the authorized user must follow the steps mentioned in the subsection "*Sincronización de fecha y hora*" of the section "*Configuración de Invishield*".
    - To apply a defined schedule into the TOE hardware device, the authorized user must follow the steps mentioned in the subsection "*Configuración de programa*" of the section "*Configuración de Invishield*". The authorized user can recovery an applied schedule in the TOE in this part of the configuration too.
    - The authorized user can also force the status of the outputs in this section of the configuration, in the subsection "*Forzar estado de salida*", update the firmware (subsection "*Actualización de Firmware*"), read the activity logs (subsection "*Lectura de registros de actividad*").
- The TOE allows two different configurations for turning off the Bluetooth interface after the device is set up. For the evaluated configuration, the "*Modo Instantáneo*" option is selected in the subsection "*Modo apagado BLE*" of the section "*Configuración de Invishield*".
- Finally, deactivate the Bluetooth connection when the device is already configured by pressing the RST button.
- To perform a factory reset to the TOE hardware device, the authorized user must follow the steps defined in the section "*Restauración de fábrica*".

DISCLAIMER: There is a hard reset option for the communication between the TOE mobile application and the TOE hardware device which is detailed below.

This feature is implemented through a hidden interface and the steps to perform this reset must be provided by the manufacturer. This option does not allow connection without knowing the PIN. In the evaluated configuration, by executing the factory reset, the PIN is known as "1234". It is a mechanism that allows connection in cases where the TOE hardware device is not synchronized with the TOE mobile application, as may be the case when the RTC battery runs out. The steps to access this reset mode are as follows:

I. (Factory Reset) Press and hold the bootloader button for approximately 10 seconds until the green LEDs start flashing.

II. Wait for the blinking sequence to end, the Bluetooth LED will also turn off.

III. Press the button to turn on Bluetooth.

IV. Search for the device in the app.

V. Enter the default PIN. For the evaluated configuration is "1234".

VI. In case the red error message "*Incorrect PIN code*" is displayed.

    a. Press 3 times (1 time every second) the lower left corner of the white PIN entry box.

    b. A hidden orange button will appear that says, "*Repair device*".

    c. Press the "*Repair Device*" button (the PIN entered must remain "1234").

d. Check that the device is added. Click on the device (the Bluetooth symbol should appear on the right) and the device screen will appear.

e. Enter the PIN to connect.

f. In case of error repeat steps (a, b, c).

g. In case of connection, synchronize the date and time of the TOE hardware device.

Apart from these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in section *5: Security Functional Requirements* of this document beyond the TOE guide's steps.

3 Operational environment

3.1 Operational environment description

There are defined the following components for the operational environment:

- **Operator**. This is the authorized user that performs the management of the TOE hardware device through the TOE mobile application.
- **Smartphone**. This is the mobile device, Android 8.0 or higher, that runs the TOE mobile application and provides the Bluetooth connection to link with the TOE hardware device.
    - The evaluated configuration considers using the following mobile devices: OnePlus 6T (Android 9) and Google Pixel 4a (Android 14).
- **Corporate network**. This is the corporate network that is connected via Ethernet to the TOE and allows the management of the backup devices located at the ETH output interfaces.
- **Server.** This is the corporate server that connects via USB to the TOE and allows the management of the backup devices located in the USB output interfaces.
- **Backup devices.** These are the backup devices (i.e., NAS or SSDs) connected to the TOE output interfaces that are managed by the input devices, based on the TOE data flow control.

The operational environment is depicted in the following diagram:

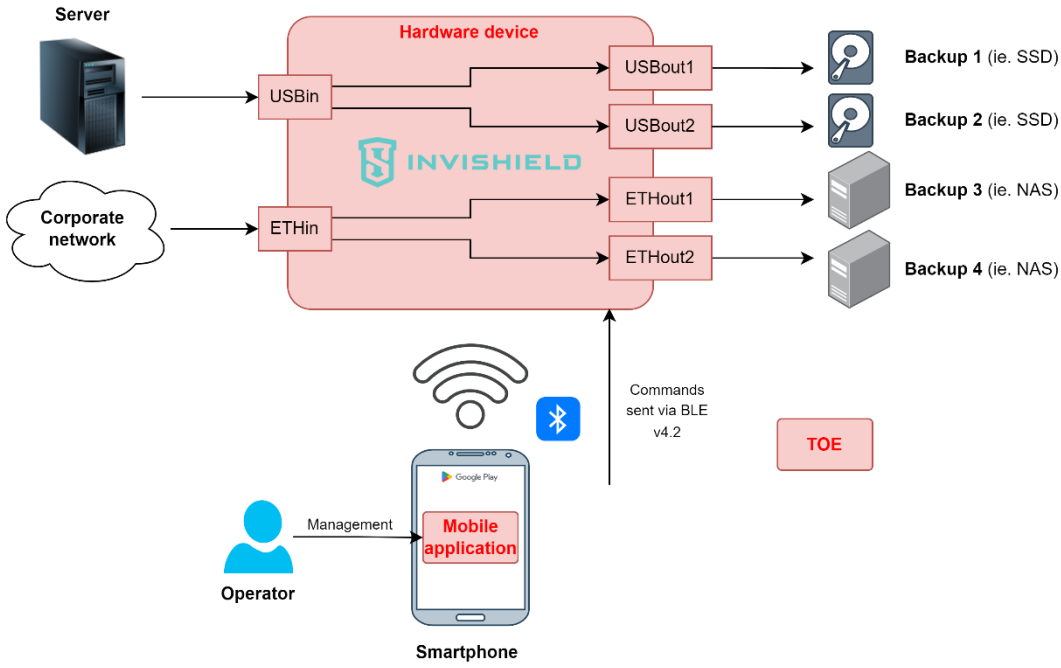

Figure 3. TOE's operational environment

There are no communication channels between the TOE hardware device and other elements of the operational environment, since the output and input interfaces make a physical connection (HUB type) also physically managed by the TOE hardware device, so it represents a communication between the operational environment itself without any routing provided by the TOE hardware device. These interfaces don't have any IP or MAC address.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.PHYSICAL PROTECTION	The TOE hardware device must be physically protected by its operational environment and not subject to physical attacks that could compromise its security or interfere with its proper operation.
A.TRUSTED ADMINISTRATION	Administrators are members of full confidence and ensure the best security interests of the organization. They must be properly trained and free of any malicious intent or conflict of interest in managing the TOE hardware device and the TOE mobile application.
A.UPDATES	TOE hardware device firmware/software is updated as updates are released to correct known vulnerabilities.
A.TRUSTED PLATFORM	The TOE mobile application component must run on a trusted platform, in this evaluation, on an Android operating system.
A.TRUSTED PLATFORM ADMINISTRATION	Platform operators must be fully trusted personal with the best security interests of the deployed TOE mobile application. They must be properly trained and free of any malicious intent or conflict of interest in the management of the device where the TOE mobile application is deployed.
A.TRUSTED PLATFORM OPERATOR	Operators with access to the mobile device operating system where the TOE mobile application runs must be members of the organization who are fully trusted and have the best interests for the organization. They must be properly trained and must be free of any malicious intent or conflict or interest in the management of the mobile operating system.
A.TRUSTED PAIRING	The communication that carries the pairing between the TOE hardware device and other operational mobile devices must be fully trusted, in order to avoid intrusions by not allowed third parties that vulnerate the secure exchange of information between the TOE hardware device and the mobile running the TOE mobile application.

4.2 Assets to protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.ADMINISTRATION	TOE's management local and remote interfaces and the information transmitted through them in both directions.	Confidentiality Authenticity Integrity
AS.PSS	Configuration data and audit records.	Integrity
AS.UPDATES	TOE's upgrades that may affect product configuration and functionality.	Integrity Authenticity
AS.COMMUNICATIONS	TOE's Bluetooth communications, established between the operational environment and the TOE hardware device.	Confidentiality Authenticity Integrity
AS.PSC	TOE's access PIN protected during transmission in the following scenarios: • Hashing the PIN and timestamp contained in the command generated to login into the TOE hardware device after the BT pairing. • Command generated for PIN change request, containing the new PIN, protected by the Bluetooth channel established in the TOE hardware device.	Confidentiality Integrity

4.3 Threat descriptions

Threat	Description	Assets
T.NOAUTH	An attacker can get unauthorized administration access by impersonating an administrator to the TOE, impersonating the product to an administrator, replaying an administration session, or performing man-in-the-middle attacks.	***AS.ADMINISTRATION*** ***AS.COMMUNICATIONS***
T.COM	Use of unauthorized protocols that allow an attacker to compromise the integrity and confidentiality of critical TOE communications.	***AS.COMMUNICATIONS***
T.ACT	An attacker can perform a malicious update that compromises product functionality.	***AS.UPDATES***
T.AUD	An attacker may attempt to modify the TOE's security functionalities without the administrator's knowledge.	***AS.PSS***
T.CRYPTO	Use of cryptographic mechanisms or weak key lengths in the TOE that allow an attacker to compromise it, primarily through brute force attacks.	***AS.COMMUNICATIONS*** ***AS.PSC***
T.FAILED	An attacker could gain access to an interface that is not enabled or not active due to a security flaw in the product and consequently gain access to unauthorized information.	***AS.ADMINISTRATION*** ***AS.COMMUNICATIONS*** ***AS.PSS*** ***AS.PSC***

4.3.1 Traceability threats/security requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.NOAUTH	T.COM	T.ACT	T.AUD	T.CRYPTO	T.FAILED
SF. AUDIT				X		
SF. ADMINISTRATION	X					X
SF. TRUSTED INSTALLATION AND UPDATES			X		X	
SF. CRYPTOGRAPHY		X	X		X	
SF. BLUETOOTH COMMUNICATION CHANNEL		X			X	
SF. TRUSTED FLOW CONTROL					X	X

5 Security Functional Requirements

The cryptographic algorithms listed in the subsections include the following nomenclature:

- Recommended (R): Refers to the cryptographic algorithms that are considered secure and suitable in the context of HIGH ENS category.
- Legacy (L): refers to the cryptographic algorithms, in the context of MEDIUM ENS category, that are considered with acceptable security in the short term, valid until 2025.

5.1 SF. Audit

Requirement	Description

AUD.1	The TOE hardware device shall generate the following audit records as defined below:
	
	• Changes in TOE configuration:
	  ○ TOE hardware device firmware updates.
	• Events related to TOE functionalities, such as:
	  ○ Enabling or disabling an interface.

AUD.2	Audit logs shall contain the following information: • Date and time of an event, through a timestamp. • Type of the event: firmware update or instruction executed. • Result of the event: installed version of the new firmware or modified configuration.
AUD.3	The following access policy shall be applied to audit logs: • Read: authorized users through the TOE mobile application. • Modify: no user. • Delete: no user.
AUD.4	The TOE hardware device shall be able to store the generated audit information in itself and transmit the generated audit information to the TOE Invishield mobile application through the Bluetooth communication channel.
AUD.5	The TOE hardware device shall overwrite the audit records according to the oldest criteria in the case that the storage for the records reaches its limit.

5.2 SF. Trusted Administration

Requirement	Description

ADM.2	The TOE shall be able to manage the following functionalities:
	
	• Local administration, through the TOE hardware device as follows:
	  ○ Enable or disable Bluetooth by pressing the RST button.
	  ○ Reset device settings by holding RST button for at least 10 seconds.
	• Remote administration, through commands generated by the TOE mobile application that allows the following:
	  ○ Create, edit and delete schedules.
	  ○ Create, edit and delete rules.
	  ○ Change the PIN.
	  ○ Perform date and time synchronization.

5.3 SF. Trusted Installation and Updates

Requirement	Description
ACT.1	The TOE mobile application shall provide the ability to query the following: • Current software version of the TOE mobile application. • Current firmware version of the TOE hardware device. and manually update the TOE hardware device firmware through the updated TOE mobile application.
ACT.2	The TOE hardware device shall authenticate the firmware update by verifying the ECDSA-256 digital signature.
ACT.4	The TOE mobile application shall be packaged in such way that, if uninstalled, it leaves no trace of its installation.
ACT.5	The TOE mobile application shall not download or modify its own binary code.

5.4 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall allow the use of cryptographic mechanisms authorized in accordance with the CCN-STIC-807 guide as follows: • ECDSA-256 (R) public-private model as defined in **ACT.2**. • SHA-256 (R) hashes of the PIN and timestamp as defined in **TFC.12**. • AES-128-CCM (R) encryption key used to encrypt and provide integrity to the data sent through the Bluetooth channel as defined in **BTH.2**. • ECDH-256 (R) key pair used in the Bluetooth pairing process as defined in **BTH.2**.

5.5 SF. Bluetooth Communication Channel

Requirement	Description
BTH.1	The TOE hardware device shall use Bluetooth Low Energy (BLE) v4.2 to provide a Bluetooth communication channel.
BTH.2	The TOE hardware device shall implement the Bluetooth communication channel, as defined in **BTH.1**, using the following cryptographic algorithms, accepted by the CCN-STIC-807 guide, based on security dimensions: • Confidentiality of transmitted data shall be provided by the encryption of data in transit, through the use of AES-128-CCM (R) algorithm. • Authenticity between paired devices shall be provided by the Secure Connection pairing phase, using the passkey method, including key exchange using ECDH (P-256) (R) algorithm. • Integrity of transmitted data shall be provided to the data exchanged between devices though the use of AES algorithm in CCM mode.
BTH.3	Commands shall only be sent to the TOE hardware device through the Bluetooth communication channel as defined in **BTH.2**.
BTH.4	The TOE hardware device shall not be managed from more than one paired device running the TOE mobile application once the Bluetooth connection has been established with the device running the TOE Mobile application.

5.6 SF. Trusted Flow Control

Requirement	Description
TFC.1	The TOE hardware device shall provide the ability to perform data flow control by enabling or disabling USB output interfaces as follows: • USBout1 enabled and USBout2 disabled • USBout2 enabled and USBout1 disabled • Both USB outputs disabled
TFC.2	The TOE hardware device shall provide the ability to perform data flow control by enabling or disabling ETH output interfaces as follows: • ETHout1 enabled and ETHout2 disabled • ETHout2 enabled and ETHout1 disabled • Both ETH outputs disabled • Both ETH outputs enabled
TFC.3	The TOE hardware device shall control data flows according to **TFC.1** and **TFC.2** requirements over time according to a pre-defined schedule.
TFC.4	Each TOE hardware device output interface shall have unique activation and deactivation assigned rules.
TFC.5	The TOE hardware device shall not allow the activation of USB output interfaces at the same time and, when this occurs, it shallperform the following: • On a scheduled-basis, the USBout1 shall have priority to be active. • In manual activation, the last activated USBout interface shall be active.
TFC.6	The TOE hardware device shall allow the configuration of the date and time for its correct operation from the TOE mobile application.
TFC.7	The TOE hardware device shall transmit the information to the output interfaces according to the pre-established schedules from the TOE mobile application.
TFC.8	The TOE hardware device shall ensure that no information is transmitted when the device is powered off.
TFC.9	The TOE hardware device shall ensure that its functionality cannot be modified through ports or interfaces other than those assigned to the Bluetooth communication channel.
TFC.10	The TOE hardware device shall ensure that the information transmitted between a specific input and output is not shared with another internal data stream or between the output interfaces.
TFC.11	The TOE hardware device shall not accept commands that are not verified with a valid PIN.
TFC.12	The TOE shall protect the PIN when it is transmitted as follows: • The TOE mobile application shall hash with SHA-256 (R) the PIN and the timestamp when generating the verification command. • The TOE hardware device shall protect the reception of the new PIN, in the change PIN command, using the protection of the Bluetooth communication channel defined in **BTH.2**.

	The TOE hardware device shall verify the PIN, contained in the verification command, by calculating the SHA-256 (R) hash of the stored PIN and timestamp of reception of the command.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
CNI	Centro Nacional de Inteligencia (Spanish National Intelligence Centre).
ENS	Esquema Nacional de Seguridad (National Security Scheme).
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
ST	Security Target – Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación (Security of Information and Communication Technologies).
TICs	Tecnologías de la Información y la Comunicación (Information and Communication Technologies).
TOE	Target Of Evaluation - Objeto a evaluar.
USB	Universal Serial Bus
MAC	Media Access Control
ETH	Ethernet
LED	Light Emitting Diode
BLE	Bluetooth Low Energy
SHA	Secure Hash Algorithm
NAS	Network Attached Storage
SSD	Solid-State Drive
RST	Reset
PDF	Portable Document Format

Table 3. Abbreviations

7 Document references

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Methodology for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2004	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Technical Report template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022 (National Security Scheme employment cryptology, May 2022).

Table 4. List of document references

8 Annex

8.1 Third party libraries used by the TOE

Library Name	Version	Vendor
esp-idf	4.2	Espressif Systems