High Sec Labs FA10A-4 and FA10AO-4

Firmware Version 40000-0E7

Peripheral Sharing Devices

Security Target

Doc No: 2149-001-D102A8
Version: 1.0
9 July 2024

High Sec Labs Ltd.
29 HaEshel St
Caesarea,
Israel 3079510

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria, Protection Profile (PP) and PP Modules.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

Section 9, References, provides a list of documents referenced in this ST.

Annex A, Letter of Volatility, provides volatility information and memory types for the High Sec Labs Peripheral Sharing Devices.

1.2 SECURITY TARGET REFERENCE

ST Title:	High Sec Labs FA10A-4 and FA10AO-4 Firmware Version 40000-0E7 Peripheral Sharing Devices Security Target
ST Version:	1.0

ST Date: 9 July 2024

1.3 TOE REFERENCE

TOE Identification: High Sec Labs FA10A-4 and FA10AO-4 Firmware Version 40000-0E7 Peripheral Sharing Devices

TOE Developer: High Sec Labs Ltd.

TOE Type: Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

The High Sec Labs (HSL) Audio Diodes ensure unidirectional audio between a connected computer and an analog audio output device.

The following security features are provided by the HSL Peripheral Sharing Devices:

- Audio Security
    - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- Hardware Anti-Tampering
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

The audio diodes are connected to a single computer and has only one peripheral output device, either speakers or headphones. The TOE device ensures that data only flows from the computer to the peripheral output device, and only analog audio data at the frequencies as described in the Protection Profile are allowed to pass.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Description
Connected Computer	1 general purpose computer
Audio output device	Analog audio output device (speakers or headphones)

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

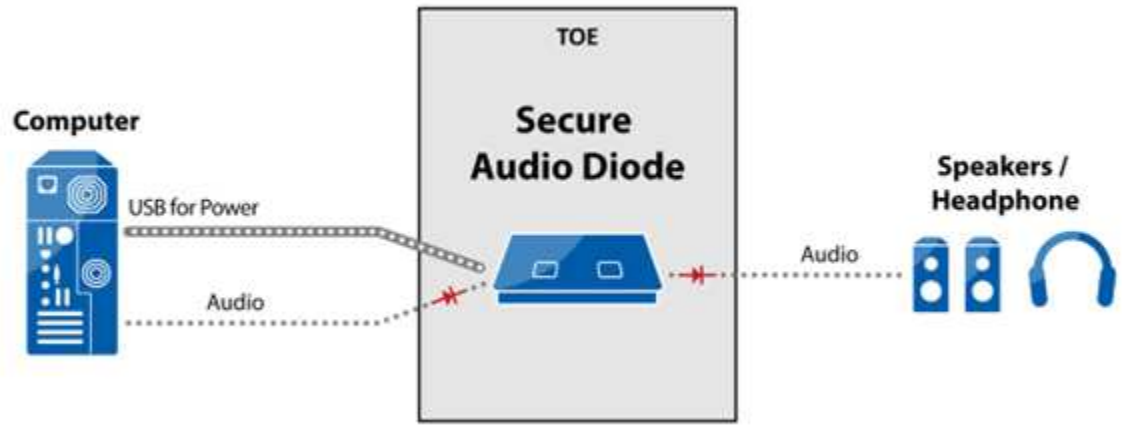

Figure 1 – Isolator Evaluated Configuration

In the evaluated configuration, the isolator is connected to the computer and to the analog audio output device to ensure unidirectional communications. The host (computer) interface is analog for the FA10A-4 and FA10AO-4. A Universal Serial Bus (USB) connection from the computer to the TOE provides power. The output interface to the speakers or headphones is analog.

1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2.

Family Description	Part Number	Model	Tamper Evident labels	Input Interface (host)	Output Interface (audio device)
Audio diode devices	CGA17129	FA10A-4	Yes	Analog	Analog
	CGA18094	FA10AO-4	Yes	Analog	Analog

Table 2 – TOE Peripheral Sharing Devices and Features

1.5.2.1 TOE Delivery

The TOE devices are delivered to the customer via a trusted carrier, such as Fed-Ex, that provides a tracking service for all shipments.

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- HSL Quick Start Guide Audio Diode, HDC19739 Rev 1.5

Guidance may be downloaded from the High Sec Labs website (https://highseclabs.com/quick-start-guides/) in .pdf format.

The following guidance is available upon request by emailing support@highseclabs.com:

- High Sec Labs FA10A-4 and FA10AO-4 Firmware Version 40000-0E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 0.3

1.5.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
User Data Protection	The TOE enforces unidirectional data flow for audio. The TOE ensures that only authorized peripheral devices may be used.
Protection of the TSF[1]	The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing. The TOE provides passive detection of physical attack.

Table 3 – Logical Scope of the TOE

[1] TOE Security Functionality

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PP-CONFIGURATION CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device and Analog Audio Output Devices, 29 May 2020 [CFG_PSD-AO_V1.0]

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD_V4.0]
- PP-Module: PP-Module for Analog Audio Output Devices, Version 1.0 [MOD_AO_V1.0]

2.3 TECHNICAL DECISIONS

The Technical Decisions in Table 4 apply to the PP and the modules and have been accounted for in the ST and in the evaluation.

TD	Name	PP affected	Relevant Y/N
TD0518	Typographical errors in dependency Table	[PP_PSD_V4.0]	Y
TD0557	Correction to Audio Filtration Specification table in	[MOD_AO_V1.0]	Y

	FDP_AFL_EXT.1		
TD0583	FPT_PHP.3 modified for remote controllers	[PP_PSD_V4.0]	Y
TD0585	Update to FDPAPC_EXT.1 Audio Output Tests	[MOD_AO_V1.0]	Y
TD0593	Equivalency Arguments for PSD	[MOD_AO_V1.0]	Y
TD0804	Clarification regarding Extenders in PSD Evaluations	[PP_PSD_V4.0]	Y
TD0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	[PP_PSD_V4.0]	Y

Table 4 – Applicable Technical Decisions

2.4 PACKAGE CLAIM

This Security Target claims conformance to the Assurance Package for Flaw Remediation V1.0.

2.5 CONFORMANCE RATIONALE

The TOE Audio Diode devices are inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP-Module for Analog Audio Output Devices, Version 1.0 [MOD_AO_V1.0], and with the PP-Configuration for Peripheral Sharing Device and Analog Audio Output Devices [CFG_PSD-AO_V1.0].

The security problem definition, statement of security objectives and statement of security requirements in this ST conform exactly to the security problem definition, statement of security objectives and statement of security requirements contained in [PP_PSD_V4.0] and the module listed in Section 2.2.

Although this ST claims conformance to the Assurance Package for Flaw Remediation V1.0, no SARs have been claimed.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats described in Section 3.1 of the [PP_PSD_V4.0]. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.DATA_LEAK	A connection via the PSD[2] between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T.UNINTENDED_USE	A PSD may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.
T.REPLACEMENT	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.

[2] Peripheral Sharing Device

Threat	Description
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.
T.MICROPHONE_USE	A malicious agent could use an unauthorized peripheral device such as a microphone, connected to the TOE audio out peripheral device interface to eavesdrop or transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	A malicious agent could repurpose an authorized audio output peripheral device by converting it to a low-gain microphone to eavesdrop on the surrounding audio or transfer data across an air-gap through audio signaling.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved. The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.
A.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
A.NO_WIRELESS_DEVICES	The environment includes no wireless peripheral devices.
A.TRUSTED_ADMIN	PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.

Assumptions	Description
A.USER_ALLOWED_ACCESS	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.
A.NO_MICROPHONES	Users are trained not to connect a microphone to the TOE audio output interface.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE, and traces each Security Functional Requirement (SFR) back to a security objective of the TOE.

Security Objective	Description
O.COMPUTER _INTERFACE _ISOLATION	The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED	The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
O.USER_DATA _ISOLATION	The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
O.NO_USER _DATA_RETENTION	The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset. Addressed by:

Security Objective	Description
	PP_PSD: FDP_RIP_EXT.1
O.NO_OTHER _EXTERNAL _INTERFACES	The PSD shall not have any external interfaces other than those implemented by the TSF. Addressed by: PP_PSD: FDP_PDC_EXT.1
O.LEAK _PREVENTION _SWITCHING	The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers. Addressed by: PP_PSD: FDP_SWI_EXT.1
O.AUTHORIZED _USAGE	The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as "hotkeys," automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended. A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated. Addressed by: PP_PSD: FDP_SWI_EXT.1

Security Objective	Description
O.PERIPHERAL _PORTS_ISOLATION	The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
O.REJECT _UNAUTHORIZED _PERIPHERAL	The PSD shall reject unauthorized peripheral device types and protocols. Addressed by: PP_PSD: FDP_PDC_EXT.1 MOD_AO: FDP_APC_EXT.1/AO, FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO, FDP_PUD_EXT.1
O.REJECT _UNAUTHORIZED _ENDPOINTS	The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub. Addressed by: PP_PSD: FDP_PDC_EXT.1
O.NO_TOE_ACCESS	The PSD firmware, software, and memory shall not be accessible via its external ports. Addressed by: PP_PSD: FPT_NTA_EXT.1
O.TAMPER _EVIDENT _LABEL	The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers. Addressed by: PP_PSD: FPT_PHP.1

Security Objective	Description
O.ANTI_TAMPERING	The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD. Addressed by: PP_PSD: FPT_PHP.1
O.SELF_TEST	The PSD shall perform self-tests following power up or powered reset. Addressed by: PP_PSD: FPT_TST.1
O.SELF_TEST _FAIL_TOE _DISABLE	The PSD shall enter a secure state upon detection of a critical failure. Addressed by: PP_PSD: FPT_FLS_EXT.1, FPT_TST_EXT.1
O.SELF_TEST _FAIL_INDICATION	The PSD shall provide clear and visible user indications in the case of a self-test failure. Addressed by: PP_PSD: FPT_TST_EXT.1
O.UNIDIRECTIONAL _AUDIO_OUT	The PSD shall enforce the unidirectional flow of audio data from the analog audio computer interface to the analog audio peripheral interface. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_AFL_EXT.1, FDP_UDF_EXT.1/AO
O.COMPUTER_TO _AUDIO_ISOLATION	The PSD shall isolate the analog audio output function from all other TOE functions. Addressed by: MOD_AO: FDP_APC_EXT.1/AO, FDP_UDF_EXT.1/AO

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.NO_TEMPEST	The operational environment will not use TEMPEST approved equipment.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.NO_WIRELESS_DEVICES	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.TRUSTED_ADMIN	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.
OE.NO_MICROPHONES	The operational environment is expected to ensure that microphones are not plugged into the TOE audio output interfaces.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The security objectives rationale describes how the assumptions and threats map to the security objectives.

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.

Threat or Assumption	Security Objective(s)	Rationale
	O.USER_DATA _ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL _PORTS _ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
T.SIGNAL_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling.
	O.LEAK_PREVENTION _SWITCHING	The TOE's use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.
	O.UNIDIRECTIONAL _AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low-gain dynamic microphones. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resultant audio stream. This prevents potential misuse of headphones connected to the TOE for audio eavesdropping.

Threat or Assumption	Security Objective(s)	Rationale
	O.COMPUTER_TO_AUDIO_ISOLATION	O.COMPUTER_TO_AUDIO_ISOLATION mitigates this threat by ensuring that analog audio output converted to input by a malicious driver cannot pick up signals from other computer interfaces. A TOE design that ensures that audio signals are not leaked to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through analog audio.
T.RESIDUAL_LEAK	O.NO_USER_DATA_RETENTION	The TOE's lack of data retention ensures that a residual data leak is not possible.
T.UNINTENDED_USE	O.AUTHORIZED_USAGE	The TOE's support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED_DEVICES	O.REJECT_UNAUTHORIZED_ENDPOINTS	The TOE's ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT_UNAUTHORIZED_PERIPHERAL	The TOE's ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
T.LOGICAL_TAMPER	O.NO_TOE_ACCESS	The TOE's prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
T.PHYSICAL_TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT_LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.

Threat or Assumption	Security Objective(s)	Rationale
T.REPLACEMENT	O.TAMPER_EVIDENT_LABEL	The TOE's use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.
T.FAILED	O.SELF_TEST	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality.
	O.SELF_TEST_FAIL_TOE_DISABLE	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL_INDICATION	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.
T.MICROPHONE_USE	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by attenuating the strength of any inbound transmission of audio data through the TOE from a connected peripheral. If the TOE design ensures that analog audio reverse signal attenuation is below the noise floor level then any audio signal should not have sufficient strength to be usable.
T.AUDIO_REVERSED	O.UNIDIRECTIONAL_AUDIO_OUT	O.UNIDIRECTIONAL_AUDIO_OUT mitigates this threat by ensuring that the TOE's audio peripheral interface(s) are exclusively used to output audio.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE's operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.
A.NO_PHYSICAL	OE.PHYSICAL	If the TOE's operational environment provides physical security, then the assumption is satisfied.

Threat or Assumption	Security Objective(s)	Rationale
A.NO_WIRELESS _DEVICES	OE.NO_WIRELESS _DEVICES	If the TOE's operational environment does not include wireless peripherals, then the assumption is satisfied.
A.TRUSTED_ADMIN	OE.TRUSTED _ADMIN	If the TOE's operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.TRUSTED _CONFIG	OE.TRUSTED _CONFIG	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A.USER_ALLOWED _ACCESS	OE.PHYSICAL	If the TOE's operational environment provides physical access to connected computers, then the assumption is satisfied.
A.NO_MICROPHONES	OE.NO_MICROPHONES	The assumption is upheld by the objective since the users in the environment are trained not to connect a microphone to the TOE audio output interface.

Table 9 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the module for analog audio output devices [MOD_AO_V1.0].

The families to which these components belong are identified in the following table:

Functional Class	Functional Families	Protection Profile Modules
User Data Protection (FDP)	FDP_AFL_EXT.1 Audio Filtration	[MOD_AO_V1.0]
	FDP_APC_EXT Active PSD Connections	[MOD_AO_V1.0]
	FDP_PDC_EXT Peripheral Device Connection	[PP_PSD_V4.0] [MOD_AO_V1.0]
	FDP_PUD_EXT Powering Unauthorized Devices	[MOD_AO_V1.0]
	FDP_RIP_EXT Residual Information Protection	[PP_PSD_V4.0]
	FDP_SWI_EXT PSD Switching	[PP_PSD_V4.0]
	FDP_UDF_EXT Unidirectional Data Flow	[MOD_AO_V1.0]
Protection of the TSF (FPT)	FPT_FLS_EXT Failure with Preservation of Secure State	[PP_PSD_V4.0]
	FPT_NTA_EXT No Access to TOE	[PP_PSD_V4.0]
	FPT_TST_EXT TSF Testing	[PP_PSD_V4.0]

Table 10 – Functional Families of Extended Components

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. This is defined in the PP as:

- Assignment: Indicated by surrounding brackets and underline, e.g., [assigned item].
- Selection: Indicated by surrounding brackets and italics, e.g., [*selected item*].
- Refinement: Refined components are identified by using **[bold surrounded by brackets]** for additional information, or ~~[strikeout surrounded by brackets]~~ for deleted text.
- Iteration: Iteration operations for iterations within the Protection Profile and associated modules are identified with a slash ('/') and an identifier (e.g. "/AO").

Extended SFRs are identified by the inclusion of "EXT" in the SFR name.

The CC operations already performed in the PP and PP modules are reproduced in plain text and not denoted in this ST. The requirements have been copied from the PP and PP modules and any remaining operations have been completed herein. Refer to the PP and PP modules to identify those operations.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components.

Class	Identifier	Name	Source
User Data Protection (FDP)	FDP_AFL_EXT.1	Audio Filtration	[MOD_AO_V1.0]
	FDP_APC_EXT.1/AO	Active PSD Connections	[MOD_AO_V1.0]
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_AO_V1.0][3]
	FDP_PDC_EXT.2/AO	Peripheral Device	[MOD_AO_V1.0]

[3] There is no modification to this SFR in the [MOD_AO_V1.0]. However, there are additions to the Peripheral Device Connections associated with this SFR and additional evaluation activities.

Class	Identifier	Name	Source
		Connection (Audio Output)	
	FDP_PUD_EXT.1	Powering Unauthorized Devices	[MOD_AO_V1.0]
	FDP_RIP_EXT.1	Residual Information Protection	[PP_PSD_V4.0]
	FDP_SWI_EXT.1	PSD Switching	[PP_PSD_V4.0]
	FDP_UDF_EXT.1/AO	Unidirectional Data Flow (Audio Output)	[MOD_AO_V1.0]
Protection of the TSF (FPT)	FPT_FLS_EXT.1	Failure with Preservation of Secure State	[PP_PSD_V4.0]
	FPT_NTA_EXT.1	No Access to TOE	[PP_PSD_V4.0]
	FPT_PHP.1	Passive Detection of Physical Attack	[PP_PSD_V4.0]
	FPT_TST.1	TSF testing	[PP_PSD_V4.0]
	FPT_TST_EXT.1	TSF Testing	[PP_PSD_V4.0]

Table 11 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_AFL_EXT.1 Audio Filtration

FDP_AFL_EXT.1.1 The TSF shall ensure outgoing audio signals are filtered as per Audio Filtration Specifications table.

Frequency (kHz)	Minimum Voltage (dB)	Maximum Voltage After Attenuation
14	23.9	127.65 mV
15	26.4	95.73 mV
16	30.8	57.68 mV
17	35.0	35.57 mV
18	38.8	22.96 mV

Frequency (kHz)	Minimum Voltage (dB)	Maximum Voltage After Attenuation
19	43.0	14.15 mV
20	46.0	10.02 mV
30	71.4	0.53 mV
40	71.4	0.53 mV
50	71.4	0.53 mV
60	71.4	0.53 mV

Table 12 – Audio Filtration Specifications

Application Note: TD0557 applies to this SFR definition.

6.2.1.2 FDP_APC_EXT.1/AO Active PSD Connections

FDP_APC_EXT.1.1/AO The TSF shall route user data only from the interfaces selected by the user.

FDP_APC_EXT.1.2/AO The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/AO The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/AO The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

6.2.1.3 FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

6.2.1.4 FDP_PDC_EXT.2/AO Peripheral Device Connection (Audio Output)

FDP_PDC_EXT.2.1/AO The TSF shall allow connections with authorized devices as defined in Appendix E **[of [MOD_AO_V1.0]]** and [*no other devices*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/AO The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E **[of [MOD_AO_V1.0]]** and [*no other devices*] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

6.2.1.5 FDP_PUD_EXT.1 Powering Unauthorized Devices

FDP_PUD_EXT.1.1 The TSF shall not provide power to any unauthorized device connected to the analog audio peripheral interface.

6.2.1.6 FDP_RIP_EXT.1 Residual Information Protection

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

6.2.1.7 FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [*the TOE supports only one connected computer*].

6.2.1.8 FDP_UDF_EXT.1/AO Unidirectional Data Flow (Audio Output)

FDP_UDF_EXT.1.1/AO The TSF shall ensure analog audio output data transits the TOE unidirectionally from the TOE analog audio output computer interface to the TOE analog audio output peripheral interface.

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

FPT_FLS_EXT.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*no other failures*].

6.2.2.2 FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE's external ports, with the following exceptions: [*no other exceptions*].

6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.2.4 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests during initial start-up and at the conditions *[no other conditions]* to demonstrate the correct operation of user control functions and *[no other functions]*.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [*TSF*].

6.2.2.5 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall respond to a self-test failure by providing users with a [*visual, auditory*] indication of failure and by shutdown of normal TSF functions.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 13.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives

Assurance Class	Assurance Components	
	Identifier	**Name**
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests (ATE)	ATE_IND.1	Independent Testing - Conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability Survey

Table 13 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

Table 7 provides a mapping between the SFRs and Security Objectives.

6.4.2 Dependency Rationale

Table 14 identifies the Security Functional Requirements and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Rationale Statement
FDP_AFL_EXT.1	FDP_PDC_EXT.1	Included
FDP_APC_EXT.1/AO	None	N/A
FDP_PDC_EXT.1	None	N/A
FDP_PDC_EXT.2/AO	FDP_PDC_EXT.1	Included
FDP_PUD_EXT.1	FDP_PDC_EXT.1	Included
FDP_RIP_EXT.1	None	N/A
FDP_SWI_EXT.1	None	N/A
FDP_UDF_EXT.1/AO	FDP_APC_EXT.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included only if anti-tamper is selected in FPT_FLS_EXT.1.1

SFR	Dependencies	Rationale Statement
FPT_NTA_EXT.1	None	N/A
FPT_PHP.1	None	N/A
FPT_TST.1	None	N/A
FPT_TST_EXT.1	FPT_TST.1	Included

Table 14 – Functional Requirement Dependencies

6.4.3 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements indicated in the [PP_PSD_V4.0].

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 USER DATA PROTECTION

7.1.1 PSD Switching

The TOE supports only one connected computer.

TOE Security Functional Requirements addressed: FDP_SWI_EXT.1.

7.1.1.1 Active PSD Connections

The TOE ensures that data flows only between the connected computer and the audio output peripheral. No data transits the TOE when the TOE is powered off, or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on.

TOE Security Functional Requirements addressed: FDP_APC_EXT.1/AO.

7.1.1.2 Residual Information Protection

The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

7.1.2 Audio Functionality

The TOE audio data flow path is electrically isolated from all other functions to prevent signaling data leakages to and from the audio paths.

Audio function is controlled by the system controller function through dedicated unidirectional command lines. Audio signals cannot be digitized or otherwise sampled by any TOE circuitry. Unidirectional flow data diodes prevent audio data flow from an audio device to a connected computer. The audio interface is electrically isolated from other interfaces, and from other TOE circuitry. These features ensure that the audio filtration specification requirements are met and that the audio signal is filtered according to the parameters set in Table 12.

The TOE does not supply power to the analog audio output interface, and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface.

When the TOE is powered off, an audio isolation relay is open, thereby isolating the audio input from the computer interface, and all other circuitry and interfaces. Following a failed self-test, the TOE will de-energize the audio isolation relay to isolate the audio inputs. The audio subsystem does not store, convert or delay audio data flows. Therefore, there is no risk of audio overflow.

The use of analog microphone or line-in audio devices is strictly prohibited as indicated in the user guidance. The TOE will reject a microphone through the following two methods:

- There is an analog audio data diode that forces data to flow only from a computer to an audio peripheral device
- There is a microphone Direct Current (DC) bias barrier that blocks an electret microphone DC bias if the TOE is deliberately or inadvertently connected to the microphone input jack of a connected computer

TOE Security Functional Requirements addressed: FDP_AFL_EXT.1, FDP_PUD_EXT.1, FDP_UDF_EXT.1/AO.

7.1.2.1 Audio Compatible Device Types

The TOE accepts analog headphones or analog speakers connected via a 1/8” (3.5mm) audio jack at the audio peripheral port. The TOE does not support a wireless connection to an audio output device and there are no additional external interfaces.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/AO.

7.2 PROTECTION OF THE TSF

7.2.1 No Access to TOE

The connected computer does not have access to TOE firmware or memory.

The TOE microcontrollers run from internal protected flash memory. Firmware cannot be updated from an external source. Firmware cannot be read or rewritten through the use of Joint Test Action Group (JTAG) tools. Firmware is executed on Static Random Access Memory (SRAM) with the appropriate protections to prevent external access and tampering of code or stacks.

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

7.2.2 Passive Anti-tampering Functionality

The TOE enclosure was designed specifically to prevent physical tampering. It features molded plastic parts connected by screws. Each device is fitted with a holographic Tampering Evident Label placed to cover both the top and bottom piece of the enclosure. If the label is removed, the word ‘VOID’ appears on both the label and the product surface.

TOE Security Functional Requirements addressed: FPT_PHP.1.

7.2.3 TSF Testing

The TOE performs a self-test at initial start-up. The self-test runs independently at each microcontroller and performs a verification check of the integrity of the microcontroller firmware.

If the self-test fails, the Light Emitting Diode (LED) on the front panel blinks to indicate the failure. The TOE remains in a disabled state until the self-test is rerun and passes.

TOE Security Functional Requirements addressed: FPT_FLS_EXT.1, FPT_TST.1, FPT_TST_EXT.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
AO	AO refers to the requirements for Analog Audio Output Devices.

Table 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
dB	decibel
DC	Direct Current
EEPROM	Electrically Erasable Programmable Read-Only Memory
HSL	High Sec Labs
IT	Information Technology
JTAG	Joint Test Action Group
kHz	kilohertz
LED	Light Emitting Diode
mV	millivolt
NIAP	National Information Assurance Partnership
OTP	One Time Programming
PP	Protection Profile
PSD	Peripheral Sharing Device
SFR	Security Functional Requirement
SRAM	Serial Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Acronym	Definition
USB	Universal Serial Bus

Table 16 – Acronyms

9 REFERENCES

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[PP_PSD_V4.0]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19
[MOD_AO_V1.0]	PP-Module for Analog Audio Output Devices, Version 1.0, 2019-07-19
[CFG_PSD-AO_V1.0]	PP-Configuration for Peripheral Sharing Device and Analog Audio Output Devices, 29 May 2020

Table 17 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the High Sec Labs Peripheral Sharing Devices. User data is not retained in any TOE device when the power is turned off.

Product Model	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
FA10A-4 FA10AO-4	1	System Controller, Host emulator: ST Microelectronics STM32F446ZCT	Embedded SRAM[1]	128KB	Connected computer	Volatile	May contain user data
			Embedded Flash[2]	256KB	Connected computer	Non-Volatile	No user data
			Embedded EEPROM[3]	4KB	Connected computer	Non-Volatile	No user data
			OTP Memory	512bytes	Connected computer	Non-Volatile	No user data

Notes:

[1] SRAM stores USB Host stack parameters and up to the last 4 key-codes. Data is erased during power off of the device. Device emulators receive power from the connected computer and therefore devices are powered on as long as the associated computer is powered on and connected.

[2] Flash storage is used to store firmware code. It contains no user data. Flash storage is permanently locked by fuses after initial programming to prevent rewriting. It is an integral part of the ST Microcontroller together with SRAM and EEPROM.

[3] EEPROM is used to store operational parameters and contains no user data.