Swedish Certification Body for IT Security

Certification Report - IHSE Secure Isolator Devices Firmware Version 44404-E7E7

Issue: 1.0, 2023-aug-14

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is IHSE Secure Isolator Devices Firmware Version 44404-E7E7, including eight models:

Model	Description
K487-1PHCA-N	Copper HD KVMA Isolated Secure Extender
K487-1PHSA-N	Fiber HD KVMA Isolated Secure Extender
K487-1PHCRA-N	Copper HD KVMA Isolated Redundant Secure Extender
K487-1PHSRA-N	Fiber HD KVMA Isolated Redundant Secure Extender
K497-1PHCA-N	Copper UHD KVMA Isolated Secure Extender
K497-1PHSA-N	Fiber UHD KVMA Isolated Secure Extender
K497-1PHCRA-N	Copper UHD KVMA Isolated Redundant Secure Extender
K497-1PHSRA-N	Fiber UHD KVMA Isolated Redundant Secure Extender

The TOE ensure unidirectional flow of data between peripheral devices and a secure connected computer.

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

The ST does not make conformance claims to any protection profile.

There are four assumptions being made in the Security Target (ST) regarding the TOE. The TOE relies on these to counter the five threats. The assumptions and the threats are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB in Växjö, Sweden (critical locations), and by Intertek/EWA-Canada in Ottawa, Canada (foreign location).

The evaluation was completed on 2023-07-21. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Tar-get (ST) and the Common Methodology for evaluation assurance level:

EAL4 + ALC_FLR.3.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2020020
Name and version of the certified IT product	IHSE Secure Isolator Devices Firmware Version 44404-E7E7
Security Target Identification	IHSE Secure Isolator Devices Firmware Version 44404-E7E7 Security Target, 2021-10-06, document version 0.5
EAL	EAL4 + ALC_FLR.3
Sponsor	IHSE GmbH,
Developer	IHSE GmbH,
ITSEF	Combitech AB and EWA Canada Ltd
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.4
Scheme Notes Release	20.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2023-08-14

3 Security Policy

- User Data Protection
- Security Management
- Protection of the TSF1

3.1 User Data Protection

The TOE enforces unidirectional data flow for keyboard and mouse, display, and audio output. The TOE ensures that only authorized peripheral devices may be used.

3.2 Security Managemrent

The TOE ensures that no user is able to modify the security attributes used to determine authorized peripheral devices and to provide data isolation between connected computers.

3.3 Protection of the TSF1

The TOE provides passive detection of physical attack and performs self-testing.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes four assumptions on the TOE.

A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data that passes through the TOE, is assumed to be provided by the environment for the TOE, the peripheral devices and all cabling.

A.TRUSTED_CONFIG

Personnel installing and configuring the TOE and its operational environment will follow the applicable guidance.

A.TRUSTED_USER

TOE users are trusted to follow and apply all guidance and security procedures in a reliable manner.

A.USER_IDENT

The operational environment is responsible for the identification and authentication of users. This determines physical access to the TOE, and access to the connected computers and their applications and resources.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.

T.DATA_LEAK

An unauthorized user may be able to access data that is transmitted via an unauthorized data transfer through the TOE or its connected peripherals.

T.DATA_PATH

A poorly designed TOE could result in a situation where a user is connected to a computer function other than the one to which the user intended to connect, resulting in an unintended flow of data.

T.PHYSICAL_TAMPER

A malicious user could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.

T.UNAUTH

A malicious user could tamper with the security attributes that determine allowed peripheral devices and allowed data flows, resulting in the use of unauthorized peripheral devices that may allow unauthorized data flows between connected devices, or an attack on the TOE or its connected computers.

T.UNAUTH_DEVICE

A malicious user could connect an unauthorized peripheral device to the TOE, and that device could cause information to flow between connected devices in an unauthorized manner, or could enable an attack on the TOE or its connected computers.

There are no Organizational Security Policies (OSPs) applicable to this TOE.

5 Architectural Information

The TOE is a combined software and hardware TOE.

The TOE devices use isolated microcontrollers to emulate connected peripherals in order to prevent display signaling, keyboard signaling, and power signaling attacks.

Figure 1 showing the TOE keyboard and mouse data path. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user key strokes into unidirectional serial data. An isolated Device Emulator (DE) is connected to the data switch on one side and to the computer on the other side. Each key stroke is converted by the selected DE into a bi-directional stream to communicate with the computer.

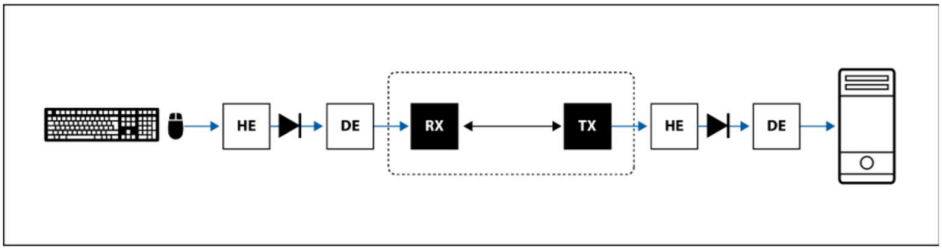

Figure 1: TOE Configuration

The TOE Security Functional Interfaces (TSFIs) and subsystems that support the TOE Security Functional Requirements (SFRs) are shown in Figure 2:

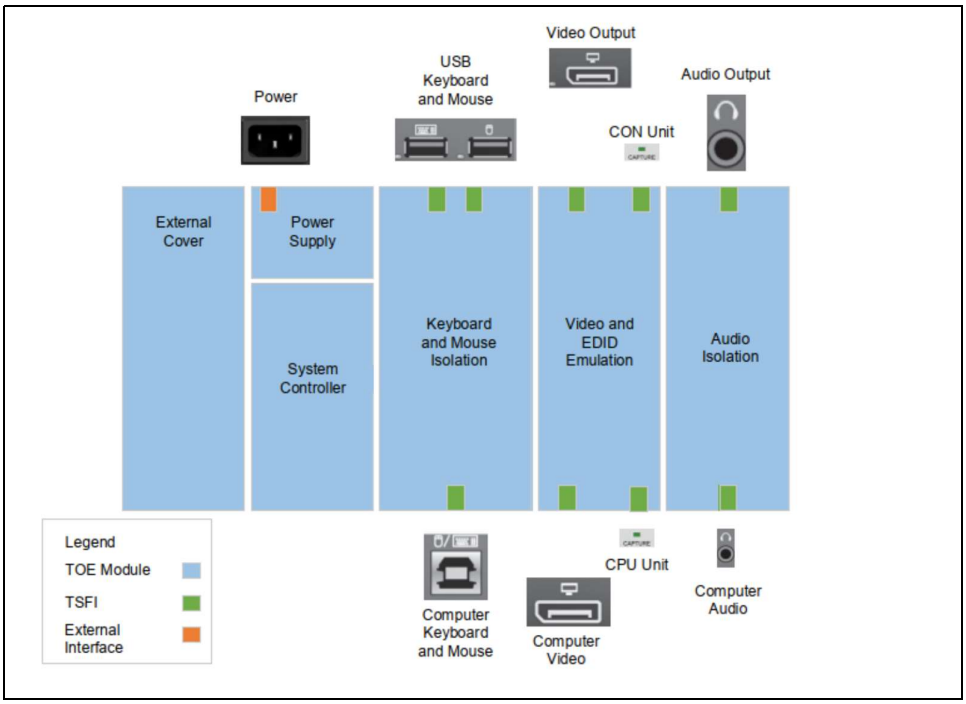

Figure 2: TOE Diagram

The following security features are provided by the IHSE Isolator devices:

- Video Security
  - The display is isolated through a dedicated, read-only, Extended Display Identification Data (EDID) emulation function
  - Access to the monitor's EDID is blocked

  - Access to the Monitor Control Command Set (MCCS commands) is blocked
  - DisplayPort and High-Definition Multimedia Interface (HDMI) video options are supported
- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (USB) device emulation
  - One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
  - Communication from computer-to-keyboard/mouse is blocked
  - Non HID (Human Interface Device) data transactions are blocked
- 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
- Self Test
  - The microcontroller firmware is subject to self test following power up.

6 Documentation

The TOE includes the following guidance documentation:

- QUICK SETUP Draco vario Secure Extender K487-1PHCA-N, K487-1PHCRA-N, K487-1PHSA-N, K487-1PHSRA-N Document no.: q487_0001 Rev.: 0001
- QUICK SETUP Draco vario Secure Extender K497-1PHCA-N, K497-1PHCRA-N, K497-1PHSA-N, K497-1PHSRA-N Document no.: q497_0001 Rev.:0001

Guidance may be downloaded from the IHSE website (www.ihse.com) in .pdf format.

7 IT Product Testing

7.1 Developer Testing

The developer's testing covers the security functional behaviour of all TSFIs and SFRs as well as the interactions of the modules. All the SFR enforcing modules are mapped to test cases. Subsystems are not applicable for the TOE.

All tests are performed manually and are well described and sequenced in at number of steps.

The result for all test cases for all the eight models are Pass. All test cases are executed for all the TOE models.

All developer tests result in a Pass.

7.2 Evaluator Testing

The tests specified are divided into three test groups depending on the behaviour to be tested:

- Test Group 1: TOE Installation
- Test Group 2: Repetitions of a chosen subset of developer tests
- Test Group 3: Tests that complements the vulnerability assessment

The used test installation and configuration with the following limitations:

- No oscilloscope
- Operating systems is only Windows 10
- Number of TOE models

The evaluator repeat almost all the developers test cases for two models. The following two models were used for the independent testing:

- K487-1PHCRA-N (HD, Copper, Redundant)
- K497-1PHSRA-N (UHD, Fiber, Redundant)

By testing these two models are the main differences for the hardware tested; copper vs fiber and HD vs Ultra HD.

This evaluator sample of test cases covers all the TSFIs, subsystems and almost all of the TSFs and SFRs.

No differences for the actual results were identified between the developer's tests and the evaluators tests. All tests result in a pass.

7.3 Penetration Testing

Penetration testing was built on the evaluation of the vulnerability assessment activities.

One vulnerability is identified to be tested: "Bad quality of tamper protection/detection".

The same type of tamper label is used for all models of the TOE as for the Vertiv KVM/KM/KVM Matrix devices. The test was not repeated for the IHSE devices. The test result for the Vertiv device KVM Matrix of model Vertiv SCM145DPH applies also for the IHSE devices.

The test passed. The vulnerability is judged as not exploitable.

8 Evaluated Configuration

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

Component	Description
Connected Computer	General purpose computer
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
Audio output device	Analog audio output device (speakers or headphones)
User display	Standard computer display (HDMI 2.0, or DisplayPort 1.1, 1.2 or 1.3)
IHSE Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort, or HDMI) 3.5mm stereo cable (Audio cable)

8.1 Excluded from the TOE Evaluated Configuration

No features were excluded from the evaluation configuration of the TOE.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of enhanced-basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance	Class/Family	Short name	Verdict
Development		ADV	PASS
	Security architecture description	ADV_ARC.1	PASS
	Complete functional specification	ADV_FSP.4	PASS
	Implementation representation of the TSF	ADV_IMP.1	PASS
	Basic modular design	ADV_TDS.3	PASS
Guidance documents		AGD	PASS
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
Life-cycle support		ALC	PASS
	Production support, acceptance procedures and automation	ALC_CMC.4	PASS
	Problem tracking CM coverage	ALC_CMS.4	PASS
	Delivery procedures	ALC_DEL.1	PASS
	Identification of security measures	ALC_DVS.1	PASS
	Developer defined life-cycle model	ALC_LCD.1	PASS
	Well-defined development tools	ALC_TAT.1	PASS
	Systematic flaw remediation	ALC_FLR.3	PASS
Security Target evaluation		ASE	PASS
	Conformance claims	ASE_CCL.1	PASS
	Extended components definition	ASE_ECD.1	PASS
	ST introduction	ASE_INT.1	PASS
	Security objectives	ASE_OBJ.2	PASS
	Derived security requirements	ASE_REQ.2	PASS
	Security problem definition	ASE_SPD.1	PASS
	TOE summary specification	ASE_TSS.1	PASS
Tests		ATE	PASS
	Analysis of coverage	ATE_COV.2	PASS
	Testing: basic design	ATE_DPT.1	PASS
	Functional testing	ATE_FUN.1	PASS
	Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment		AVA	PASS
	Focused vulnerability analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

11 Bibliography

ST — IHSE Secure Isolator Devices Firmware Version 44404-E7E7 Security Target, 2021-10-06, document version 0.5

CCguide — IHSE Secure Isolator Devices Common Criteria Guidance Supplement Evaluation Assurance Level (EAL): EAL4+ , 2021-02-12, document version 0.2

QS_1 — QUICK SETUP, Draco vario Secure Extender K487-1PHCA-N, K487-1PHCRA-N, K487-1PHSA-N, K487-1PHSRA-N

QS_2 — QUICK SETUP Draco vario ultra Secure Extender K497-1PHCA-N, K497-1PHCRA-N, K497-1PHSA-N, K497-1PHSRA-N

CCpart1 — Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 — Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 — Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC — CCpart1 + CCpart2 + CCpart3

CEM — Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

EP-002 — EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34

Appendix A Scheme Versions

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application.

QMS 1.23.2	valid from 2020-05-11
QMS 1.24	valid from 2020-11-19
QMS 1.24.1	valid from 2020-12-03
QMS 1.25	valid from 2021-06-17
QMS 2.0	valid from 2021-11-24
QMS 2.1	valid from 2022-01-18
QMS 2.1.1	valid from 2022-03-09
QMS 2.2	valid from 2022-06-27
QMS 2.3	valid from 2023-01-26
QMS 2.3.1	valid from 2023-04-20
QMS 2.4	valid from 2023-06-15

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 2.4”.

The certifier concluded that, from QMS 1.23.2 to the current QMS 2.4, there are no changes with impact on the result of the certification.

A.1 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for aplication, evaluation ad certification
- Scheme Note 31 - New procedures for site visit oversight and testing oversight