Swedish Certification Body for IT Security

Certification Report MilDef KSW5101 PSD

Issue: 1.0, 2025-nov-05

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device.

The TOE allows users to securely share keyboard, video, mouse peripherals, and Universal Serial Bus (USB) authentication device peripherals between up to 4 connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

The TOE consists of:

- Ruggedized Secure KVM Switch, Model KSW5101, Firmware version 4444-M1D1
- Remote Control, Model KSW4202

and the following guidance:

- MilDef Quick Installation Guide KSW5101 4 Ports Secure Ruggedized HDMI KVM Switch, HLT32537 Rev 1.3, 2024-08-29
- MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Common Criteria Guidance Supplement, Version 1.2, 2025-07-02

The TOE is the complete product. No part of the product has been excluded from the scope.

TOE physical devices, together with its corresponding cables are delivered to the customer via trusted carrier. The TOE guidance MilDef Quick Installation Guide KSW5101 4 Ports Secure Ruggedized HDMI KVM Switch, HLT32537 Rev 1.3, 2024-08-29 can be downloaded from MilDefs website (https://download.mildef.com/se) and MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Common Criteria Guidance Supplement, Version 1.2 can be requested by sending an e-mail to service@mildef.com.

ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 2019-07-19 [CFG_PSD-KM-UA-VI].

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD]
- PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0 [MOD_KM]
- PP-Module: PP-Module for Video/Display Devices, Version 1.0 [MOD_VI]
- PP-Module: PP-Module for User Authentication Devices, Version 1.0 [MOD_UA]

There are seven assumptions made in the ST regarding the secure usage and environment of MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device. The TOE relies on these being met to counter the nine threats. No organizational security policies are specified in the ST. The assumptions and threats are described in ST 3 Security Problem Definition.

The evaluation has been performed by Intertek in their premises in Kista, Sweden. The evaluation was completed on 2025-09-22. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release 5.

Intertek is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Intertek is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive version of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 1 + ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, in accordance with the evaluation activities implied by the Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD], PP-Module for Keyboard/Mouse Devices Version 1.0 [MOD_KM], PP-Module for Video/Display Devices Version 1.0 [MOD_VI], PP-Module for User Authentication Devices Version 1.0 [MOD_UA].

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Intertek.

2 Identification

Certification Identification	
Certification ID	CSEC2024003
Name and version of the certified IT product	MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device
Security Target Identification	MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Security Target, 02 September 2025, version 1.4
Protection Profile Configuration	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, Version 1.0.
Protection Profile	Protection Profile for Peripheral Sharing Device, Version 4.0, PP-Module for Keyboard/Mouse Devices, Version 1.0, PP-Module for Video/Display Devices, Version 1.0 PP-Module for User Authentication Devices, Version 1.0
EAL	EAL 1+ ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, in accordance with Protection Profile and PP-Modules
Sponsor	MilDef Group AB
Developer	MilDef Group AB
ITSEF	Intertek
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2025-11-05

3 Security Policy

The TOE allows users to securely share keyboard, video, mouse peripherals, and Universal Serial Bus (USB) authentication device peripherals between up to 4 connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

The following security features are provided by the MilDef Peripheral Sharing Device:

- Video Security
- Keyboard and Mouse Security
- Authentication Device
- Anti-Tampering
- TOE Access

3.1 Video Security

- Computer video input interfaces are isolated through the use of separate electronic components, power and ground domains
- The display is isolated by dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
- Access to the monitor's EDID is blocked
- EDID file is transferred to connected hosts via a secure mechanism to assure unidirectional information flow.
- Access to the Monitor Control Command Set (MCCS commands) is blocked
- Only HDMI Interfaces are supported.
- Bi-directional interfaces of HDMI, for example, HEC, ARC, CEC and more are not connected.

3.2 Keyboard and Mouse Security

- Keyboard and mouse are isolated by dedicated, USB device emulation for each computer.
- 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.

3.3 Authentication Device

- Unauthorized USB devices are blocked
- USB authentication devices are authorized by default; all other devices are blocked
- Anti-Tampering
- The TOE provides passive detection of physical attack. Tamper evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

3.4 TOE Access

- The TOE provides continuous indication of which computer is currently selected.

3.5 Assumptions

The Security Target [ST] makes seven assumptions on the usage of the TOE:

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.

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_SPECIAL_ANALOG _CAPABILITIES

The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

3.6 Clarification of Scope

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

T.DATA_LEAK

A connection via the PSD2 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.

T.FAILED

Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

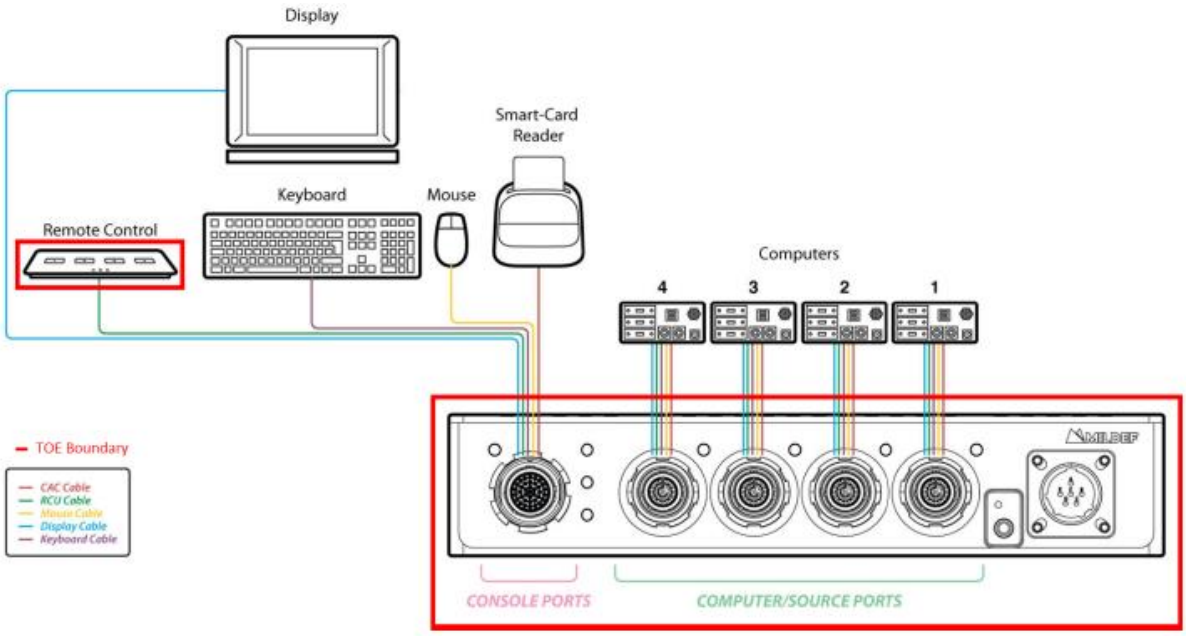
The Security Target contains no Organisational Security Policies (OSPs), which have been considered during the evaluation.

4 Architectural Information

The TOE is the MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device which consists of the MilDef Firmware version 4444-M1D1, including remote control.

Family Description	Part Number	Model
Ruggedized Secure KVM Switch	211-4403	KSW5101
Remote Control	CGA32549	KSW4202

The figure below shows a basic evaluated configuration. In the evaluated configuration, the TOE is connected to a keyboard, a mouse, and up to four computers. The video input is HDMI and a single display is connected. The TOE uses all metallic, ruggedized pin connectors (MIL-SDT-38999) that support both HDMI and USB 2.0 protocols. The KVM is used with a wired remote control.



The TOE provides the following TOE security functions:

- User Data Protection
- Protection of the TSF
- TOE Access

The TOE does not provide a management function to configure aspects of the TSF.

4.1 User Data Protection

Each device includes a System Controller which is responsible for device management, user interaction, system control security functions, and device monitoring. It receives user input from the switches on the front panel or remote control, and drives the TOE channel select lines that control switching circuits within the TOE.

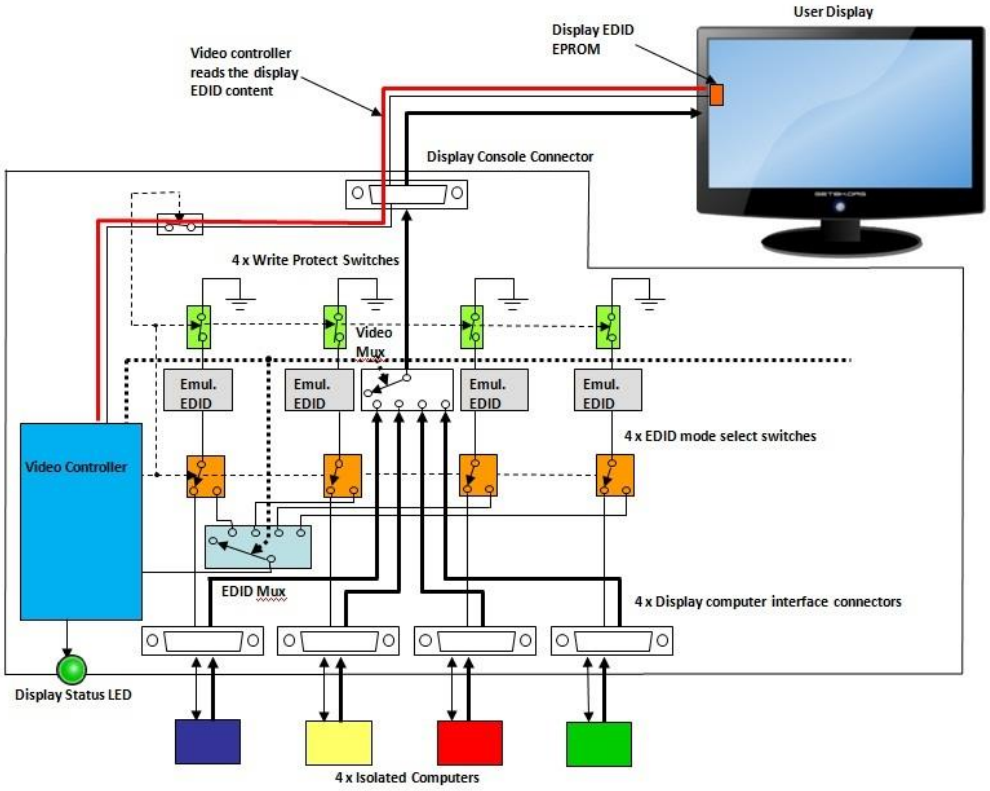
The System Controller includes a microcontroller with internal non-volatile, Read Only Memory (ROM). The controller function manages the TOE functionality through a pre-programmed state machine loaded on the ROM as read-only firmware during product manufacturing.

Following boot up of the TOE, the channel select lines are set to Channel 1 by default. The channel select lines are also used to link the System Controller channel select commands to the Field Programmable Gate Array (FPGA) that supports video processing.

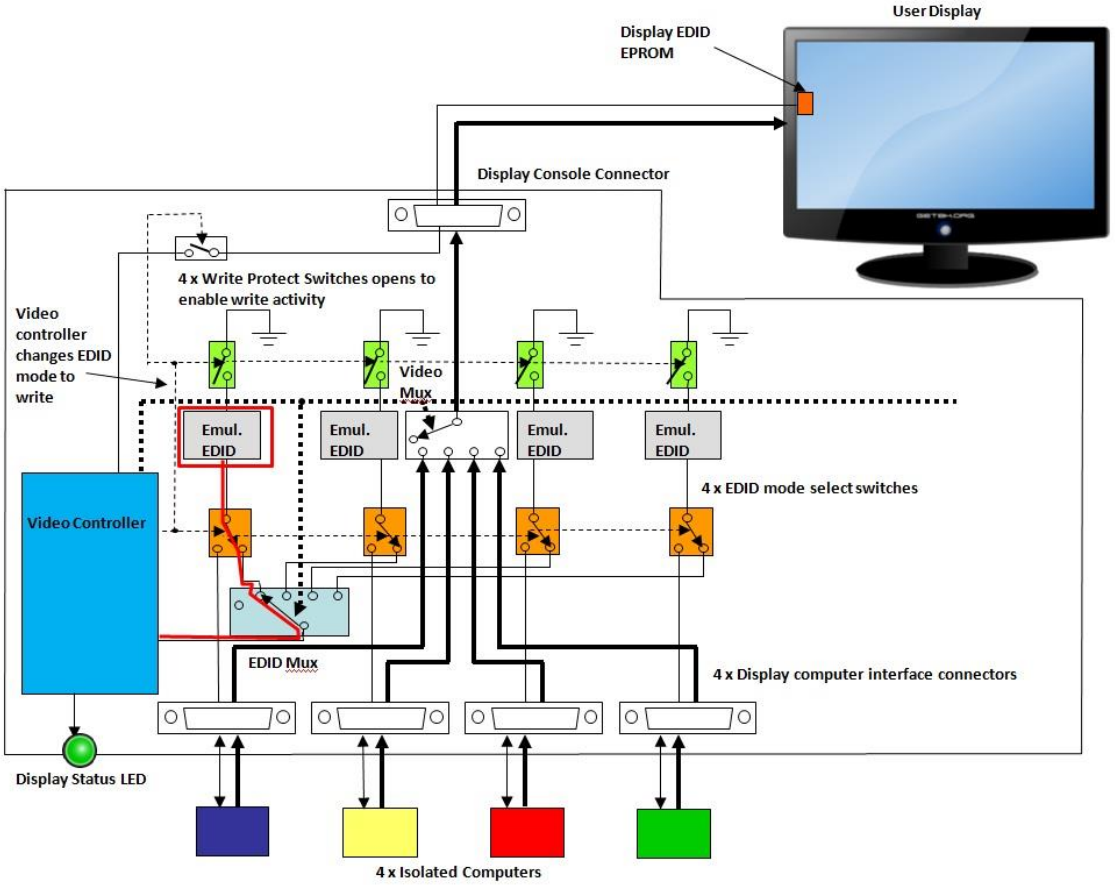
The user determines the host computer to be connected to the peripherals by pressing a button on the TOE front panel or on the wired remote control device. The front panel button of the selected computer is illuminated. Switching can only be initiated through express user action and not through automated port scanning, connected computer control, or keyboard shortcuts.

The TOE ensures that data flows only between the peripherals and the connected computer selected by the user. The TOE ensures that no electrical signal flows between the connected computers selected by the user. No data or electrical signal 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.

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow paths. The figure below shows a data flow during the display EDID read function

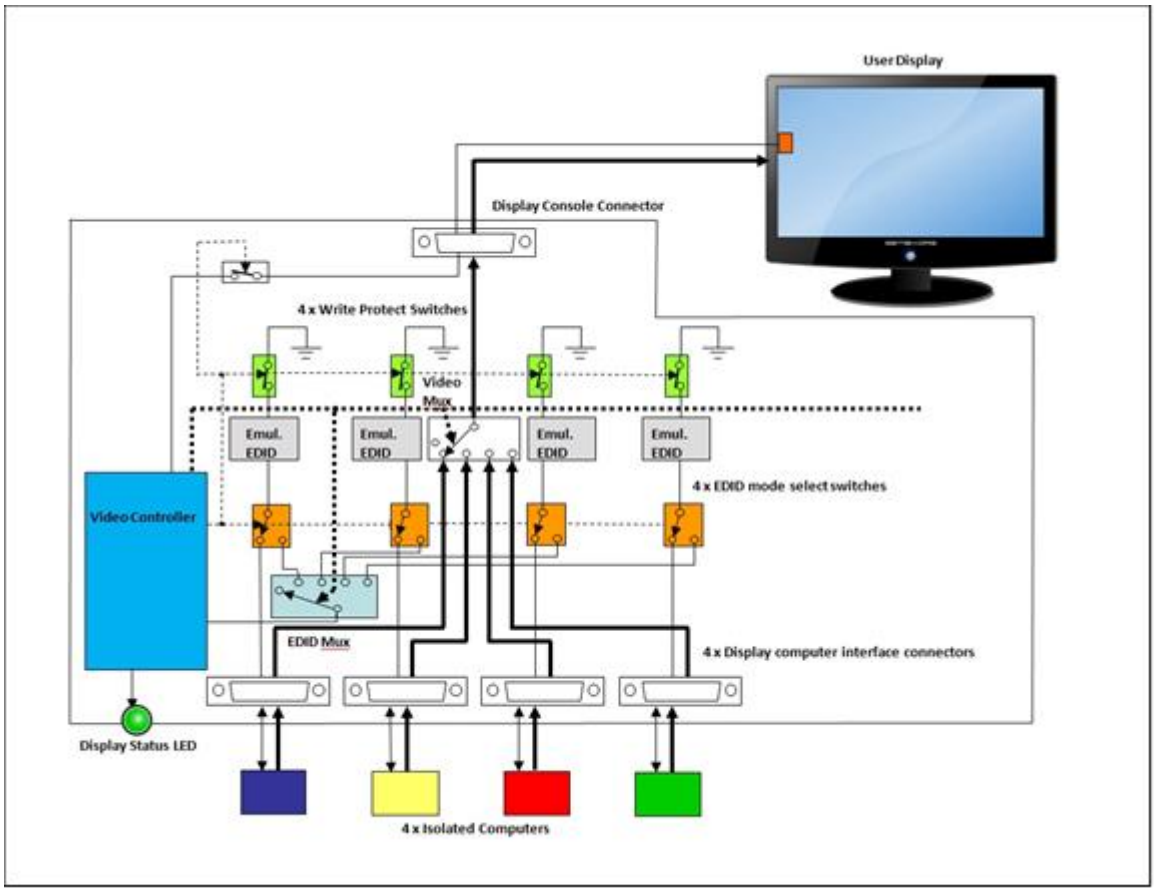


The next figure illustrates the video controller as it writes the EDID content into the first channel emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) chip (shown in gray).



The chip write protect switch opens to enable writing. The video controller uses the I2C lines to write to the first emulated EDID EEPROM chip. Once the write operation is complete and verified, the video controller switches the EDID multiplexer to the next channel and the operation repeats until all chips are programmed. Once the write operation is complete, the video controller switches to normal operating mode, which is demonstrated in the figure below.

In EDID write mode, the Emulated EDID EEPROM chips are switched to their respective computers to enable reading of the EDID information. The write protect switches are switched back to protected mode to prevent any attempt to write to the EEPROM or to transmit MCCS commands.



In normal mode, each computer interface operates independently. The power to each emulated EDID EEPROM is received from its respective computer through the video cable. The main video multiplexer is switched to the user selected computer to enable the proper video display.

During TOE normal operation, any attempt by a connected computer to affect the EDID channel is blocked by the architecture. Each computer is only able to affect its own emulated EDID EEPROM.

The TOE supports the use of an external user authentication device with a feature called Freeze USB (fUSB). The TOE does not support internal user authentication devices. By default, only standard USB smart-card readers or biometric authentication devices with USB smart-card class interfaces that comply with the USB Organization standard Chip Card Interface Device (CCID) Revision 1.1 or CCID Revision 1.0 will be accepted by the TOE on the fUSB port.

4.2 Protection of the TSF

Connected computers do not have access to TOE firmware or memory, with the following exceptions:

- EDID data is accessible to connected computers from the TOE

All the TOE microcontrollers run from internal protected flash memory. Firmware cannot be updated from an external source.

The TOE provides passive anti-tampering functionality. The TOE enclosure was designed specifically to prevent physical tampering. It features a stainless-steel welded chassis and panels that prevent external access through bending or brute force.

Additionally, the KVM switch fitted with Tampering Evident Labels placed at critical locations on the TOE enclosure. The remote control also has a Tampering Evident Label placed at a critical location.

The TOE performs a self-test at initial start-up. The self-test runs independently at each microcontroller. If the self-test fails, the LEDs on the front panel blink and the device makes a clicking sound to indicate the failure.

4.3 TOE Access

The TOE user switches between computers by pressing the corresponding front panel button on the device, or on the remote control. The front panel button of the KVM or the remote control button corresponding to the selected computer will illuminate. When the button to switch computers is pressed, a signal is sent and the TOE peripheral sharing device switches to the indicated channel.

5 Documentation

The TOE includes the following guidance documentation:

- MilDef Quick Installation Guide KSW5101 4 Ports Secure Ruggedized HDMI KVM Switch, HLT32537 Rev 1.3, 2024-08-29
- MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Common Criteria Guidance Supplement, Version 1.2, 2025-07-02

The MilDef Quick Installation Guide can be downloaded on the MilDef website: https://download.mildef.com/se, and MilDef KSW5101 Common Criteria Guidance Supplement is made available upon request by emailing service@mildef.com.

6 IT Product Testing

6.1 Developer Testing

No developer testing was claimed in this certification.

6.2 Evaluator Testing

The evaluator performed the installation and configuration of the TOE into the evaluated configuration. All mandatory test cases specified in the following PP and modules have been performed:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD_V4.0]
- PP-Module: PP-Module for Keyboard/Mouse Devices, Version 1.0 [MOD_KM_V1.0]
- PP-Module: PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_V1.0]
- PP-Module: PP-Module for User Authentication Devices, Version 1.0 [MOD_UA_V1.0]

In total 33 tests were performed by the evaluator and the evaluator determined that no additional tests were deemed necessary.

6.3 Penetration Testing

Negative tests were performed as part of functional testing mandated by PP and modules. No vulnerability scan was performed since TOE lacks network interface. The public vulnerability search resulted in no findings. Therefore, no additional penetration test was performed.

7 Evaluated Configuration

The TOE shall be installed and configured in accordance with the TOE guidance listed in this document, chapter 5.

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

Component	Description
Connected Computers	1-4 General purpose computers
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
User authentication device	Standard USB smartcard reader/authentication device
User display	Standard computer display (HDMI 2.0)
KVM Cables	Ruggedized 37 pin console cable. The console cable has a round 37 pin connector on the KVM side. On the peripheral side, there is an HDMI video connector, three USB 2.0 connectors for the keyboard, mouse and CAC reader and a port for connecting the KSW4202 remote control. Ruggedized 26 pin PC cables. The PC cables have a single round 26 pin connector on the KVM side. On the PC side, there is an HDMI video connector and two USB 2.0 connectors for the keyboard and mouse and a second cable for CAC.
Power Supply	28 Volt Direct Current (VDC) Power Supply.

Computers and peripheral devices connected to the TOE shall not be TEMPEST approved.

8 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 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 Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Functional Specification	ADV_FSP.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-Cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.1	PASS
CM Scope	ALC_CMS.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Component Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ,2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing	ATE IND.1	PASS
Vulnerability Analysis	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS

9 Evaluator Comments and Recommendations

None.

10 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within an evaluation and certification scheme
I2C	Inter-Integrated Circuit
KVM	Keyboard, Video, Mouse
MCCS	Monitor Control Command Set
PP	Protection Profile
PSD	Peripheral Sharing Device
ROM	Read Only Memory
ST	Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation
TOE	Target of Evaluation
USB	Universal Serial Bus

11 Bibliography

ST	MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Security Target, MilDef Group AB, 2025-09-02, document version 1.4, 24FMV2376-55
QIG	MilDef Quick Installation Guide KSW5101 4 Ports Secure Ruggedized HDMI KVM Switch, HLT32537 Rev 1.3, 2024-08-29
CCGS	MilDef KSW5101 Firmware Version 4444-M1D1 Peripheral Sharing Device Common Criteria Guidance Supplement, Version 1.2, 2025-07-02
PP_PSD	Protection Profile for Peripheral Sharing Device, 2019-07-19, version 4.0
MOD_KM	PP-Module for Keyboard/Mouse Devices, 2019-07-19, version 1.0
MOD_KM-SD	Supporting Document Mandatory Technical Document PP-Module for Keyboard/Mouse Devices. 2019-07-19, version 1.0
MOD_UA	PP-Module for User Authentication Devices. 2019-07-19, version 1.0
MOD_UA-SD	Supporting Document Mandatory Technical Document PP-Module for User Authentication Devices. 2019-07-19, version 1.0
MOD_VI	PP-Module for Video/Display Devices. 2019-07-19, version 1.0
MOD_VI-SD	Supporting Document Mandatory Technical Document PP-Module for Video/Display Devices. 2019-07-19, version 1.0
CFG_PSD-KM-UA-VI	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices. 2019-07-19, version 1.0
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-

	2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003
CC	CCpart1 + CCPart2 + CCPart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004
EP-002	EP-002 Evaluation and Certification, CSEC, 2025-03-25, document version 36.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.6.1	2025-10-16	*None.*
2.6	2025-04-23	*None.*
2.5.2	2024-06-14	*None.*
2.5.1	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on ST	Compliant
SN-21	3.0	NIAP-Approved PP Certifications	Compliant
SN-22	4.0	Vulnerability Assessment	Compliant
SN-23	1.0	Evaluation reports for NIAP PPs and cPPs	Compliant
SN-27	1.0	ST requirements at the time of application	Compliant
SN-28	2.0	Updated procedures	Compliant