High Sec Labs SK41D-4TR KVM

Firmware Version 44404-E7E7

Common Criteria Guidance Supplement

Doc No. 2149-001-D105A5
Version: 0.5
14 September 2021

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

intertek
ewa
canada

CONTENTS

LIST OF TABLES

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT

1.1 OPERATIONAL ENVIRONMENT

For secure operation, users are required to ensure the following conditions are met in the operational environment:

- TEMPEST approved equipment may not be used with the secure peripheral sharing device
- The operational environment must provide physical security, commensurate with the value of the peripheral sharing device and the data that transits it
- Wireless keyboards, mice, audio, user authentication, or video devices may not be used with the secure peripheral sharing device
- Peripheral sharing device Administrators and users are trusted individuals who are appropriately trained
- Administrators configuring the peripheral sharing device and its operational environment follow the applicable security configuration guidance
- Special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions may not be used with the secure peripheral sharing device

2 SECURE ACCEPTANCE PROCEDURES

High Sec Labs (HSL) SK41D-4TR KVM may be purchased directly from HSL, or through distributors and resellers / integrators.

Upon receipt of the device, the customer can verify the configuration and revision by comparing the part number and revision on the packing list with the label on the back of the hardware unit. The nameplate includes the product part number (CGA) which is linked directly to the revision of the hardware components and firmware. Verification of the part number provides assurance that the correct product has been received.

The customer must download the SK41D-4TR product documentation from the HSL website in Adobe Acrobat Portable Document Format (PDF). The customer can confirm that the documentation matches the purchased model.

Customers are instructed to check all delivered products for package container seals, and to verify that product tampering evident labels are intact. If an issue is discovered, the customer is instructed to return the product immediately.

3 SECURE INSTALLATION PROCEDURES

This section describes the steps necessary for secure installation and configuration.

3.1 SECURE INSTALLATION

Instructions for secure installation may be found in the Quick Installation Guide.

4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the HSL SK41D-4TR.

Users should be aware that the SK41D-4TR KVM does not provide indication of CAPS LOCK, NUM LOCK, or SCROLL LOCK status on the switch or on the remote control. If the behavior of the CAPS LOCK, NUM LOCK, or SCROLL LOCK features are not as expected, users are advised to toggle these settings.

4.1 SELF TESTS

A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

A user may initiate a self test by following the procedures outlined in Table 1. In the case of a self test failure, users are directed to contact HSL Technical Support.

Device Type	Procedure
SK41D-4TR KVM	1. To enter self test mode, press and hold the channel 1 button, and power on the device. The channel indicators on the front panel light up sequentially, and the keyboard, mouse and video ports are disabled. 2. To exit self test mode, cycle the power.

Table 1 – Procedure to Initiate a Self Test

4.2 SELECTED CHANNEL AT STARTUP

Channel 1 is selected by default when the device is started or reset.

4.3 NUMBER OF SUPPORTED DISPLAYS

The SK41D-4TR KVM supports a single display.

4.4 CLOCK

The SK41D-4TR device includes a real-time clock powered by a battery. The purpose of the clock is to provide an accurate timestamp for audited events. The time is set during production using the Central Time Zone. Administrators are not permitted to modify the time. Time is not provided to external devices. If the battery fails, the device enters the tampered mode. The user must then replace the device.

5 USE OF TERMINAL MODE

The HSL Administrator Guide, HDC19968 Rev. C provides guidance on the user of Terminal/Admin Mode. Not all of the Terminal Mode functions are supported in the SK41D-4TR device. The applicable sections are as follows:

Terminal Mode Option	Applicability
General	An Administrator may enter and exit terminal mode. This is the administrative interface for the device. An Administrator may power cycle the KVM using Terminal Mode, or by unplugging the device's power cable from the power outlet and plugging it back in. This is not a security function related to any Security Functional Requirement (SFR) in the High Sec Labs SK41D-4TR KVM Security Target.
0 Asset Management	This function is not supported. This is not a security function related to any SFR.
1 Firmware Versions	Although this may be used to verify the firmware version, this is not a security function related to any SFR.
2 Configure DPP	This function is not supported. The devices do not have a Dedicated Peripheral Port (DPP).
3 Configure SC	This function is not supported.
4 Account Management	An administrator may use these options to create and delete administrator accounts. Administrators can change their own passwords.
5 Reset to Factory Defaults	This is used to reset the device to factory defaults.
6 Logs and Events	This is used to access the logs created in accordance with FAU_GEN.1.
7 Configure Peripheral Devices	This function is not supported.

Table 2 – Applicable Sections of HSL Administrator Guide