Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader

Firmware Version 40040-0E7

Common Criteria Guidance Supplement

Doc No. 2149-001-D105C5
Version: 1.4
5 October 2021

Vertiv IT Systems
1050 Dearborn Dr,
Columbus, OH 43085

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

CONTENTS

1 PREPARATION OF THE OPERATIONAL ENVIRONMENT 1

1.1 OPERATIONAL ENVIRONMENT 1

2 SECURE ACCEPTANCE PROCEDURES 2

3 SECURE INSTALLATION PROCEDURES 3

3.1 SECURE INSTALLATION 3

4 SECURE OPERATION 4

4.1 SELF TESTS 4

4.2 SELECTED CHANNEL AT STARTUP 4

4.3 ERROR STATE 4

4.4 AUTHENTICATION DEVICE SWITCHING AND REMOVAL 4

LIST OF TABLES

Table 1 – Procedure to Initiate a Self Test 4

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

2 SECURE ACCEPTANCE PROCEDURES

Vertiv Multi-Domain Smart Card Reader devices may be purchased directly from Vertiv, or through distributors and resellers / integrators.

Upon receipt of the Vertiv multi-domain smart card reader, 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 product documentation from the Vertiv 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 Vertiv Multi-Domain Smart Card Reader.

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 for the applicable device type. In the case of a self test failure, users are directed to contact Vertiv Technical Support.

Device Type	Procedure
SCMDR0001	1. To enter self test mode, press the button to select Computer 1 while plugging in the power. The channels change and the channel indicators on the front panel light up sequentially. 2. To exit self test mode, cycle the power.

Table 1 – Procedure to Initiate a Self Test

4.2 SELECTED CHANNEL AT STARTUP

No channel is selected by default when the peripheral sharing device is started or reset. When the smart card reader becomes available, the Light Emitting Diode (LED) indicators on the front panel flash to show the available connected computers. The user must select the connected computer to be used with the multi-domain smart card reader device.

4.3 ERROR STATE

As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any smart card or pass data to any connected computer.

4.4 AUTHENTICATION DEVICE SWITCHING AND REMOVAL

An open authentication device session is terminated when the device is switched to a different computer, or when the authentication element (i.e. smart card) is removed from the device.