National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7

Version 1.0

Report Number: CCEVS-VR-VID11145-2021

Dated: October 22, 2021

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin: Senior Validator

Chris Thorpe: Lead Validator

Lisa Mitchell: ECR Team

Linda Morrison: ECR Team

Clare Parran: ECR Team

Common Criteria Testing Laboratory

Kenneth Lasoski

Joshua Gola

Acumen Security, LLC

Table of Contents

1 Executive Summary 4

2 Identification 6

3 Architectural Information 8

4 Security Policy 9

4.1 User Data Protection 9
4.2 Protection of the TSF 9
4.3 TOE Access 9

5 Assumptions, Threats & Clarification of Scope 10

5.1 Assumptions 10
5.2 Threats 10
5.3 Clarification of Scope 12

6 Documentation 13

7 TOE Evaluated Configuration 14

7.1 Evaluated Configuration 14
7.2 Excluded Functionality 14

8 IT Product Testing 15

8.1 Developer Testing 15
8.2 Evaluation Team Independent Testing 15

9 Results of the Evaluation 16

9.1 Evaluation of Security Target 16
9.2 Evaluation of Development Documentation 16
9.3 Evaluation of Guidance Documents 17
9.4 Evaluation of Life Cycle Support Activities 17
9.5 Evaluation of Test Documentation and the Test Activity 17
9.6 Vulnerability Assessment Activity 17
9.7 Summary of Evaluation Results 18

10 Validator Comments & Recommendations 19

11 Annexes 20

12 Security Target 21

13 Glossary 22

14 Bibliography 23

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in October 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device, and User Authentication Devices, which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the PP-Module for User Authentication Devices, Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the PP-Configuration for Peripheral Sharing Device, and User Authentication Devices, which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the PP-Module for User Authentication Devices, Version 1.0. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate,

the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.
Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Vertiv CYBEX™ SCMDR0001 Multi-Domain Card Reader Firmware Version 40040-0E7
Protection Profile	PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and User Authentication Devices, which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the PP-Module for User Authentication Devices, Version 1.0
Security Target	Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Security Target, Version 1.12, October 20, 2021
Evaluation Technical Report	Evaluation Technical Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device, Version 1.2, October 20, 2021
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Vertiv IT Systems
Developer	Vertiv IT Systems

Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd, Rockville MD 20850
CCEVS Validators	Daniel Faigin, Chris Thorpe, Lisa Mitchell, Linda Morrison, Clare Parran

3 Architectural Information

The Vertiv Multi-Domain Smart Card Reader allows users to share a single card reader between a number of connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

The evaluated features of the TOE are described further in Section 4.

4 Security Policy

The TOE is comprised of several security features. Each of the security features consists of several security functionalities, as identified below:

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

These features are described in more detail in the subsections below.

4.1 User Data Protection

The TOE provides secure isolation between connected computers and a smartcard.

4.2 Protection of the TSF

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.

4.3 TOE Access

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

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1 TOE Assumptions

Assumption	Assumption Definition
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved.
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.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 2 TOE Threats

Threat	Threat Definition
T.DATA_LEAK	A connection via the PSD 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.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the PP-Configuration for Peripheral Sharing Device, and User Authentication Devices, which references the Protection Profile for Peripheral Sharing Device Version 4.0 [PP_PSD_V4.0], and the PP-Module for User Authentication Devices, Version 1.0.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Security Target, Version 1.12, October 20, 2021
- CYBEX™ SECURE MULT-DOMAIN SMART CARD READER, 590-2296-501 Rev. A
- Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Common Criteria Guidance Supplement, Version 1.3, September 15, 2021

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

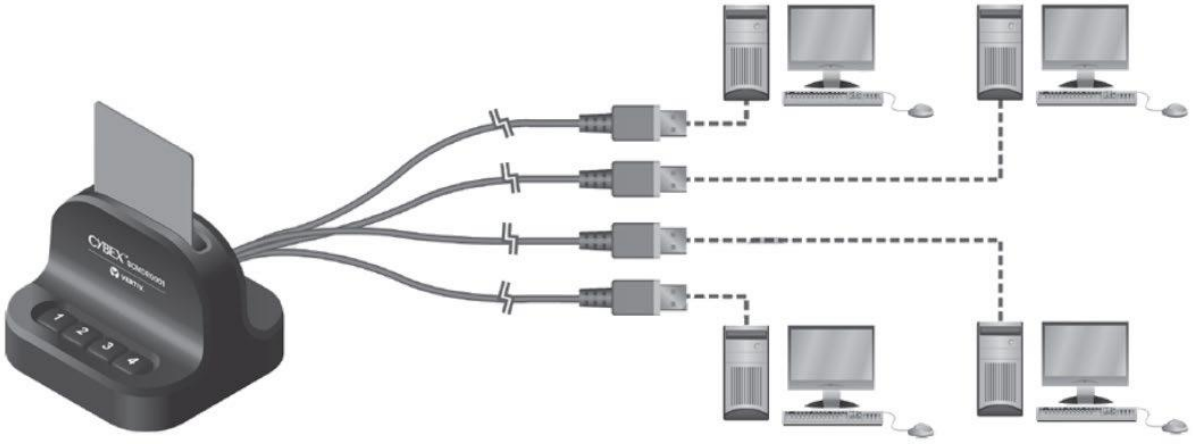

Figure 1 – Multi-Domain Smart Card Reader Evaluated Configuration

The Multi-Domain Smart Card Reader (MDR) is connected to up to four computers and is used with a smart card.

7.2 Excluded Functionality

The ST does not describe excluded functionality.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Technical Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile and the claimed module.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0 related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0 related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- National Vulnerability Database: https://nvd.nist.gov/vuln/search
- Vertiv Support: https://www.vertiv.com/en-ca/support/
- Common Vulnerabilities and Exposures: https://google.com

The evaluator performed the public domain vulnerability searches using the following key words: (The search was performed on October 6, 2021.)

- Vertiv
- Cybex
- SCMDR0001
- Firmware Version 40040-0E7
- Multi-Domain Smart Card Reader
- NAK transaction and
- STMicroelectronics 32-Bit.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the Protection Profile for Peripheral Sharing Device Version 4.0, and the PP-Module for User Authentication Devices, Version 1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Vertiv CYBEX SMDR0001Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Common Criteria Guidance Supplement, Version 1.4, October 5, 2021, document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation.

It should be noted that this device provides no user interfaces beyond the device selection buttons and the ability to insert a PIV/CAC card. As such, there is no ability to filter devices; indeed, there is no ability to connect anything to the TOE other than the computers selected by the device selection buttons.

11 Annexes

Not applicable.

12 Security Target

Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Security Target, Version 1.12, October 20, 2021.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Security Target, Version 1.12, October 20, 2021.
6. Assurance Activity Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device [AAR], Version 1.2, October 20, 2021.
7. Evaluation Technical Report for Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Peripheral Sharing Device [ETR], Version 1.2, October 20, 2021.
8. Vertiv CYBEX™ SCMDR0001 Multi-Domain Smart Card Reader Firmware Version 40040-0E7 Common Criteria Guidance Supplement, Version 1.4, October 5, 2021.
9. CYBEX™ SECURE MULT-DOMAIN SMART CARD READER, 590-2296-501 Rev. A.