Ärendetyp: 6
Diarienummer: 20FMV3898-33
Dokument ID CSEC2020019

Swedish Certification Body for IT Security

Certification Report - Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-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 Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-E7E7, including the following models:

Model	Type	FW
SC820DPH	KVM	44404-E7E7
SC840DPH	KVM	44404-E7E7
SC920DPH	KVM	44404-E7E7
SC940DPH	KVM	44404-E7E7
SC845DPH	KVM	44444-E7E7
SC945DPH	KVM	44444-E7E7
SC840DPHC	KVM	44404-E7E7
SC845DPHC	KVM	44444-E7E7
SC940DPHC	KVM	44404-E7E7
SC945DPHC	KVM	44444-E7E7
SC840DVI	KVM	44404-E7E7
SC940DVI	KVM	44404-E7E7
SC985DPH	KVM	44444-E7E7
SCKM145PP4	KM	40444-E7E7
SCM145DPH	KVM Matrix	44444-E7E7
SCM185DPH	KVM Matrix	44444-E7E7

The TOE is a KVM Switch and allow users to share keyboard and mouse functionality between a number of connected computers. Security features ensure isolation between computers and peripherals1 to prevent data leakage between connected systems.

The TOE is delivered as a single package including the device hardware and software and the cables required to connect to the computers. The TOE is delivered to the customer via trusted courier.

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 Target (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	CSEC2020019
Name and version of the certified IT product	Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-E7E7
Security Target Identification	Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-E7E7, Security Target, 2021-09-24, document version 0.5
EAL	EAL4 + ALC_FLR.3
Sponsor	Vertiv
Developer	Vertiv
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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

3.1 Security Audit

Audit entries are generated for security related events.

3.2 User Data Protection

The TOE ensures that only authorized device types may be successfully connected to the TOE. The TOE ensures that user data only flows from the peripheral devices to the selected computer, and video data flows only from the connected computer to the display.

3.3 Identification and Authentication

Administrators must be identified and authenticated prior to accessing administrative functions. Users may only switch the connected computer channel.

3.4 Security Management

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. Only switching between connected computers is permitted. Administrators may perform security management functions.

3.5 Protection of the TSF

The TOE provides clear indications of tampering attempts. The TOE provides reliable time stamps.

3.6 TOE Access

The TOE provides a visual indication showing which channel is currently selected.

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 is provided 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.PHYSICAL_TAMPER

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

T.SWITCHING

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

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

Vertiv Secure KVM, KM and KVM Matrix Devices allow users to share keyboard and mouse functionality between a number of connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

TOE devices include:

- Keyboard, Video, Mouse (KVM) Switches
  - Firmware version 44444-E7E7 and 44404-E7E7
- Keyboard, Mouse (KM) Switches
  - Firmware version 40444-E7E7
- KVM Matrix Switches
  - Firmware version 44444-E7E7

Devices that support keyboard, video, mouse, audio and user authentication (DPP) devices have firmware version 44444-E7E7. Devices that do not support DPP have firmware version 44404-E7E7. The KM device does not support video, but does support DPP, and therefore the firmware version is 40404-E7E7. The firmware for each programmable component is the same for all devices. The devices that do not support video or DPP do not have firmware for those functions.

5.1 TOE Design

The TOE is a combined software and hardware TOE.

Figure 1 shows a basic evaluated configuration for KVM Switches. In the evaluated configuration, the TOE may be connected to two or four computers. The video input may be DisplayPort, HDMI, DVI-D or USB Type-C with DisplayPort as an alternate function, and one or two displays may be connected. The peripheral sharing device is connected to speakers or headphones, and some devices are connected to a user authentication device.

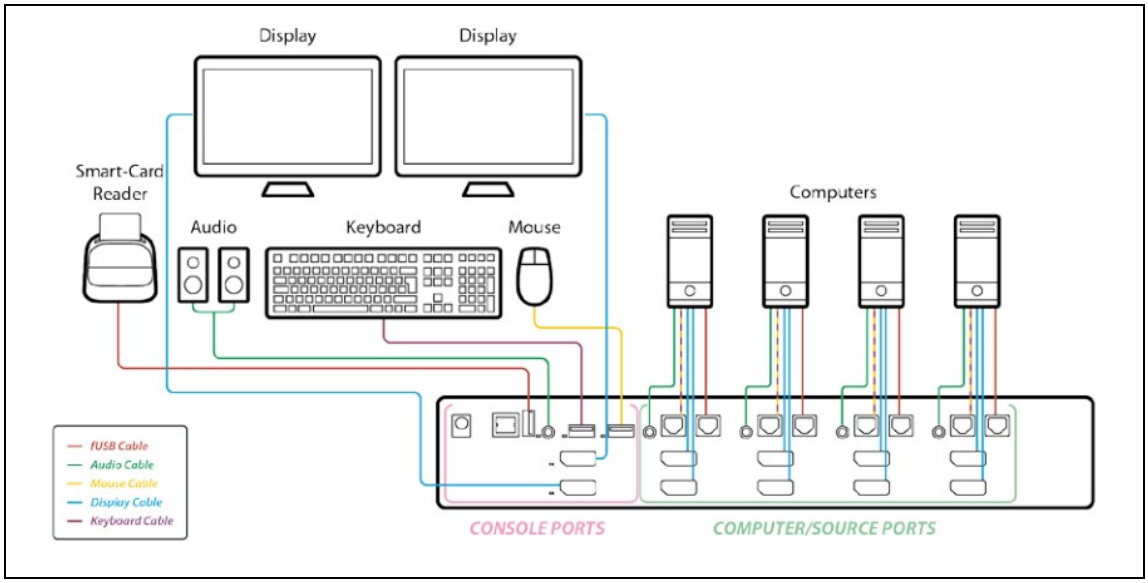

Figure 1 – KVM Switch Evaluated Configuration

This configuration applies to the following TOE models:

- SC820DPH
- SC840DPH
- SC920DPH
- SC940DPH
- SC845DPH
- SC945DPH
- SC840DPHC
- SC845DPHC
- SC940DPHC
- SC945DPHC
- SC840DVI
- SC940DVI
- SC985DPH

Figure 2 shows the evaluated configuration for the KM switches. In the evaluated configuration, the peripheral sharing device may be connected to a user authentication device.

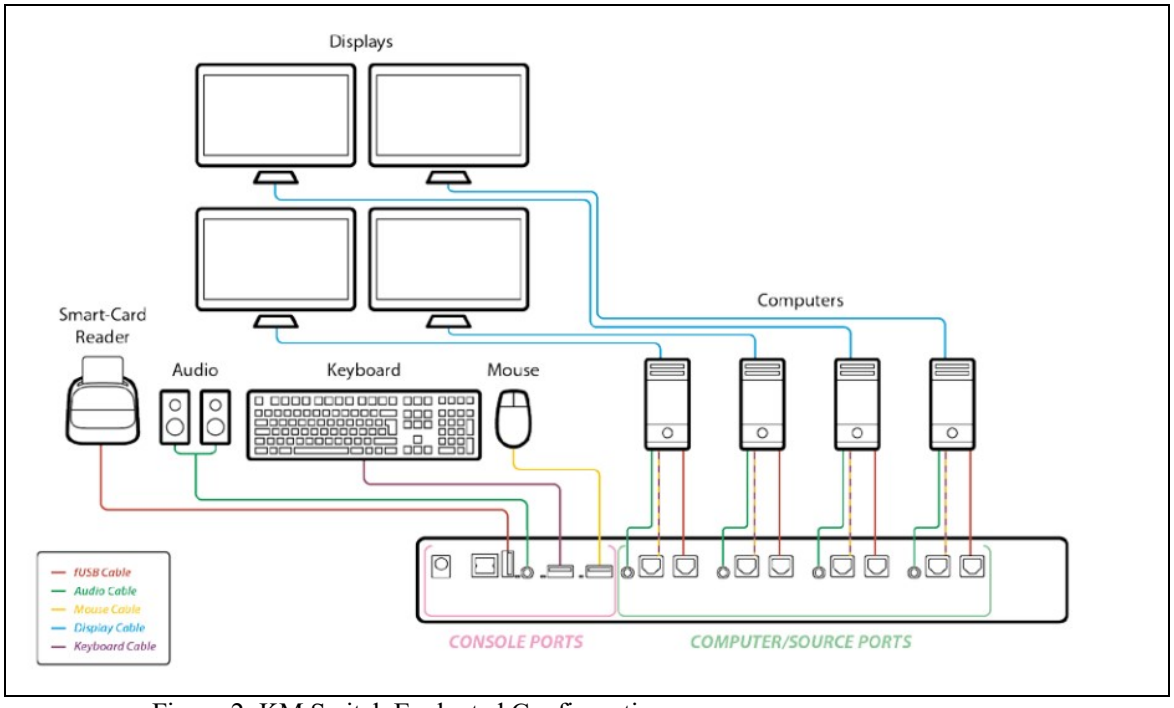

Figure 2: KM Switch Evaluated Configuration

This configuration applies to the following model:

- SCKM145PP4

The evaluated configuration for the KVM Matrix devices is similar to the configuration for KVM devices (Figure 1), with four or eight connected computers, two connected displays, keyboard, mouse, audio and authentication device. This configuration applies to the following models:

- SCM145DPH
- SCM185DPH

The TOE Security Functional Interfaces (TSFIs) and subsystems that support the TOE Security Functional Requirements (SFRs) are shown in Figure 3:

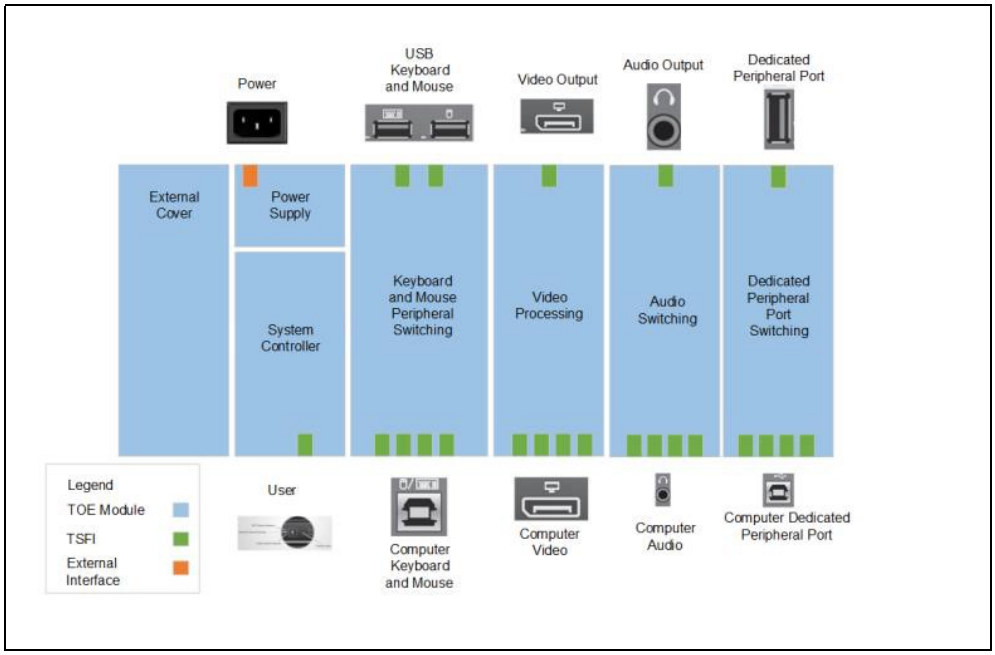

Figure 3: TOE Diagram

The following security features are provided by all the Vertiv TOE devices:

- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (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
- Audio Security
  - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- Hardware Anti-Tampering Indication
  - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

The following security features are provided by the Vertiv Secure KVM and KVM Matrix Devices:

- Video Security

  - Computer video input interfaces are isolated through the use of different electronic components, power and ground domains.
  - The display is isolated by a dedicated, read-only, Extended Display
  - Identification Data (EDID) emulation for each computer
  - Access to the monitor's EDID is blocked
  - Access to the Monitor Control Command Set (MCCS commands) is blocked

The following security features are provided by the SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM185DPH, SC985DPH and SCKM145PP4 Devices:

- Authentication Device
  - Unauthorized USB devices are blocked
  - USB authentication devices are authorized by default; all other devices are blocked by default
  - Devices may be whitelisted or blacklisted based on Vendor Identification/Product Identification (VID/PID) characteristics
  - Secure management functions allow configuration of allowed devices, and maintain a record of any changes to that configuration

6 Documentation

The TOE includes the following guidance documentation, which may be downloaded in Portable Document Format (pdf) from the Vertiv website:

- CYBEX™ SC SERIES SECURE SWITCHES SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Installation Guide
- CYBEX™ SC SERIES SECURE SWITCHES SC800DPHC/SC900DPHC Quick Installation Guide
- CYBEX™ SC SERIES SECURE SWITCHES SCM100DPH DESKTOP MATRIX Quick Installation Guide
- Cybex™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin

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 16 models are Pass. All test cases are executed for all the TOE models, with a few exceptions.

All developer tests result in a Pass.

7.2 Evaluator Testing

The tests are divided into four 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: Additional tests defined by the evaluator
- Test Group 4: Tests that complements the vulnerability assessment

Not all models of the TOE are used and only Windows 10 is used as operating system.

Evaluator site (hands-on tests):

- 2 source computers and 2 displays.

Developer site (performed remotely, overseeing by the evaluator):

- 4 source computers and 4 displays.

For the following sample of devices were used for the evaluator tests:

- SCM145DPH – KVM Matrix, FW 44444-E7E7
  - Received unit from the developer, used for all tests at the evaluator site
- SCKM145PP4 – KM, FW 40444-E7E7
  - The only device with FW 40444-E7E7, developer site
- SC820DPH - KVM, FW 44404-E7E7, developer site
- SC945DPH – KVM, FW 44444-E7E7, developer site

The evaluator decided to repeat quite many of the test cases for the received model SCM145DPH.

This sample of test cases will cover TSFIs, and almost all of the TSFs and SFRs.

The coverage of the developer tests is assessed to be high, therefore the number of additional tests was low, three test cases were added:

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". This test was executed for one model SCM145DPH.

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 computers (2, 4 or 8 depending upon device model)	General purpose computing hardware supporting DisplayPort or High-Definition Multimedia Interface (HDMI) (supporting Ultra-high-definition (UHD) 4K resolution up to 3840 x 2160) video and USB type B mouse and keyboard connections. Operating system as specified in section 2.4 below.
Video monitor (up to 2 monitors)	HDMI 1.4, DisplayPort 1.1, 1.2 or Digital Visual Interface Type D (DVI-D)
Keyboard	USB Type A
Mouse	USB Type A
Audio output device	Analog audio output device (speakers or headphones)
User authentication device	Standard USB smartcard reader/authentication device
Vertiv KVM Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort, DVI-D, USB-C and HDMI) 3.5mm stereo cable (Audio cable) USB Type-A to USB Type-B (authentication device)

8.1 Excluded from the TOE Evaluated Configuration

For the purposes of this evaluation, Windows Server 2008 R2 host machines were used. However, the use of other operating systems does not affect the security functionality provided by the TOE devices.

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 Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-E7E7, Security Target, Vertiv, 2021-09-24, document version 0.5

CCguide Vertiv Secure KVM, KM and KVM Matrix Devices Firmware Versions 44444-E7E7, 44404-E7E7 and 40444-E7E7, Common Criteria Guidance Supplement, Vertiv, 2021-02-12, document version 0.2

QS_1 CYBEX™ SC SERIES SECURE SWITCHES SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Installation Guide

QS_2 CYBEX™ SC SERIES SECURE SWITCHES SC800DPHC/SC900DPHC Quick Installation Guide

QS_3 CYBEX™ SC SERIES SECURE SWITCHES SCM100DPH DESK-TOP MATRIX Quick Installation Guide

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

A.1 Scheme/Quality Management System

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.2 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