Swedish Certification Body for IT Security

Certification Report HP GIF HCDPP

Issue: 1.0, 2018-okt-22

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1   Executive Summary

The Target of Evaluation, TOE, is a multifunction printer (MFP). The following model series are included in the scope of the evaluation:

HP LaserJet Enterprise MFP M631/M632/M633,

HP Color LaserJet Enterprise M681/M682,

HP LaserJet Managed MFP E72525/E72530/E72535/E82540/E82550/E82560/ E62555/E62565/E62575,

HP Color LaserJet Managed MFP E77822/E77825/E77830/E87640/E87650/ E87660/E67550/E67560

These MFPs provide network printing, copying, faxing, scanning, and storing.

The evaluated security features include administrator and user identification and authentication, encrypted network communication (IPSec), encrypted storage of files etc.

The ST claims conformance to the Protection Profile for Hardcopy Devices v1.0, Errata #1, and TD0074, TD0157, TD0176, TD0219, TD0253, TD0261, and TD0299. The evaluation has verified exact conformance to the PP.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, to some extent in the approved foreign location in Austin, Texas, USA, and the developer's premises in Boise, Idaho, USA, and was completed on the 18th of October 2018.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation conforms to both the evaluation activities in the HCDPP and to evaluation assurance level EAL 1, augmented by ASE_SPD.1.

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

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for the evaluation assurance level EAL 1 + ASE_SPD.1 as well as the requirements in HCDPP.

2   Identification

Certification Identification	
Certification ID	CSEC2017011

Name and version of the certified IT product	HP LaserJet Enterprise MFP M631/M632/M633
	    MFP firmware version 2405143_000032
	    JDI firmware version JSI24050403
	HP Color LaserJet Enterprise M681/M682,
	    MFP firmware version 2405143_000033
	    JDI firmware version JSI24050403
	HP LaserJet Managed MFP E72525/E72530/E72535
	    MFP firmware version 2405143_000035
	    JDI firmware version JSI24050403
	HP LaserJet Managed MFP E82540/E82550/E82560
	    MFP firmware version 2405143_000030
	    JDI firmware version JSI24050403
	HP LaserJet Managed MFP E62555/E62565/E62575
	    MFP firmware version 2405143_000032
	    JDI firmware version JSI24050403
	HP Color LaserJet Managed MFP E77822/E77825/
	E77830
	    MFP firmware version 2405143_000031
	    JDI firmware version JSI24050403
	HP Color LaserJet Managed MFP E87640/E87650/
	E87660
	    MFP firmware version 2405143_000034
	    JDI firmware version JSI24050403
	HP Color LaserJet Managed MFP E67550/E67560
	    MFP firmware version 2405143_000033
	    JDI firmware version JSI24050403

Security Target	HP LaserJet Enterprise MFP M631/M632/M633, HP Color LaserJet Enterprise M681/M682, HP LaserJet Managed MFP E72525/E72530/ E72535/E82540/E82550/E82560/E62555/E62565/ E62575, HP Color LaserJet Managed MFP E77822/E77825/ E77830/E87640/E87650/E87660/E67550/E67560 Security Target
Assurance packages	EAL 1 + ASE_SPD.1 and Protection Profile for Hardcopy Devices v1.0 with Erra-ta #1

Sponsor	HP Inc.
Developer	HP Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.21.4
Scheme Notes Release	1.21.4
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2018-10-22

3 Security Policy

The TOE provides the following security services:

- Identification, Authentication, and Authorization
- Access Control
- Cryptography
- Trusted Communications
- Administrative Roles
- Auditing
- Trusted Operation
- PSTN Fax - Network Separation
- Data Clearing

A brief description of each security policy is given below. A more detailed description is given in the ST.

3.1 Identification, Authentication, and Authorization

The TOE supports user accounts in the local device (in the evaluated configuration only for administrators), for Control Panel, EWS and RESTful users. SNMPv3 users also uses the local user account database. All other users have to use external authentication via LDAP or a Windows Domain Server.

3.2 Access Control

The TOE enforces access control on TSF data and User Data. Each piece of User Data is assigned ownership and access to the data is limited by the access control mechanism. The PSs used to define roles also affect the access control of each user.

Depending on the TOE model, the TOE contains either one or two field-replaceable, nonvolatile storage devices. These devices are disk-based SEDs whose cryptographic functions have been FIPS 140-2 validated. Together with the drive-lock password, these SEDs ensure that the TSF Data and User Data on the drives are not stored as plaintext on the storage device.

3.3 Cryptography

● IPsec

The TOE's IPsec supports both pre-shared keys (PSKs) and X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange version 1 (IKEv1) protocol.

● Drive-lock password

For secure storage, all TOE models contain a single field-replaceable nonvolatile storage device. This device is a FIPS 140-2 validated, disk-based, self-encrypting drive (SED). Some TOE models contain a second disk-based SED that is non-field replaceable.

● Digital signatures for trusted update

The TOE uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to protect downloaded updates.

● Digital signatures for TSF testing

The TOE also uses digital signatures as part of its TSF self-testing functionality.

3.4 Trusted Communications

The TOE uses IPsec to protect the communications between the TOE and trusted IT entities and between the TOE and client computers. IPsec provides assured identification of the endpoints. It implements IKEv1 and transport mode. The TOE also supports both X.509v3 certificates and pre-shared keys (PSKs) for endpoint authentication.

3.5 Administrative Roles

The TOE supports roles implemented as permission sets. The administrator assigns users to these roles. The SNMPv3 and RESTful interfaces are only accessible to administrators.

3.6 Auditing

The TOE supports both internal and external storage of audit records. The evaluated configuration requires the use of an external syslog server for external audit record storage. The connection between the TOE and the syslog server is protected using IPsec. No unauthorized access to the audit records is allowed by the TOE.

3.7 Trusted Operation

TOE updates can be downloaded from the HP Inc. website. These updates are digitally signed by HP Inc. using the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 signature generation.

The TOE's EWS interface allows an administrator to install the update images. When installing an update image, the TOE validates the digital signature of the update image before installing the update image.

The TOE contains TSF testing functionality referred to as Whitelisting to help ensure only authentic, known-good System firmware files that have not been tampered with are loaded into memory. Whitelisting uses digital signatures based on the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 to validate the firmware files.

3.8 PSTN Fax - Network Separation

The PSTN fax capability is either included with or can be added to the TOE, depending on model. In either case, the TOE provides a distinct separation between the fax capabilities and the Ethernet network connection of the TOE prohibiting communication via the fax interface except when transmitting or receiving User Data using fax protocols.

3.9 Data Clearing

The TOE also supports the Image Overwrite function (O.IMAGE_OVERWRITE) defined in [HCDPP] for the field-replaceable nonvolatile storage device.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes four assumptions on the usage and the operational environment of the TOE.

A.PHYSICAL - Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.

A.TRUSTED_ADMIN - TOE Administrators are trusted to administer the TOE according to site security policies.

A.TRAINED_USERS - Authorized Users are trained to use the TOE according to site security policies.

A.NETWORK - The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.

4.2 Clarification of Scope

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

T.UNAUTHORIZED_ACCESS - An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.

T.TSF_COMPROMISE - An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.

T.TSF_FAILURE - A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.

T.UNAUTHORIZED_UPDATE - An attacker may cause the installation of unauthorized software on the TOE.

T.NET_COMPROMISE - An attacker may access data in transit or otherwise compromise the security of the TOE by

monitoring or manipulating network communication.

The Security Target contains seven Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.AUTHORIZATION - Users must be authorized before performing Document Processing and administrative functions.

P.AUDIT - Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.

P.COMMS_PROTECTION - The TOE must be able to identify itself to other devices on the LAN.

P.STORAGE_ENCRYPTION - If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.

P.KEY_MATERIAL - Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

P.FAX_FLOW - If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

P.IMAGE_OVERWRITE - Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.

5   Architectural Information

The TOE is the HCD designed to be shared by many client computers and human users. It performs the functions of copying, printing, faxing, scanning, and storing of documents. It can be connected to a local network through Ethernet, to an analog telephone line using its internal analog fax modem, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration).

The HTTP-based EWS administrative interface allows administrators to remotely manage the features of the TOE using a web browser. This interface is protected using IPsec.

The Web Services (WS) interfaces allow administrators to externally manage the TOE. The evaluated configuration only supports the RESTful Web Services interface. The RESTful interface is protected using IPsec.

The SNMP network interface allows administrators to remotely manage the TOE using external SNMP-based management tools. The evaluated configuration supports SNMPv3 only. This interface is protected using IPsec.

Printer Job Language (PJL) is used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL to send print jobs to the TOE as well as to receive job status. In general, PJL supports password-protected administrative commands, but in the evaluated configuration these commands are disabled

The TOE protects all network communications with Internet Protocol Security (IPsec). Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using X.509v3 certificates or PSK. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) into the TOE with the Certificate Authority's CA certificate.

Because IPsec authenticates the computers (IPsec authenticates the computer itself; IPsec does not authenticate the individual users of the computer), access to the Administrative Computer should be restricted to TOE administrators only.

The TOE distinguishes between the Administrative Computer and Network Client Computers by using IP addresses, IPsec, and the embedded JetDirect Inside's internal firewall. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one and the Device Administrator Password must be set.

Network Client Computers connect to the TOE using IPsec with X.509v3 certificates or PSK to protect the communication and to mutually authenticate. These client computers can send print jobs to the TOE using the PJL Interface as well as receive job status.

The TOE supports an optional analog telephone line connection for sending and receiving faxes.

Each HCD contains a user interface (UI) called the Control Panel. The Control Panel consists of a touchscreen LCD, a physical home screen button that are attached to the HCD, and a pull-out keyboard as part of the Control Panel. The Control Panel is the physical interface that a user uses to communicate with the TOE when physically using the HCD. The LCD screen displays information such as menus and status to the user. It also provides virtual buttons to the user such as an alphanumeric keypad for entering usernames and passwords. Both administrative and non-administrative users can access the Control Panel.

6   Documentation

For proper configuration of the TOE into the evaluated configuration, the following guidance documents are available:

- CCECG

  HP Preparatory Procedures and Operational Guidance for HP Multifunction Printers

- E70000_UG

  HP LaserJet Managed MFP E72525, HP LaserJet Managed MFP E72530, HP LaserJet Managed MFP E72535, HP LaserJet Managed Flow MFP E72525, HP LaserJet Managed Flow MFP E72530, HP LaserJet Managed Flow MFP E72535, HP Color LaserJet Managed MFP E77822, HP Color LaserJet Managed MFP E77825, HP Color LaserJet Managed MFP E77830, HP Color LaserJet Managed Flow MFP E77822, HP Color LaserJet Managed Flow MFP E77825, HP Color LaserJet Managed Flow MFP E77830 User Guide

- E80000_UG

  HP LaserJet Managed MFP E82540, HP LaserJet Managed MFP E82550, HP LaserJet Managed MFP E82560, HP LaserJet Managed Flow MFP E82540, HP LaserJet Managed Flow MFP E82550, HP LaserJet Managed Flow MFP E82560, HP Color LaserJet Managed MFP E87640, HP Color LaserJet Managed MFP E87650, HP Color LaserJet Managed MFP E87660, HP Color LaserJet Managed Flow MFP E87640, HP Color LaserJet Managed Flow MFP E87650, HP Color LaserJet Managed Flow MFP E87660 User Guide

- M630 IG

  HP LaserJet Enterprise MFP M631, M632, M633 Installation Guide

- M630 UG

  HP LaserJet Enterprise MFP M631, M632, M633 User Guide

- M680 IG

  HP LaserJet Enterprise MFP M681, M682 Installation Guide

- M680 UG

  HP LaserJet Enterprise MFP M681, M682 User Guide

7 IT Product Testing

7.1 Evaluator Testing

The evaluators have performed all required tests listed in the HCDPP and have tested a selection of MFP models covering each distinct binary that implements any part of the security functionality in any of the TOE models.

The evaluator testing also covers the requirements of ATE_IND.1.

All test results were as expected.

7.2 Penetration Testing

The evaluator examined all potential interfaces (UDP and TCP ports) and tried to spoof the administrative computers IP address under three different scenarios.

The evaluator determined that only UDP port 500 (ISAKMP) is available outside of IPsec, and no packets were sent from the TOE to the Administrative computer in response to the replayed packets sent from the Client computer.

All test results were as expected.

8   Evaluated Configuration

The following items will need to be adhered to in the evaluated configuration.

- HP Digital Sending Software (DSS) must be disabled.
- Only one Administrative Computer is used to manage the TOE.
- HP and third-party applications cannot be installed on the TOE.
- PC Fax Send must be disabled.
- Fax polling received must be disabled.
- Type A and B USB ports must be disabled.
- Remote Firmware Upgrade through any means other than the EWS (e.g., PJL) and USB must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- File System External Access must be disabled.
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Full Authentication must be enabled (this disables the Guest role).
- SNMP support is limited to SNMPv3.
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- Near Field Communication (NFC) must be disabled.
- Wireless networking (WLAN) must be disabled.
- PJL device access commands must be disabled.
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections.
- The "Save to HTTP" function is disallowed and must not be configured to function with an HTTP server.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the Device Administrator account is allowed as a Local Device Sign In account).
- The following Web Services (WS) must be disabled:
  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services

The following required components are part of the Operational Environment.

- Domain Name System (DNS) server
- Network Time Service (NTS) server
- One administrative client computer network connected to the TOE in the role of an Administrative Computer. It must contain:
  - SNMP tool that supports SNMPv3 for reading and writing objects
  - Web browser
- One or both of the following:
  - Lightweight Directory Access Protocol (LDAP) server
  - Windows domain controller/Kerberos server

- Syslog server
- Windows Internet Name Service (WINS) server

The following optional components are part of the Operational Environment.
- Client computers network connected to the TOE in a non-administrative computer role
- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- Microsoft SharePoint ('Flow' models only)
- Remote file systems:
  - File Transfer Protocol (FTP)
  - Server Message Block (SMB)
- Simple Mail Transfer Protocol (SMTP) gateway

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 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 respective assurance classes and components are summarised in the following table:

Assurance Class/Family	Short name	Verdict
Development	ADV	PASS
Basic functional specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
PP assurance activities	AGD_HCDPP.1	PASS
Life-cycle Support	ALC	PASS
Labeling of the TOE	ALC_CMC.1	PASS
TOE CM coverage	ALC_CMS.1	PASS
PP assurance activities	ALC_HCDPP.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 for the Operational Environment	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Stated Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
PP assurance activities	ASE_HCDPP.1	PASS
Tests	ATE	PASS
Independent Testing - conformance	ATE_IND.1	PASS
PP assurance activities	ATE_HCDPP.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability survey	AVA_VAN.1	PASS
PP assurance activities	AVA_HCDPP.1	PASS
Entropy Description	AEN	
PP assurance activities	AEN_HCDPP.1	PASS
Key Management Description	AKM	
PP assurance activities	AKM_HCDPP.1	PASS

Note that the evaluators have used a notation similar to assurance classes for PP assurance activities that does not belong to a particular assurance class in CC.

For PP requirements that are related to existing assurance classes, the evaluators have used a notation similar to assurance components for the requirements.

10   Evaluator Comments and Recommendations

None.

11   Glossary

BEV	Border Encryption Value
CC	Common Critera
CSEC	The Swedish Certification Body for IT Security
DNS	Domain Name System
EAL	Evaluated Assurance Level
ESP	Encapsulating Security Payload (IPsec)
EWS	Embedded Web Server
GUI	Graphical User Interface
HCD	Hardcopy Device
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IKE	Internet Key Exchange (IPsec)
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Printer
NTS	Network Time Service
OS	Operating System
OXP	Open Extensibility Platform
OXPd	OXP device layer
PJL	Printer Job Language
PP	Protection Profile
PSTN	Public Switched Telephone Network
REST	Representational State Transfer (a.k.a. RESTful)
RESTful	See REST
SED	Self-Encrypting Drive
SHA	Secure HashAlgorithm
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
WS	Web Services

12   Bibliography

ST   HP LaserJet Enterprise MFP M631/M632/M633,

                  HP Color LaserJet Enterprise M681/M682,

                  HP LaserJet Managed MFP E72525/E72530/E72535/E82540/

                  E82550/E82560/E62555/E62565/E62575,

                  HP Color LaserJet Managed MFP E77822/E77825/E77830/

                  E87640/E87650/E87660/E67550/E67560 Security Target,

                  HP Inc., 2018-09-05, document version 2.0

CCECG   HP Preparatory Procedures and Operational Guidance for

                  HP Multifunction Printers, HP Inc., 2018-09-06, Edition 1 9/2018

E70000_UG   HP LaserJet Managed MFP E72525, HP LaserJet Managed MFP

                  E72530, HP LaserJet Managed MFP E72535, HP LaserJet Managed

                  Flow MFP E72525, HP LaserJet Managed Flow MFP E72530, HP

                  LaserJet Managed Flow MFP E72535, HP Color LaserJet Managed

                  MFP E77822, HP Color LaserJet Managed MFP E77825, HP Color

                  LaserJet Managed MFP E77830, HP Color Laser-Jet Managed Flow

                  MFP E77822, HP Color LaserJet Managed Flow MFP E77825, HP

                  Color LaserJet Managed Flow MFP E77830 User Guide, HP Inc.,

                  2017-04, Edition 1

E80000_UG   HP LaserJet Managed MFP E82540, HP LaserJet Managed MFP

                  E82550, HP LaserJet Managed MFP E82560, HP LaserJet Managed

                  Flow MFP E82540, HP LaserJet Managed Flow MFP E82550, HP

                  LaserJet Managed Flow MFP E82560, HP Color LaserJet Managed

                  MFP E87640, HP Color LaserJet Managed MFP E87650, HP Color

                  LaserJet Managed MFP E87660, HP Color Laser-Jet Managed Flow

                  MFP E87640, HP Color LaserJet Managed Flow MFP E87650, HP

                  Color LaserJet Managed Flow MFP E87660 User Guide, HP Inc.,

                  2017-04, Edition 1

M630 UG   HP LaserJet Enterprise MFP M631, M632, M633 User Guide, HP

                  Inc., 2017-05, Edition 1

M680 UG   HP LaserJet Enterprise MFP M681, M682 User Guide, HP Inc.,

                  2017-05, Edition 1

HCDPP   Protection Profile for Hardcopy Devices, IPA/NIAP/MFP TC,

                  2015-09-10, document version 1.0

ERRATA   Protection Profile for Hardcopy Devices - v1.0 Errata#1 June 2017,

                  IPA/NIAP/HCD TC, 2017-06

                  27 February 2015, version 1.0

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

SP-002   SP-002 Evaluation and Certification, CSEC, 2018-04-24, document
                 version 29.0

SP-188   SP-188 Scheme Crypto Policy, CSEC, 2017-04-04, document
                 version 7.0

Appendix A   Scheme Versions

During the certification project, the following versions of the quality management sys-tem (QMS) have been applicable since the certification application was received 2017-08-21:

QMS 1.20.5   valid from 2017-06-28

QMS 1.21   valid from 2017-11-15

QMS 1.21.1   valid from 2018-03-09

QMS 1.21.2   valid from 2018-03-09 SIC!

QMS 1.21.3   valid from 2018-05-24

QMS 1.21.4   valid from 2018-09-13

In order to ensure consistency in the outcome of the certification, the certifier has ex-amined the changes introduced in each update of the quality management sys-tem.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.21.4".

The certifier concluded that, from QMS 1.20.5 to the current QMS 1.21.4, there are no changes with impact on the result of the certification.