Swedish Certification Body for IT Security

Certification Report - HP YA 2600

Issue: 1.0, 2020-Jun-09

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the HP FutureSmart 4.6.3 firmware for the HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner.

The TOE is comprised of the contents of the firmware with the exception of the operating system, which is part of the Operational Environment.

The firmware and guidance documentation are packaged in a single ZIP file and available for download from the HP Inc. website. The firmware is packaged in this ZIP file as a single firmware bundle. This firmware bundle contains the HP FutureSmart firmware, which in turn contains the System firmware and the JDI firmware.

In order to download the ZIP file, the customer needs to register with HP and sign into a secure website (HTTPS) to access the download page. The customer can receive sign-in credentials by sending an email to ccc-hp-enterprise-imaging-printing@hp.com. On the download site, a SHA-256 checksum is provided along with instructions on how to use it for verification of the integrity of the downloaded package.

This Security Target claims conformance to the following Protection Profiles and PP packages:

- [PP2600.1]: IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A", Version 1.0 as of June 2009; demonstrable conformance
- [PP2600.1-SCN]: SFR Package for Hardcopy Device Scan Functions, Version 1.0 as of June 2009; demonstrable conformance
- [PP2600.1-SMI]: SFR Package for Hardcopy Device Shared-medium Interface Functions, Version 1.0 as of June 2009; demonstrable conformance

The evaluation has been performed by atsec information security AB in atsec information security AB in Danderyd, Sweden. Site-visit was performed in Bangalore, India and testing was performed in Boise, Idaho, USA.

The evaluation was completed on 2020-05-29. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

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 EAL 3 augmented ALC_FLR.2.

2 Identification

Certification Identification	
Certification ID	CSEC2019013
Name and version of the certified IT product	• HP Digital Sender Flow 8500 fn2 Document Capture Workstation, System firmware version 2406249_032755, JDI firmware version JSI24060306 • HP ScanJet Enterprise Flow N9120 fn2 Document Scanner , System firmware version 2406249_032756, JDI firmware version JSI24060306
Security Target Identification	HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target, 2020-05-05, Version 1.6
EAL	EAL3 + ALC_FLR.2.
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	1.23.2
Scheme Notes Release	15.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2020-06-09

3 Security Policy

The security features performed by the TOE are as follows:

- Auditing
- Cryptography
- Identification and authentication (I&A)
- Data protection and access control
- Protection of the TSF
- TOE access protection
- Trusted channel communication and certificate management
- User and access management

3.1 Auditing

The TOE performs auditing of security-relevant functions. The TOE connects and sends audit records to a syslog server (part of the Operational Environment) for long-term storage and audit review. Each audit record includes the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Events resulting from actions of identified users are associated with the identity of the user that caused the event.

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library is used to supply the cryptographic algorithms for IPsec.

The TOE's on-demand Data Integrity Test and Code Integrity Test use the SHA-256 algorithm to verify the integrity of specific TSF Data and TOE executable code, respectively. The HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation, which is part of the operational environment, supplies the SHA-256 algorithm.

3.3 Identification and authentication (I&A)

The TOE supports multiple Control Panel sign in methods, both local and remote methods:

- Local sign in method:
  - Local Device Sign In (Local Administrator account only)
- Remote sign in methods:
  - LDAP Sign In
  - Windows Sign In (via Kerberos)

The Control Panel allows both non-administrative users (U.NORMAL) and administrative users (U.ADMINISTRATOR) to sign in.

The TOE also uses IPsec to identify and mutually authenticate the following user type:

- Administrative Computer (U.ADMINISTRATOR)

3.4 Data protection and access control

3.4.1 Permission Sets

For Control Panel users, the TOE uses a user's User Role (as determined by each user's Permission Set) to determine a user's access to many TOE functions. Only U.ADMINISTRATOR can query, create, modify, and delete Permission Sets. In addition, only U.ADMINISTRATOR can query, create, modify, and delete the Permission Set associations to users.

3.4.2 Common access control

Scan jobs are ephemeral on the TOE by design. The TOE does not provide a user the ability to store a scan job on the HCD and retrieve it later. Because of this, only the U.NORMAL user creating the scan job has access to the scan job and only this user can read and delete the scan job document (D.DOC) and modify and delete the job's function data (D.FUNC). Other U.NORMAL users do not have access to this scan job.

3.4.3 TOE function access control -

The TOE controls TOE functions available at the Control Panel using permissions defined in Permission Sets. During the Control Panel sign-in process, the TOE authorizes the user after they are successfully identified and authenticated. As part of the user authorization process, the TOE associates Permission Sets to the user and then applies a Permission Set (which is the combination of the Permission Sets associated to the user). The applied Permission Set (a.k.a. session Permission Set) becomes the user's User Role. Control Panel applications (e.g., Email) use the user's session Permission Set to determine which of the application's functions should be allowed or disallowed for the user.

For IPsec users, the TOE uses the IPsec/Firewall to control access to the supported network service protocols. The IPsec/Firewall contains the IP addresses of authorized client computers grouped into address templates and the network service protocols grouped into service templates. The administrator maps an address template to a service template using an IPsec/Firewall rule. Service templates, therefore, act as the User Roles for IPsec users. IP addresses of computers not contained in a rule are denied access to the TOE.

3.4.4 Residual information protection

When the TOE deletes an object, the contents of the object are no longer available to TOE users. This prevents TOE users from attempting to recover deleted objects of other users via the TOE interfaces.

3.5 Protection of the TSF

Restricted forwarding of data to external interfaces

The TOE allows an administrator to enable / disable the forwarding of data received from an External Interface to the Shared-medium interface. In the evaluated configuration, the forwarding of data functionality is disabled.

3.5.1 TSF self-testing

The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of TSF functional tests (including system clock verification, LDAP settings verification, and Windows settings verification), TSF data integrity tests, and TSF code integrity tests.

3.5.2 Reliable timestamps

The TOE contains a system clock that is used to generate reliable timestamps. Only administrators can manage the system clock. The administrator can optionally configure the TOE to synchronize its system clock with a Network Time Protocol (NTP) server.

3.6 TOE access protection

3.6.1 Inactivity timeout

The TOE supports an inactivity timeout for Control Panel sign-in sessions. If a signed-in user is inactive for longer than the specified period of inactivity, the user is automatically signed out of the Control Panel by the TOE. The inactivity period is managed by the administrator via EWS (HTTP) or the Control Panel.

3.7 Trusted channel communication and certificate management

Shared-medium communications (i.e., Ethernet) between the TOE and other trusted IT products use a trusted channel mechanism to protect the communications from disclosure and modification. The TOE also ensures the cryptographic operations are validated during policy processing such as validating digital signatures or encrypting and decrypting data. IPsec with X.509v3 certificates is used to provide the trusted communication channels. The EWS (HTTP) allows administrators to manage X.509v3 certificates used by IPsec.

3.8 User and access management

The TOE supports the following roles:

- Administrators (U.ADMINISTRATOR)
- Users (U.NORMAL)

Administrators maintain and configure the TOE and Operational Environment. Users perform the standard scan function on the system.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.USER.TRAINING- TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

A.ADMIN.TRAINING- Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.

A.ADMIN.TRUST- Administrators do not use their privileged access rights for malicious purposes.

4.2 Environmental Assumptions

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

A.ACCESS.MANAGED - The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

A.ADMIN.PC.SECURE - The Administrative Computer is in a physically secured and managed environment and only the authorized administrator has access to it.

A.SERVICES.RELIABLE- When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, NTP, SMTP, SharePoint, syslog, and/or WINS, these services provide reliable information and responses to the TOE.

A.EMAILS.PROTECTED- For emails received by the SMTP gateway from the TOE, the transmission of emails between the SMTP gateway and the email’s destination is protected.

4.3 Clarification of Scope

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

T.DOC.DIS - User Document Data may be disclosed to unauthorized persons.

T.DOC.ALT- User Document Data may be altered by unauthorized persons.

T.FUNC.ALT- User Function Data may be altered by unauthorized persons.

T.PROT.ALT- TSF Protected Data may be altered by unauthorized persons.

T.CONF.DIS- TSF Confidential Data may be disclosed to unauthorized persons.

T.CONF.ALT- TSF Confidential Data may be altered by unauthorized persons.

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

P.USER.AUTHORIZATION - To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.

P.SOFTWARE.VERIFICATION - To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.

P.AUDIT.LOGGING - To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT - To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

P.ADMIN.PASSWORD - To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that it is required to perform security-relevant actions through the EWS and at the Control Panel.

P.USERNAME.CHARACTER_SET - To prevent ambiguous user names in the TOE's audit trail, the user names of the LDAP and Windows Sign In users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

P.REMOTE_PANEL.DISALLOWED - To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature.

5 Architectural Information

The TOE is the firmware of a scanner designed to be shared by many human users. It performs the functions of scanning documents. It can be connected to a wired local network through the embedded Jetdirect Inside's built-in Ethernet or to a USB device using its USB port (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 TOE protects all non-broadcast/non-multicast network communications with IPsec. Though IPsec supports multiple authentication methods, in the evaluated configuration, both ends of the IPsec connection are authenticated using X.509v3 certificates. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) into the TOE along with the CA certificate.

Because IPsec authenticates the computers (not 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 other trusted IT products 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.

The TOE also supports Microsoft SharePoint and remote file systems for the storing of scanned documents. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to SharePoint and the remote file systems. For remote file system connectivity, the TOE supports the FTP and SMB protocols.

The TOE can be used to email scanned documents. In addition, the TOE can send email alert messages to administrator-specified email addresses, or send automated emails regarding product configuration and HCD supplies to HP. The TOE supports protected communications between itself and SMTP gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate with the SMTP gateway. The TOE can only protect unencrypted emails up to the SMTP ateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email’s destination. Also, the TOE can only send emails; it does not accept inbound emails. Also, the TOE can only send emails; it does not accept inbound emails.

The TOE automatically synchronizes its system clock with an NTP server. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to the NTP server.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of a touchscreen LCD, and a physical home screen button that is attached to the HCD. In addition, all TOE models include a pull-out keyboard as part of the Control Panel. The Control Panel is the physical interface for a user 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

The following guidance documents are available:

- Common Criteria Evaluated Configuration Guide for HP Scanners HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner, Edition 1 [CCECG]
- HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide, Edition 3 [UG]
- HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide, Edition 1 [IG]

7 IT Product Testing

7.1 Developer Testing

Testing was performed by the developer at the HP site in Boise, Idaho, USA.

The testing was performed both automatically and manually.

The approach for testing was to provide at least one test case for each Security Functional Requirement mapped to the TOE security functionality documented in FSP. The developer also tested TSF subsystems

The developer reported that all tests were completed successfully, and the evaluator has examined the test evidence and verified that test results for the manual and automated test result to be consistent and clearly identified the outcome of the test action.

7.2 Evaluator Testing

The evaluators performed testing of the TOE at the developers site in Boise, US. The testing was performed between 2018-11-01 and 2018-11-08.

Testing was performed on the following models of the TOE:

HP ScanJet Enterprise Flow Yellowstone N9120 FN2 Flatbed Scanner

- All manual tests (except IPsec testing)
- All automated tests

HP Digital Sender Flow 8500 fn2 Arches Document Capture Workstation

- All manual tests (including IPsec testing)
- All automated tests

All tests performed by the evaluator were completed successfully.

7.3 Penetration Testing

Penetration testing was performed against the TOE interfaces that are accessible to a potential attacker, i.e., the IPv4 and IPv6 TCP and UDP ports of the TOE.

The results of the port scan indicate that only UDP port 500 (ISAKMP) is open, which is in line with the expected outcome.

8 Evaluated Configuration

The following components are required as part of the Operational Environment:

- The applicable scanner model for running the TOE firmware
- Domain Name System (DNS) server
- One administrative client computer connected to the TOE in the role of an Administrative Computer, which must contain a 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 components are optional in the Operational Environment:

- Microsoft SharePoint
- Network Time Protocol (NTP) server
- Remote file systems:
  - File Transfer Protocol (FTP)
  - Server Message Block (SMB)
- Simple Mail Transfer Protocol (SMTP) gateway

In the evaluated configuration the following requirements must be met:

- HP Digital Sending Software (DSS) must be disabled.
- Device Administrator Password must be set as per P.ADMIN.PASSWORD.
- Only one Administrative Computer is used to manage the TOE.
- Third-party solutions are not installed on the TOE.
- Device USB and Host USB plug and play must be disabled.
- Jetdirect Inside management via telnet and FTP must be disabled.
- Jetdirect XML Services must be disabled.
- IPsec authentication using X.509v3 certificates must be enabled (IPsec authentication using Kerberos or Pre-Shared Key is not supported).
- IPsec Authentication Headers (AH) must be disabled.
- Device Guest permission set's permissions must be configured to deny access (this disables the Guest role).
- SNMPv1/v2 and SNMPv3 must be disabled
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled.
- User names for the LDAP and Windows Sign In users must only contain the characters defined in P.USERNAME.CHARACTER_SET.
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.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).
- Access must be blocked to the following Web Services (WS):

  - Open Extensibility Platform device (OXPd) Web Services
  - WS* Web Services
- An IPv4 address must be statically assigned as per the instructions in TOE's configuration guidance [CCECG].
- Internet Fax and LAN Fax must be disabled.
- HP Jetdirect 2900Nw Print Server (HP product #: J8031A) must not be installed.

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 evaluator 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 Name / Assurance Family Name	*Short name*	*Verdict*
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Functional specification with complete summary	ADV_FSP.3	PASS
Architectural design	ADV_TDS.2	PASS
Guidance documents	AGD:	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Life-cycle support	ALC:	PASS
Authorisation controls	ALC_CMC.3	PASS
Implementation representation CM coverage	ALC_CMS.3	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Flaw reporting procedures	ALC_FLR.2	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
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

AH	Authentication Header (IPsec)
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
DNS	Domain Name System
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
EWS	Embedded Web Server
HCD	Hardcopy Device
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol (IPsec)
LCD	Liquid Crystal Display
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OXP	Open Extensibility Platform
OXPd	OXP device layer
PIN	Personal Identification Number
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
USB	Universal Serial Bus
WINS	Windows Internet Name Service
XML	Extensible Markup Language

12 Bibliography

ST	HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target, 2020-05-05, Version 1.6
CCECG	Common Criteria Evaluated Configuration Guide for HP Scanners HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner, 2019-05, Edition 1
UG	HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner User Guide, 2019-02-05, Edition 3
IG	HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Installation Guide, 2019-02-05, Edition 1,
PP2600.1	IEEE Std 2600.1-2009; "2600.1-PP, Protection Profile for Hard-copy Devices, Operational Environment A", Version 1.0 as of June 2009
PP2600.1-SCN	SFR Package for Hardcopy Device Scan Functions, Version 1.0 as of June 2009
PP2600.1-SMI	SFR Package for Hardcopy Device Shared-medium Inter-face Functions, Version 1.0 as of June 2009
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, 2019-09-24, document version 31.0

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 was received:

QMS 1.22.3 valid from 2019-05-20

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

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 1.23.2". The certifier concluded that, from QMS 1.22.3 to the current QMS 1.23.2, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification