Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti
ISO/IEC 15408 Common Criteria (CC) ver.3.1 rel. 5

Certificato n. *(Certificate No.)*	08/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/09/2025/RC, v. 1.0
Decorrenza *(Date of 1st Issue)*	9 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware
Sviluppatore *(Developer)*	HP Inc.
Tipo di Prodotto *(Type of Product)*	Dispositivi multifunzione (Multi-Function Devices)
Conformità a cPP *(cPP Conformance)*	collaborative Protection Profile for Hardcopy Devices; HCD-iTC. Version 1.0e

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 9 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware

OCSI/CERT/ATS/09/2025

Version 1.0

9 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	09/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AES	Advanced Encryption Standard
AESCBC	Advanced Encryption Standard-Cipher Block Chaining
AH	Authentication Headers
ARM	Advanced RISC Machine
ASIC	Application Specific Integrated Circuit
BLE	Bluetooth Low Energy
CBC	Cipher Block Chaining
CTR_DRBG	Counter (CTR) mode block cipher algorithm DRBG

DH	Diffie-Hellman
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EDK2	EFI Development Kit
ESP	Encapsulated Security Payload
EWS	Exchange Web Services
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
HCD	Hardcopy Device
HMAC	Hashed Message Authentication Codes
HMAC_DRBG	Hashed Message Authentication Code Deterministic Random Bit Generator
HTTP	HyperText Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
IT	Information Technology
KAS	Key Agreement Scheme
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LUKS	Linux Unified Key Setup
NFC	Near Field Communication
NTLM	New Technology LAN Manager
NTS	Network Time Service
OXPd	Open Extensibility Platform device
PIN	Personal Identification Number
PJL	Printer Job Language
PKCS	Public-Key Cryptography Standards
PS	Permission Set
RDP	Remote Desktop Protocol
REST	Representational State Transfer

ROM	Read-only memory
RSA	Rivest, Shamir, Adleman
SFP	Single Function Printer
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSS	Security Sub-System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface
USB	Universal Serial Bus
VTL	Virtual Test Laboratory
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WS	Web Services
XFRM	IP packet transformation package
XML	eXtensible Markup Language

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 – Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[CCECG] Common Criteria Evaluated Configuration Guide for HP Single-function Printers HP LaserJet Enterprise 8501, Edition 1, 1/2026.

[ETRv2] HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware, Version 2.0, 2025-12-11.

[ETRv3] HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware, Version 3.0, 2026-01-09.

[HCDcPP_v1.0E] collaborative Protection Profile for Hardcopy Devices; HCD-iTC. Version 1.0e 2024-03-04.

[SDM_HCDcPP] Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices Version 1.0e, 4 March 2024.

[ST] HP LaserJet Enterprise 8501 Security Target, Version 1.11, 2025-12-03.

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates conformant to collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate, conformant to a collaborative Protection Profile (cPP), is recognised under CCRA for all claimed assurance components up to and including EAL4 and ALC_FLR only.

6 Statement of Certification

The Target of Evaluation (TOE) is identified as follows "**HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware**", developed by HP Inc.

The TOE is a hardcopy device (HCD), also known as a single-function printer (SFP), including internal firmware, but exclusive of non-security relevant options such as finishers. The TOE also includes the English-language guidance documentation.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 for the assurance components included in the cPP [HCDcPP_v1.0E], according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the TOE “HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware ” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware
Security Target	HP LaserJet Enterprise 8501 Security Target, Version 1.11, 2025-12-03 [ST]
Evaluation Assurance Level	Conformant to cPP including the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1
Developer	HP Inc.
Sponsor	HP Inc.
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	collaborative Protection Profile for Hardcopy Devices; HCD-iTC. Version 1.0e [HCDcPP_v1.0E]
Evaluation starting date	21 February 2025
Evaluation ending date	11 December 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and, in the configuration shown in “Annex B – Evaluated configuration” of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The Target of Evaluation (TOE) is identified as follows "HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware".

The following firmware modules are included in the TOE:

- System firmware.
- Jetdirect Inside firmware.

Both firmware modules run on top of the same Linux 5.10 operating system.

The System firmware controls all functionality except for the network-related functionality and functionality implemented by the operating system. The Jetdirect Inside firmware controls the network-related functionality from Ethernet to Internet Key Exchange (IKE). These firmware modules and the operating system are bundled into a single installation bundle.

Several models of HCDs are included in this evaluation. Physically speaking, all models use the same ASIC and processor. All models contain one field-replaceable, nonvolatile storage device. They all have a Control Panel for operating the HCD locally and Ethernet network capability for connecting to a network. They all support the submission of print jobs over the network and remote administration over the network. The main physical differences between models are the number and size of paper feeders, print speed, the number of output bins, and whether they contain a stapler/stacker.

The Table 1 shows the HCD models included in the evaluation and the System firmware version.

Product model name	**Product number**	**Product model name (Name displayed in the EWS)**	**System firmware version**	**Jetdirect Inside firmware version**
HP LaserJet Enterprise 8501	9S187A	HP LaserJet 8501	2509306_000339	JOL25090252
	AJ7J3A			
	AQ1E4A			
	BD5H0A			
	BH6N7AV			

Table 1 - TOE hardware and firmware reference

For a detailed description of the TOE, consult sections 1.4 and 1.5 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE is designed to be shared by many client computers and human users. It performs the functions of printing and storing of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet, or to a USB device using its USB port (but the use of which must be disabled in the evaluated configuration except when the administrator performs trusted update via the USB).

[HCDcPP_v1.0E] defines the TOE's physical boundary as the entire HCD product with the possible exclusion of physical options and add-ons that are not security relevant. These exclusions include paper/media trays and feeders, document feeders, output bins, and printer stands.

Operating system and processor

The TOE's operating system is Linux 5.10 running on an ARM Cortex-A72 processor.

Networking

The TOE supports Local Area Network (LAN) capabilities. The LAN is used to communicate with client computers, the administrative computer, and several trusted IT entities. Some TOE models include support for Wireless LAN (WLAN), but the WLAN must be disabled in the evaluated configuration. The Linux operating system implements IPsec using its XFRM framework. The Jetdirect Inside firmware implements Internet Key Exchange version 2 (IKEv2) and supports X.509v3 certificate-based authentication. The TOE supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), although IPv6 is disabled in the evaluated configuration.

Administrative Computer and administrative interfaces

The Administrative Computer connects to the TOE using IPsec. This computer can administer the TOE using the following interfaces over the IPsec connection.

- Embedded Web Server (EWS)
- Representational state transfer (REST) Web Services

EWS

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.

REST Web Services

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

Administrative Computer and Network Client Computers

For design reasons, only one computer can be used as the Administrative Computer for the TOE in the evaluated configuration. This computer is used for administration of the TOE. All other client computers connecting to the TOE to perform non-administrative tasks are known as Network Client Computers in this ST.

Network Client Computers connect to the TOE to submit print jobs to the TOE using the Printer Job Language (PJL) interface. They can also receive job status from the TOE using PJL. The PJL interface connection is protected using IPsec.

PJL

The PJL interface is used by unauthenticated users via Network Client Computers to submit print jobs and receive job status (e.g., view the print queue). The unauthenticated users use PJL over an IPsec connection. It is also used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL over IPsec 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. For the purposes of this Certification Report, we define the PJL interface as PJL data sent to port 9100.

SMB

The TOE supports a remote file system for storing and retrieving backup files during Back up and Restore operations. The TOE uses IPsec to protect the communication to the remote file system. For remote file system connectivity, the TOE supports the SMB protocol

SMTP mail server

The TOE can send email alert messages to administrator-specified email addresses, mobile devices, or to a website. The TOE supports protected communications between itself and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec to protect the communication with the SMTP gateway. The TOE can only protect unencrypted email up to the SMTP gateway. 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.

Audit Server (syslog server)

The TOE supports the auditing of security-relevant functions by generating and forwarding audit records to an external syslog server. It supports both internal and external storage of audit records. The TOE uses IPsec to protect the communications between itself and the syslog server.

DNS, NTS, and WINS servers

The TOE requires a DNS server, an NTS server, and a WINS server in the Operational Environment. The TOE connects to the servers over an IPsec connection.

Control Panel

Each HCD contains a user interface (UI) called the Control Panel which consists of a touchscreen LCD. 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.

Internal and External Authentication

Note: The terms Internal Authentication and External Authentication start with a capitalized first character to match the [HCDcPP_v1.0E] usage of these terms.

The TOE supports the Local Device Sign In Internal Authentication mechanisms in the evaluated configuration. The TOE supports the LDAP Sign In and Windows Sign In (i.e., Kerberos) External Authentication mechanisms in the evaluated configuration.

The TOE's guidance documents and firmware refer to the following mechanisms as sign-in methods: Local Device Sign In, LDAP Sign In, and Windows Sign In. The Local Device Sign In method maintains the account information within the TOE. Only the Device Administrator account, which is an administrative account, is supported through this method in the evaluated configuration. The LDAP Sign In method supports the use of an external LDAP server for authentication. The Windows Sign In method supports the use of an external Windows Domain server for authentication.

Non-volatile Storage

All TOE models contain one field-replaceable nonvolatile storage device. This storage device is a self-encrypting Solid State Drive (SSD). The drive contains a section called **Job Storage** which is a user-visible file system where user document data, such as stored print, are located.

Firmware Components

The Jetdirect Inside firmware and System firmware components comprise the firmware on the system. Both of these firmware components share the same operating system (Linux 5.10). These firmware components and the operating system work together to provide the security functionality defined in this document for the TOE. The Jetdirect Inside firmware provides the network connectivity and network device drivers used by the System firmware. The Jetdirect Inside firmware includes IKE and the management functions for managing these network- related features. It also provides the network stack and drivers controlling the TOE's embedded Ethernet interface. The System firmware controls the overall functions of the TOE from the Control Panel to the storage device to print jobs. The operating system implements dm-verity, dm-crypt, IPsec, and includes the HP FutureSmart Firmware Linux Kernel Crypto API which implements cryptographic algorithms relied upon by TOE security functionality (e.g.., IPsec).

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, please refers to sections 1.5.3 and 7.1 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

7.3.2.1 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.

7.3.2.2 Data Encryption (a.k.a. cryptography)

IPsec

The TOE's IPsec supports X.509v3 certificates for authentication, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange version 2 (IKEv2) protocol, and the following cryptographic algorithms: Diffie-Hellman (DH), Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard-Cipher Block Chaining (AESCBC), Secure Hash Algorithm-based (SHA-based) Hashed Message Authentication Codes (HMACs), Public-Key Cryptography Standards (PKCS) #1 v1.5 signature generation and verification, counter mode deterministic random bit generator using AES (CTR_DRBG (AES)) for IKE negotiations, and HMAC_DRBG(HMAC-SHA2-256) deterministic random bit generator for IPsec ESP. It supports multiple DH groups, transport mode, and uses Main Mode for Phase 1 exchanges in IKEv2. IKEv2 uses the DH ephemeral (dhEphem) scheme to implement the key agreement scheme finite field cryptography (KAS FFC) algorithm when establishing a protected communication channel. DSA key generation is a prerequisite for KAS FFC when using DH ephemeral. IKEv2 uses imported RSA-based X.509v3 certificates to authenticate the connections.

The RSA authentication is accomplished using the IKEv2 digital signature authentication method.

Storage Encryption

The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an SSD. The TOE performs encryption of User Document Data and confidential TSF data on the SSD without any user intervention.

- Customer Data Encryption: The TSF implements a feature called customer data encryption, which encrypts the partitions on the storage device designated for customer data. In the evaluated configuration, this feature is configured to use AESCBC-256 to encrypt these partitions. Data stored on the customer data partitions includes stored jobs (e.g., print), temporary job files, PJL and PostScript filesystem files including downloaded fonts, and extensibility customer data (if stored there by the extensibility solution). On every HCD boot, the customer partitions (LUKS-encrypted volumes) are recreated and reformatted. This process effectively performs a cryptographic erase of all data previously stored on these partitions.
- Certificate Data Encryption. The TSF encrypts identity certificates, and their corresponding private keys stored on the storage device.
    - Certificates XML file: The TSF stores the IPsec identity certificate and its corresponding private key in encrypted form in a certificates XML file stored on the storage device. AES-CBC-256 is used to encrypt the IPsec identity certificate and its private key contained in the certificates XML file.
    - Thumbprint files: The TSF stores identity certificates and their corresponding private keys in individual files (a.k.a., thumbprint files) stored in encrypted form on the storage device. AES-CBC-256 is used to encrypt thumbprint files.

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 verify the authenticity of the signed update images. The TOE's EWS interface allows an administrator to verify and install the signed update images.

Digital signatures for TSF testing

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

Cryptographic implementations/modules

The TOE uses multiple cryptographic implementations to accomplish its cryptographic functions.

The following Table 2 provides the complete list of cryptographic implementations used to satisfy the [HCDcPP_v1.0E] cryptographic requirements.

Cryptographic implementation	Version	Usage
HP FutureSmart Firmware OpenSSL 1.1.1	5.9.2.1	Trusted update TSF testing Certificates XML file encryption Thumbprint files encryption RSA key pair generation during CSR creation
HP FutureSmart Firmware OpenSSL 1.1.1 (EDK2)	5.9.2.1	Secure boot
HP FutureSmart Firmware QuickSec 9.1 Cryptographic Module	5.9.2.1	IKE
HP FutureSmart Firmware Linux Kernel Crypto API	5.10	IPsec Customer data encryption TSF testing
Security Sub-System (SSS)	8.2	Secure boot

Table 2 - TOE cryptographic implementations

7.3.2.3 Identification, authentication, and authorization to use HCD functions

The following Table 3 shows the Internal and External Authentication mechanisms supported by the TOE in the evaluated configuration and maps the mechanisms to the interfaces that use them. The PJL interface does not appear in this table because the PJL interface does not perform authentication of users.

Authentication type	Mechanism name	Supported interfaces
Internal Authentication	Local Device Sign In	Control Panel, EWS, REST
External Authentication	LDAP Sign In	Control Panel, EWS
	Windows Sign In	Control Panel, EWS, REST

Table 3 - TOE authentication mechanisms and their supported interfaces

7.3.2.4 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.

The TOE contains one field-replaceable, nonvolatile storage device. This storage device is an SSD. The TSF ensures that confidential TSF Data and User Document Data stored on the drive is not stored as plaintext.

7.3.2.5 Trusted Communication

The TOE uses IPsec to protect the communications between the TOE and trusted IT entities as well as between the TOE and client computers. IPsec provides assured identification of the endpoints. It implements IKEv2 and transport mode. The TOE supports X.509v3 certificates for endpoint authentication.

7.3.2.6 Administrative roles

The TOE supports administrative and non-administrative roles. Assignment to these roles is controlled by the TOE's administrator. In the case of a user authenticated using an External Authentication mechanism (Windows Sign In and LDAP Sign In), the roles are implemented as permission sets. In the case of a user authenticated using an Internal Authentication mechanism (Local Device Sign In), only an administrative account exists. In addition, the TOE provides security management capabilities for TOE functions, TSF data, and security attributes as defined by the [ST].

7.3.2.7 Trusted operation

TOE firmware bundles can be downloaded from the HP Inc. website to update the TOE's firmware. These updates are digitally signed by HP Inc. using the RSA 2048-bit algorithm, SHA2-256 algorithm, and PKCS#1 v1.5 signature scheme. The TOE's EWS interface allows an administrator to install the firmware bundles. Before installation, the TSF verifies the digital signature of the firmware bundle to ensure its integrity and authenticity.

The TOE's secure boot function includes an immutable hardware root of trust implemented in ROM. When power is applied to the HCD, the boot ROM executes first and verifies the integrity of the initial boot stage, which resides outside the root of trust. Each subsequent stage in the boot process then validates the integrity of the next, establishing a continuous chain of trust. The integrity of each boot stage is verified by checking its digital signature using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5.

The TOE supports dm-verity to verify the integrity of SquashFS filesystem firmware images, helping ensure the correct operation of the TSF during startup. At each boot, the TSF verifies the digital signature of the dm-verity root hash corresponding to a SquashFS firmware image. During operation (including boot time), dm-verity checks the integrity of each filesystem block before loading it into memory by comparing it to the authenticated hash tree. The digital signature is verified using the RSA 2048-bit algorithm, SHA2-256, and PKCS#1 v1.5.

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.3 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims exact conformance to the following Protection Profile:

- collaborative Protection Profile for Hardcopy Devices; HCD-iTC. Version 1.0e, 2024-03-04 [HCDcPP_v1.0E].

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived by extension from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

Considering that the Security Target claims exact conformance to the collaborative Protection Profile for Hardcopy Devices [HCDcPP_v1.0E], all the SFRs from such cPP are included.

The security assurance requirements (SARs) for the TOE correspond to the following assurance components: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3], [NIS5] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM]. Furthermore, all specific assurance activities required by the collaborative Protection Profile for Hardcopy Devices [HCDcPP_v1.0E] have been carried out.

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security s.r.l.

The evaluation was completed on December 11th, 2025with the issuance by LVS of the Evaluation Technical Report [ETRv2], that has been approved by the Certification Body on December 22nd , 2025. A final version of the ETR was delivered by the LVS on 9 January 2026 [ETRv3] including some changes requested by the CB.

Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B – Evaluated configuration”.

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

Certification is not a guarantee that no vulnerabilities exist; there is a probability that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv2] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level defined by the SARs included in the cPP [HCDcPP_v1.0E], with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in “Annex B – Evaluated configuration”.

Table 4 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level defined by the SARs included in the cPP [HCDcPP_v1.0E].

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives for the operational environment	ASE_OBJ.1	Pass
Stated security requirements	ASE_REQ.1	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Test	**Class ATE**	Pass
Independent testing - conformance	ATE_IND.1	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability survey	AVA_VAN.1	Pass

Table 4 - Final verdicts for assurance requirements

8.2 Additional assurance activities

The collaborative Protection Profile for Hardcopy Devices [HCDcPP_v1.0E] includes additional assurance activities specific to the TOE technology type, and are required for exact conformance to the PP.

The Evaluators used for the cPP assurance activities a notation similar to assurance components of existing CC assurance classes. The objective of these sub-activities is to determine whether the requirements of the assurance activities included in the cPP are met.

Table 5 summarizes the final verdict of the cPP assurance activities carried out by the LVS.

cPP assurance activities[1]		**Verdict**
ASE: Security Target evaluation	ASE_HCDCPP.1	Pass
ADV: Development	ADV_HCDCPP.1	Pass
AGD: Guidance documents	AGD_HCDCPP.1	Pass
ATE: Tests	ATE_HCDCPP.1	Pass
AVA: Vulnerability assessment	AVA_HCDCPP.1	Pass
AEN: Entropy Description	AEN_HCDCPP.1	Pass
AKM: Key Management Description	AKM_HCDCPP.1	Pass

Table 5 - Final verdicts for cPP assurance activities

8.3 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the TOE "HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Assumptions and Organizational Security Policies described, respectively, in section 3.5 and 3.4 of the Security Target [ST] are complied.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, "Annex A – Guidelines for the secure usage of the product" includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG]).

[1] Activities with the _HCDCPP extension were entered by the lab to clearly organize the activities from the PP's "Assurance Activities" for each SFR and Appendixes E and F of the [HCDPP] and [SDM_HCDcPP].

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The firmware and guidance documentation are packaged in a single ZIP file and available for download from the HP SW Depot. The firmware is packaged in this ZIP file as a single firmware bundle which contains both the System firmware and the Jetdirect Inside firmware. The evaluated firmware versions have been already provided in Table 1.

The steps to perform download of the TOE files are provided in the following:

1. Request a username and password by sending an email to the following address: ccc-hp-enterprise-imaging-printing@hp.com.
2. Open the following URL in a web browser: https://h30670.www3.hp.com/portal/kiosk.
3. On the PPS KIOSK login page, enter the username and password obtained in step 1, then click Next.
4. Click the link for your printer in the **Tools, products, and technologies** section. An overview of the Common Criteria certification is displayed. Do not click **Request** at this point.
5. Click the **Installation** link. The **Installation** page containing information to securely download the .zip file containing the evaluated firmware and guidance documentation opens.
6. Confirm that the Installation page was downloaded securely by verifying the following:
   - The text in the URL field starts with https://
   - The host following the https:// prefix is within the hp.com domain.
   - A locked padlock icon is displayed by the web browser.
   - The web browser has not displayed any warnings related to the website’s certificate.

   Anything to the contrary indicates that the Installation page was not downloaded securely, in which case nothing on the page can be trusted. If the connection is secure, either save or print the **Installation** page. After downloading the .zip file, its integrity must be verified using the information in the **Installation** page.
7. After saving the **Installation** page, click **Request**. A sign in page opens.
8. If you have HP sign-in credentials, enter your username and password, then click **Sign In**. If you do not have HP sign-in credentials, click the **Don’t have an account? Sign up** link and complete the registration process. The **Product specifications** page opens after signing in.
9. Review and make any necessary changes in the **Customer Information** and **Address** sections.
10. Review and agree to the software license terms, then click **Next**. An electronic delivery receipt is sent to the email address associated with your HP account. The **Software downloads and licenses** page appears.
11. Click the **Download** link for the .zip file in the **Software** section.

In order to verify the integrity of the HP SW Depot download, there is a tool called DigitalVolcano Hash Tool (version 1.1.0.0) capable of generating SHA-256 hashes. The steps below were written specifically with the DigitalVolcano Hash Tool:

1. Launch the DigitalVolcano Hash Tool.
2. Select **SHA-256** from the **Hash Type** drop-down menu.
3. Click the **Select File(s)** button in the **Input Field** section and browse to the .zip file. The DigitalVolcano Hash Tool generates a SHA-256 hash of the .zip file and displays it in the area labeled **Last Hash**.
4. Visually compare the SHA-256 hash generated in the previous step with the SHA-256 hash contained in the **Installation** page from the HP SW Depot. If the hashes match, then the .zip file has not been compromised. If the hashes don't match, then either an error occurred during the download or the .zip file on the server is not the same as the original. Try downloading the .zip file again and repeat the verification steps. If on the successive attempt the hashes still do not match, and you are certain that the download proceeded without any issues, send an email to ccc-hp-enterprise-imaging-printing@hp.com describing the comparison failure.

The customer receives the hardware independent of the ZIP file. The evaluated hardware models, which are listed in Table 1, are either already on the customer's premise or must be obtained from HP. The user can use the following steps to verify that the TOE hardware has not been tampered with during the delivery:

- Inspect the cardboard box the TOE hardware was delivered in. Ensure the cardboard box contains the HP logo, has not been opened and resealed, the product information label is present, and no major physical damage exists.
- Inspect the contents of the cardboard box. Ensure all expected items have been delivered, the packaging the TOE hardware is contained in has not been tampered, and no missing or reapplied tape exists on the TOE hardware.

After that, the user can verify that the delivered TOE hardware is the correct model by taking the following steps:

- Verify the full product model name, serial number and product number in the order confirmation is consistent with the label on the cardboard box.
- Verify the invoice located in the cardboard box the TOE hardware was delivered in is consistent with the order confirmation.
- Verify the serial number and product number on the product label on the back of the TOE hardware is consistent with the order confirmation.

9.2 Identification of the TOE by the User

The TOE user can identify TOE components as described below:

- **Hardware**: The model name is marked on the front of the TOE hardware and the product number on the product label on the back.
- **Firmware**: The user can verify firmware version by checking the “Configuration Page” through the EWS administrative interface or using the Control Panel.
- **Guidance documentation**: the version number is printed in the documents.

9.3 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation shall be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

Namely, the Common Criteria Evaluated Configuration Guide for HP Single-function Printers HP LaserJet Enterprise 8501 [CCECG] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is identified as follows “HP LaserJet Enterprise 8501 printers with HP FutureSmart 5.9.2.1 Firmware”, developed by HP Inc.

The evaluated configuration of the TOE includes the hardware models and firmware versions listed in Table 1.

The physical boundary of the TOE is the physical boundary of the HCD product. Options and add-ons that are not security relevant, such as finishers, are not part of the evaluation but can be added to the TOE without any security implications.

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

- Only one Administrative Computer is used to manage the TOE.
- Third-party solutions must not be installed on the TOE.
- Device USB must be disabled.
- Host USB plug and play must be disabled.
- Firmware upgrades through any means other than the EWS (e.g., PJL) and USB must be disabled.
- HP Jetdirect XML Services must be disabled.
- External file system access through PJL and PS must be disabled.
- Only X.509v3 certificates are supported methods for IPsec authentication (IPsec authentication using pre-shared keys is not supported).
- IPsec Authentication Headers (AH) must be disabled.
- Control Panel Mandatory Sign-in must be enabled (this disables the Guest role).
- SNMP must be disabled.
- The Service PIN, used by a customer support engineer to access functions available to support personnel, must be disabled.
- Wireless functionality must be disabled:
    - Near Field Communication (NFC) must be disabled.
    - Bluetooth Low Energy (BLE) must be disabled.
    - Wireless Direct Print must be disabled.
    - Wireless station 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.
- Remote Control-Panel use is disallowed.
- Local Device Sign In accounts must not be created (i.e., only the built-in Device Administrator account is allowed as a Local Device Sign In account).
- Access must be blocked to the following Web Services (WS) using IPsec:

    - Open Extensibility Platform device (OXPd) Web Services.
    - WS* Web Services.
- Device Administrator Password must be set.
- Remote Configuration Password must not be set.
- OAUTH2 use is disallowed.
- SNMP over HTTP use is disallowed.
- HP Workpath Platform must be disabled.
- Licenses must not be installed to enable features beyond what is supported in the evaluated configuration.
- Firmware updates through REST Web Services is disallowed.
- PS privileged operators must be disabled.
- Cancel print jobs after unattended error must be enabled.
- FIPS-140 must be disabled.
- Partial clean functionality of the TOE is disallowed.
- Smart Cloud Print must be disabled.
- IPv6 addressing must be disabled.
- All stored jobs must be assigned a Job PIN or Job Encryption Password.

10.1 TOE operational environment

The following required components are part of the Operational Environment (refer also to section 1.4.1 of the Security Target [ST]):

- One administrative client computer network connected to the TOE in the role of an Administrative Computer.
- Web browser installed on the administrative client computer network connected to the TOE in the role of an Administrative Computer.
- A Domain Name System (DNS) server.
- A Network Time Service (NTS) server.
- A Windows Internet Name Service (WINS) server.
- A Syslog server.
- One or both of the following:
    - A Lightweight Directory Access Protocol (LDAP) server.
    - A Windows domain controller/Kerberos server.
- At least one OCSP responder capable of processing OCSP requests originating from the TOE.

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).
- The following remote file systems:
  - Server Message Block (SMB).
- A Simple Mail Transfer Protocol (SMTP) gateway.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level defined by the SARs included in the cPP [HCDcPP_v1.0E], such activities do not require the execution of functional tests by the Developer, but only independent functional tests and penetration tests by the Evaluators.

11.1 Test configuration

All testing activities have been carried out remotely from the LVS premises on the Virtual Test Laboratory (VTL) located at the Developer site in Boise, Idaho, USA. The Evaluators used this documentation as the basis for testing, and found it to be consistent with the [CCECG] and [ST].

The Evaluators performed testing remotely by connecting to the test environment using Microsoft Remote Desktop (RDP) and the communication was protected using TLSv1.2.

Before starting the test activities, the Evaluators verified that the hash of the bundle files installed on the TOE matched with the SHA-256 hash included in [CCECG].

The [ST] claims conformance to the collaborative Protection Profile [HCDcPP_v1.0E] which defines test cases mapped to SFRs. The Evaluators performed both automated and manual test cases to fulfil the required tests, thereby also fulfilling the requirements for ATE_IND.1.

All remote test activities have been carried out in accordance with the instructions provided by the Italian Certification Body in the Scheme Information Note 5/23 - Conditions for performing tests remotely in Common Criteria evaluations [NIS5].

11.2 Functional and independent tests performed by the Evaluators

The Security Target [ST] claims exact conformance to the cPP [HCDcPP_v1.0E], which defines test cases mapped to SFRs. The Evaluators performed both automated and manual test cases to fulfil the required tests, thereby also fulfilling the requirements for ATE_IND.1.

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly according to the [CCECG]. They also verified that the test environment had been correctly prepared by the Developer.

Model in Table 6 was tested.

TOE model name	System firmware version	Jetdirect Inside Firmware Version
HP LaserJet Enterprise 8501	2509306_000339	JOL25090252

Table 6 - TOE model tested

The Evaluators, for each SFR declared in the [ST], has performed all tests required by the [HCDcPP_v1.0E] and Technical Decisions listed in section 2.1.1 of [ST].

11.3 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same Virtual Test Laboratory (VTL) and the same TOE models already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

Since an attack requires an attack surface, the Evaluators decided to start by examining if the TOE exposes such interfaces, i.e., open ports.

Port scans were performed against the TOE interfaces that are accessible to a potential attacker (IPv4 UDP and TCP ports of the TOE). The Evaluators determined that only UDP port 500 (ISAKMP) is available outside of IPsec which was the expected outcome. Moreover, the Evaluators performed additional tests on the UDP 500 port used by IPsec, by sending malformed packets to it. No logs were observed and there were no unexpected behaviours as a result of these additional penetration tests.

The Evaluators, based on search result, compiled a table of potentially applicable public vulnerabilities: based on the analysis, the Evaluators determined there are no potential vulnerabilities in the TOE.

The Evaluators could then conclude that the TOE is resistant to an attack potential of level basic in its intended operational environment. No exploitable or residual vulnerabilities have been identified.