



Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione



Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 7/21

(Certification No.)

Prodotto: HP Digital Sender Flow 8500 fn2 Document Capture Workstation
(Product) and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner
with HP FutureSmart 4.11.0.1 Firmware

Sviluppato da: HP, Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard
ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

*The product identified in this certificate complies with the requirements of the standard
ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:*

Conforme a: Protection Profile for Hardcopy Devices v1.0 +Errata #1

(Conformant to)

(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)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 23 settembre 2021



Questa pagina è lasciata intenzionalmente vuota



Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione



Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

**HP Digital Sender Flow 8500 fn2 Document Capture Workstation
and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner
with HP FutureSmart 4.11.0.1 Firmware**

OCSI/CERT/ATS/13/2020/RC

Versione 1.0

23 settembre 2021

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

| Versione | Autori | Modifiche | Data |
|----------|--------|-----------------|------------|
| 1.0 | OCSI | Prima emissione | 23/09/2021 |
| | | | |

2 Indice

| | | |
|-------|--|----|
| 1 | Revisioni del documento | 5 |
| 2 | Indice..... | 6 |
| 3 | Elenco degli acronimi | 8 |
| 4 | Riferimenti..... | 11 |
| 4.1 | Criteri e normative | 11 |
| 4.2 | Documenti tecnici | 12 |
| 5 | Riconoscimento del certificato | 13 |
| 5.1 | Riconoscimento di certificati CC in ambito internazionale (CCRA) | 13 |
| 6 | Dichiarazione di certificazione..... | 14 |
| 7 | Riepilogo della valutazione | 15 |
| 7.1 | Introduzione..... | 15 |
| 7.2 | Identificazione sintetica della certificazione..... | 15 |
| 7.3 | Prodotto valutato | 16 |
| 7.3.1 | Architettura dell'ODV..... | 16 |
| 7.3.2 | Caratteristiche di sicurezza dell'ODV | 18 |
| 7.4 | Documentazione | 20 |
| 7.5 | Conformità a Profili di Protezione | 21 |
| 7.6 | Requisiti funzionali e di garanzia | 21 |
| 7.7 | Conduzione della valutazione | 21 |
| 7.8 | Considerazioni generali sulla validità della certificazione | 21 |
| 8 | Esito della valutazione..... | 23 |
| 8.1 | Risultato della valutazione | 23 |
| 8.2 | Attività di garanzia aggiuntive | 24 |
| 8.3 | Raccomandazioni..... | 24 |
| 9 | Appendice A – Indicazioni per l'uso sicuro del prodotto..... | 26 |
| 9.1 | Consegna dell'ODV..... | 26 |
| 9.2 | Identificazione dell'ODV | 26 |
| 9.3 | Installazione, inizializzazione e utilizzo sicuro dell'ODV | 27 |
| 10 | Appendice B – Configurazione valutata..... | 28 |
| 10.1 | Ambiente operativo dell'ODV | 29 |

| | | |
|------|---|----|
| 11 | Appendice C – Attività di test | 31 |
| 11.1 | Configurazione per i test | 31 |
| 11.2 | Test funzionali ed indipendenti svolti dai Valutatori | 31 |
| 11.3 | Analisi delle vulnerabilità e test di intrusione..... | 32 |

3 Elenco degli acronimi

| | |
|---------------|---|
| AES | Advanced Encryption Standard |
| AH | Authentication Headers |
| BEV | Border Encryption Value |
| BLE | Bluetooth Low Energy |
| CBC | Cipher Block Chaining |
| CC | Common Criteria |
| CCRA | Common Criteria Recognition Arrangement |
| CEM | Common Evaluation Methodology |
| DH | Diffie-Hellman |
| DNS | Domain Name System |
| DPCM | Decreto del Presidente del Consiglio dei Ministri |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| EAL | Evaluation Assurance Level |
| ECB | Electronic CodeBook |
| ECDH | Elliptic-curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| ESP | Encapsulating Security Payload |
| EWS | Exchange Web Services |
| FIPS | Federal Information Processing Standards |
| FTP | File Transfer Protocol |
| HCD | Hardcopy Device |
| HMAC | Keyed-Hash Message Authentication Code |
| HTTP | HyperText Transfer Protocol |

| | |
|---------------|---|
| HTTPS | HTTP over Secure Socket Layer |
| IKE | Internet Key Exchange |
| IPsec | Internet Protocol Security |
| ISAKMP | Internet Security Association and Key Management Protocol |
| IT | Information Technology |
| LAN | Local Area Network |
| LCD | Liquid Crystal Display |
| LDAP | Lightweight Directory Access Protocol |
| LGP | Linea Guida Provvisoria |
| LVS | Laboratorio per la Valutazione della Sicurezza |
| NFC | Near Field Communication |
| NIAP | National Information Assurance Partnership |
| NIS | Nota Informativa dello Schema |
| NTLM | New Technology LAN Manager |
| NTS | Network Time Service |
| OCSI | Organismo di Certificazione della Sicurezza Informatica |
| ODV | Oggetto della Valutazione |
| XPd | Open Extensibility Platform device |
| PIN | Personal Identification Number |
| PKCS | Public-Key Cryptography Standards |
| PP | Protection Profile |
| PSK | Pre-shared Key |
| RDP | Remote Desktop Protocol |
| REST | Representational State Transfer |
| RFV | Rapporto Finale di Valutazione |
| RSA | Rivest, Shamir, Adleman |
| SAR | Security Assurance Requirement |

| | |
|-------------|------------------------------------|
| SED | Self-encrypting Drive |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| TCP | Transmission Control Protocol |
| TDS | Traguardo di Sicurezza |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| 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 |
| XML | eXtensible Markup Language |

4 Riferimenti

4.1 Criteri e normative

- [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. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013
- [NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013
- [NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[NIS120] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/20 – Condizioni per l’effettuazione di test da remoto in valutazioni Common Criteria, versione 1.0, 6 aprile 2020

4.2 Documenti tecnici

[CCECG] “Common Criteria Evaluated Configuration Guide for HP Document Scanners HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner”, Edition 1, HP Inc., May 2021

[HCDPP] Protection Profile for Hardcopy Devices, IPA, NIAP, and the MFP Technical Community, Version 1.0, 10 September 2015

[HCDPP-ERR] Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

[RFV] Final Evaluation Technical Report “HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware”, Version 1, atsec information security S.r.l., 3 September 2021

[TDS] “HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target”, Version 1.2, HP Inc., 24 August 2021

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su <https://www.commoncriteriaportal.org/>.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware", sviluppato dalla società HP, Inc.

L'ODV è un'apparecchiatura per l'acquisizione di documenti cartacei (*hardcopy device* o HCD), chiamata anche scanner, che include il firmware interno, ma esclude opzioni non rilevanti per la sicurezza come i fascicolatori. L'ODV include anche la documentazione di guida in lingua inglese.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per i componenti di garanzia inclusi nel PP [HCDPP], in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

| | |
|---|--|
| Nome dell'ODV | HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware |
| Traguardo di Sicurezza | "HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target", Version 1.2 [TDS] |
| Livello di garanzia | Conforme a PP con i seguenti componenti di garanzia: 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 e AVA_VAN.1 |
| Fornitore | HP, Inc. |
| Committente | HP, Inc. |
| LVS | atsec information security S.r.l. |
| Versione dei CC | 3.1 Rev. 5 |
| Conformità a PP | Protection Profile for Hardcopy Devices v1.0 [HCDPP] integrato da Errata#1 [HCDPP-ERR] |
| Data di inizio della valutazione | 17 dicembre 2020 |
| Data di fine della valutazione | 3 settembre 2021 |

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware", composto dai seguenti elementi:

- HP Digital Sender Flow 8500 fn2 Document Capture Workstation;
- HP ScanJet Enterprise Flow N9120 fn2 Document Scanner;
- Documentazione di guida.

L'ODV include i seguenti moduli firmware:

- Jetdirect Inside;
- firmware di Sistema.

Tutti i modelli dell'ODV utilizzano il firmware Jetdirect Inside versione JSI24110014.

L'ODV include le seguenti versioni del firmware di Sistema:

1. 2411097_060492
2. 2411097_060482

La Tabella 1 mostra i modelli di HCD inclusi nella valutazione con la corrispondente versione del firmware di Sistema installato.

| Famiglia di prodotti | Modello | Numero prodotto | Codici opzione | Versione firmware di Sistema |
|----------------------------|---------------------------------------|-----------------|----------------|------------------------------|
| HP ScanJet Enterprise Flow | N9120 fn2 Document Scanner | L2763A | #201 | 2411097_060492 |
| HP Digital Sender Flow | 8500 fn2 Document Capture Workstation | L2762A | #201 | 2411097_060482 |

Tabella 1 – Elenco dei componenti hardware dell'ODV con rispettivo firmware di Sistema

Per una descrizione dettagliata dell'ODV, si faccia riferimento al par. 1.4 e al par. 1.5 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV è progettato per essere condiviso da un gran numero di utenti umani. L'ODV fornisce funzionalità di scansione di documenti e può essere collegato a una rete locale tramite la Ethernet integrata in Jetdirect Inside o a un dispositivo USB esterno mediante la

porta USB in dotazione (l'uso della porta USB deve essere disabilitato nella configurazione valutata, tranne quando l'amministratore esegue l'aggiornamento sicuro tramite USB).

Il sistema operativo dell'ODV è Windows Embedded CE 6.0 R3 in esecuzione su un processore Arm Cortex-A8.

L'ODV supporta le funzionalità di rete locale (LAN). La LAN viene utilizzata per comunicare con il computer amministrativo (Administrative Computer) e diverse entità IT attendibili. Alcuni modelli dell'ODV includono il supporto per reti locali wireless (WLAN), ma la funzionalità WLAN deve essere disabilitata nella configurazione valutata. L'ODV protegge tutte le comunicazioni di rete con IPsec, che fa parte del firmware Jetdirect Inside. L'ODV implementa Internet Key Exchange versione 1 (IKEv1) e supporta sia l'autenticazione con chiave pre-condivisa (PSK), sia l'autenticazione basata su certificato X.509v3. L'ODV supporta Internet Protocol version 4 (IPv4) e Internet Protocol version 6 (IPv6).

L'Administrative Computer si connette all'ODV utilizzando IPsec. Questo computer può amministrare l'ODV utilizzando le seguenti interfacce tramite la connessione IPsec:

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

L'interfaccia amministrativa EWS basata su HTTP consente agli amministratori di gestire in remoto le funzionalità dell'ODV utilizzando un browser Web. Questa interfaccia è protetta tramite IPsec.

Le interfacce dei Web Service (WS) consentono agli amministratori di gestire esternamente l'ODV. La configurazione valutata supporta solo l'interfaccia REST Web Services. L'interfaccia REST Web Services è protetta tramite IPsec.

Per motivi di progettazione, nella configurazione valutata è possibile utilizzare un solo computer come Administrative Computer per l'ODV. Questo computer viene utilizzato per l'amministrazione dell'ODV.

L'ODV supporta Microsoft SharePoint e *file system* remoti per l'archiviazione dei documenti scansionati. L'ODV utilizza IPsec per proteggere la comunicazione con SharePoint e con i *file system* remoti. Per la connessione con i *file system* remoti l'ODV supporta i protocolli FTP e SMB (SharePoint si basa su HTTP, ma le comunicazioni HTTP sono protette tramite IPsec).

L'ODV può inviare i documenti scansionati via Email. Inoltre, l'ODV può inviare messaggi di avviso via Email ad indirizzi Email specificati dall'amministratore o inviare Email automatizzate ad HP relative alla configurazione del prodotto e ai materiali di consumo dell'HCD. L'ODV protegge le comunicazioni con i gateway SMTP (Simple Mail Transfer Protocol) mediante IPsec. L'ODV può solamente proteggere Email non cifrate fino al gateway SMTP. È responsabilità dell'ambiente operativo proteggere le Email dal gateway SMTP fino alla destinazione. Inoltre, l'ODV può solo inviare Email e non accetta Email in ingresso.

L'ODV supporta l'audit delle funzioni rilevanti per la sicurezza generando e inoltrando i record di audit a un server *syslog* esterno. L'ODV supporta l'archiviazione interna ed esterna dei record di audit. La comunicazione con il server *syslog* è protetta tramite IPsec.

L'ODV richiede un server DNS, un server NTS e un server WINS nell'ambiente operativo. L'ODV si connette a questi server tramite una connessione IPsec.

Ogni HCD implementa un'interfaccia utente (UI) chiamata Pannello di Controllo, costituita da uno schermo tattile LCD, un pulsante fisico per la schermata iniziale e una tastiera a scomparsa. Il Pannello di Controllo è l'interfaccia fisica che l'utente usa per comunicare con l'ODV quando utilizza fisicamente l'HCD. Lo schermo LCD mostra all'utente informazioni quali menu e stato e fornisce anche pulsanti virtuali come ad es. una tastiera alfanumerica per l'immissione di nomi utente e password. Al Pannello di Controllo possono accedere sia gli utenti amministrativi, sia quelli non amministrativi.

L'ODV supporta sia meccanismi di autenticazione interna (Local Device Sign In), sia meccanismi di autenticazione esterna (LDAP Sign In e Windows Sign In, cioè Kerberos).

Tutti i modelli dell'ODV contengono un dispositivo di archiviazione non volatile sostituibile sul campo. Questo dispositivo è un'unità disco con crittografia automatica (SED) validata FIPS 140-2.

Il firmware dell'ODV comprende i componenti Jetdirect Inside e il firmware di Sistema. I due componenti firmware insieme forniscono le funzionalità di sicurezza dell'ODV. Questi componenti sono separati ma condividono entrambi lo stesso sistema operativo. Il sistema operativo fa parte del firmware di Sistema.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit:** l'ODV supporta l'archiviazione interna ed esterna dei record di audit. La configurazione valutata richiede l'uso di un server *syslog* per l'archiviazione esterna dei record di audit. La connessione tra l'ODV e il server *syslog* è protetta tramite IPsec. L'ODV non consente alcun accesso non autorizzato ai record di audit.
- **Cifratura dei dati (funzioni crittografiche):**
 - **IPsec:** l'implementazione di IPsec dell'ODV supporta chiavi pre-condivise (PSK) e certificati X.509v3 per l'autenticazione, i protocolli Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP) e Internet Key Exchange version 1 (IKEv1) e i seguenti algoritmi crittografici e lunghezze di chiavi: DH (P=2048, SHA2-256), DSA (L=2048, N=224; L=2048, N=256; L=3072, N=256), ECDH (P-256, SHA2-256; P-384, SHA2-384; P521, SHA2-512), ECDSA (P-256, P-384, P-521), RSA (2048 e 3072 bit), AES-CBC (128 e 256 bit), AES-ECB (256 bit), SHA-

1, SHA2-256, SHA2-384, SHA2-512, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 e HMAC-SHA2-512.

- **Drive-lock password:** per l'archiviazione sicura, tutti i modelli dell'ODV contengono un dispositivo di archiviazione non volatile sostituibile sul campo. Questo dispositivo di archiviazione è un'unità SED (Self-Encrypting Drive) basata su disco validata FIPS 140-2. L'unità SED dell'ODV utilizza una *drive-lock password* (password di blocco unità) a 256 bit come BEV (Border Encryption Value) che viene utilizzato per sbloccare i dati sull'unità. Il BEV viene generato dall'ODV utilizzando un algoritmo CTR_DRBG(AES-256) e viene memorizzato come una catena di chiavi di un solo elemento in una memoria non volatile e non sostituibile sul campo (una EEPROM) situata all'interno dell'ODV. L'algoritmo CTR_DRBG(AES-256) utilizza l'algoritmo Advanced Encryption Standard-Counter (AES-CTR).
- **Firme digitali per aggiornamenti sicuri:** per verificare l'autenticità dei file immagine di aggiornamento firmati, l'ODV utilizza firme digitali basate sull'algoritmo RSA a 2048 bit, SHA2-256 e PKCS#1 v1.5.
- **Firme digitali per il test del TSF:** l'ODV utilizza le firme digitali come parte della sua funzionalità di test del TSF.
- **Implementazioni crittografiche:** l'ODV utilizza diverse implementazioni crittografiche per svolgere le sue funzioni crittografiche. La tabella seguente fornisce l'elenco completo delle implementazioni crittografiche mappate sui componenti del firmware:

| Comp. firmware | Implementazione crittografica | Utilizzo |
|---------------------------|--|---|
| Firmware Jetdirect Inside | HP FutureSmart OpenSSL FIPS Object Module 2.0.4 | Generazione della Drive-lock password (BEV) |
| | HP FutureSmart QuickSec 5.1 | IPsec |
| Firmware di Sistema | HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 | Test del TSF |
| | HP FutureSmart Rebex Total Pack 2017 R1 2470159 | Aggiornamenti sicuri |

- **Identificazione, autenticazione e autorizzazione all'uso delle funzioni degli HCD:** la tabella seguente elenca i meccanismi di autenticazione interna ed esterna supportati dall'ODV nella configurazione valutata, mappati sulle interfacce che li utilizzano:

| Tipo di autenticazione | Meccanismo | Interfacce supportate |
|------------------------|----------------------|----------------------------------|
| Autenticazione interna | Local Device Sign In | Pannello di Controllo, EWS, REST |
| Autenticazione esterna | LDAP Sign In | Pannello di Controllo, EWS |
| | Windows Sign In | Pannello di Controllo, EWS, REST |

- **Controllo di accesso:** l'ODV applica il controllo di accesso sui dati del TSF e sui dati d'utente. Ad ogni elemento dei dati utente viene assegnato un proprietario e l'accesso ai dati è limitato dal meccanismo di controllo di accesso. Gli insiemi di permessi utilizzati per definire i ruoli influiscono anche sul controllo di accesso di ciascun utente. L'ODV contiene un SED validato FIPS 140-2 sostituibile sul campo. Insieme alla *drive-lock password*, il SED garantisce che i dati del TSF e i dati d'utente sull'unità non vengano memorizzati come testo in chiaro sul dispositivo di archiviazione.
- **Image Overwrite:** L'ODV supporta anche la funzione opzionale Image Overwrite definita nel PP [HCDPP]. Il PP limita l'ambito di questa funzione al dispositivo di archiviazione non volatile sostituibile sul campo.
- **Comunicazioni sicure:** l'ODV utilizza IPsec per proteggere le comunicazioni tra l'ODV e le entità IT attendibili, nonché tra l'ODV e i computer client. IPsec fornisce l'identificazione certa degli *endpoint* e implementa IKEv1 e la modalità di trasporto. L'ODV supporta anche i certificati X.509v3 e le chiavi pre-condivise (PSK) per l'autenticazione degli *endpoint*.
- **Ruoli amministrativi:** l'ODV supporta ruoli amministrativi e non amministrativi. L'assegnazione a questi ruoli è controllata dall'amministratore dell'ODV. Nel caso di un utente autenticato mediante un meccanismo di autenticazione esterno (Windows Sign In e LDAP Sign In), i ruoli vengono implementati come insiemi di permessi. Nel caso di un utente autenticato usando un meccanismo di autenticazione interno (Local Device Sign In), esiste solo un account di amministratore.
- **Operatività sicura:** gli aggiornamenti dell'ODV possono essere scaricati dal sito Web di HP Inc. Gli aggiornamenti sono firmati digitalmente da HP Inc. utilizzando l'algoritmo RSA a 2048 bit, SHA2-256 e la generazione della firma secondo la specifica PKCS#1 v1.5. L'interfaccia EWS dell'ODV consente ad un amministratore di installare i file immagine degli aggiornamenti. Prima di consentire l'installazione dell'immagine di un aggiornamento, l'ODV ne convalida la firma digitale. L'ODV implementa la funzionalità di test del TSF denominata Whitelisting per garantire che solo file del firmware di Sistema autentici e non manomessi vengano caricati in memoria. La funzione di Whitelisting utilizza firme digitali basate sull'algoritmo RSA a 2048 bit, SHA2-256 e PKCS#1 v1.5 per convalidare i file del firmware.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.3 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* ai seguenti Profili di Protezione:

- Protection Profile for Hardcopy Devices, Version 1.0 [HCDPP]
- Protection Profile for Hardcopy Devices – v1.0 Errata #1 [HCDPP-ERR]

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

Considerando che il TDS dichiara conformità *exact* al PP [HCDPP], sono inclusi anche tutti gli SFR di tale PP.

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM]. Inoltre, sono state eseguite tutte le attività di garanzia specifiche richieste dal PP [HCDPP].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS atsec information security S.r.l.

L'attività di valutazione è terminata in data 3 settembre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 16 settembre 2021. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è

stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS atsec information security S.r.l. e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia definito dai SAR inclusi nel PP [HCDPP], in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 2 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia definito dai SAR inclusi nel PP [HCDPP].

| Classi e componenti di garanzia | | Verdetto |
|---|-------------------|----------|
| Security Target evaluation | Classe ASE | Positivo |
| Conformance claims | ASE_CCL.1 | Positivo |
| Extended components definition | ASE_ECD.1 | Positivo |
| ST introduction | ASE_INT.1 | Positivo |
| Security objectives for the operational environment | ASE_OBJ.1 | Positivo |
| Stated security requirements | ASE_REQ.1 | Positivo |
| Security problem definition | ASE_SPD.1 | Positivo |
| TOE summary specification | ASE_TSS.1 | Positivo |
| Development | Classe ADV | Positivo |
| Basic functional specification | ADV_FSP.1 | Positivo |
| Guidance documents | Classe AGD | Positivo |
| Operational user guidance | AGD_OPE.1 | Positivo |
| Preparative procedures | AGD_PRE.1 | Positivo |
| Life cycle support | Classe ALC | Positivo |
| Labelling of the TOE | ALC_CMC.1 | Positivo |
| TOE CM coverage | ALC_CMS.1 | Positivo |
| Test | Classe ATE | Positivo |
| Independent testing - conformance | ATE_IND.1 | Positivo |
| Vulnerability assessment | Classe AVA | Positivo |

| Classi e componenti di garanzia | | Verdetto |
|---------------------------------|-----------|----------|
| Vulnerability survey | AVA_VAN.1 | Positivo |

Tabella 2 - Verdetti finali per i requisiti di garanzia

8.2 Attività di garanzia aggiuntive

Il PP [HCDPP] include attività di garanzia aggiuntive che sono specifiche per il tipo di tecnologia dell'ODV e sono richieste per la conformità *exact* al PP.

I Valutatori hanno utilizzato per le attività di garanzia del PP una notazione simile a quella dei componenti delle classi di garanzia CC esistenti. L'obiettivo di queste sotto-attività è quello di determinare se sono soddisfatti tutti i requisiti delle attività di garanzia incluse nel PP.

La Tabella 3 riassume i verdetti finali di ciascuna attività di garanzia del PP svolta dall'LVS.

| Attività di garanzia del PP | | Verdetto |
|--|-------------|----------|
| ASE: Security Target evaluation | ASE_HCDPP.1 | Positivo |
| AGD: Guidance documents | AGD_HCDPP.1 | Positivo |
| ALC: Life cycle support | ALC_HCDPP.1 | Positivo |
| ATE: Tests | ATE_HCDPP.1 | Positivo |
| AVA: Vulnerability assessment | AVA_HCDPP.1 | Positivo |
| AEN: Entropy Description | AEN_HCDPP.1 | Positivo |
| AKM: Key Management Description | AKM_HCDPP.1 | Positivo |

Tabella 3 - Verdetti finali per le attività di garanzia del PP

8.3 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel cap. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi e le Politiche di sicurezza organizzative descritte rispettivamente nel par. 3.2 e nel par. 3.3 del [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse una serie di raccomandazioni relative alla consegna, all'inizializzazione, alla configurazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([CCECG]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

Il firmware e la documentazione di guida sono contenuti in un unico file ZIP e possono essere scaricati dal sito Web di HP Inc. Il firmware è inserito in questo file ZIP sotto forma di un unico pacchetto contenente sia il firmware di Sistema, sia il firmware Jetdirect Inside. Le versioni del firmware valutate sono elencate in Tabella 1.

Per scaricare il file ZIP, il cliente deve registrarsi con HP ed effettuare il login su un sito Web protetto (HTTPS) per accedere alla pagina di download. Il cliente può ricevere le credenziali di accesso inviando un'Email a ccc-hp-enterprise-imaging-printing@hp.com. Sul sito di download viene fornito un *checksum* SHA-256 insieme alle istruzioni su come utilizzarlo per la verifica dell'integrità del pacchetto scaricato.

Il cliente riceve l'hardware indipendentemente dal file ZIP. I modelli hardware valutati, elencati in Tabella 1, si trovano già in possesso del cliente o devono essere ottenuti da HP. L'utente può utilizzare i seguenti passaggi per verificare che l'hardware dell'ODV non sia stato manomesso durante la consegna:

- Ispezionare la scatola di cartone in cui è stato consegnato l'hardware dell'ODV. Assicurarsi che la scatola di cartone contenga il logo HP, non sia stata aperta e richiusa, sia corredata dell'etichetta informativa del prodotto e che non siano presenti danni fisici di rilievo.
- Ispezionare il contenuto della scatola di cartone. Assicurarsi che tutti gli articoli previsti siano stati consegnati, che l'imballaggio che contiene l'hardware dell'ODV non sia stato manomesso e che sull'hardware dell'ODV non vi sia alcun nastro mancante o riapplicato.

Successivamente, l'utente può verificare che l'hardware dell'ODV consegnato sia il modello corretto procedendo come segue:

- Verificare che il nome completo del modello, il numero di serie e il codice del prodotto indicati nella conferma dell'ordine corrispondano con quelli dell'etichetta sulla scatola di cartone.
- Verificare che la fattura che si trova nella scatola di cartone in cui è stato consegnato l'hardware dell'ODV sia coerente con la conferma dell'ordine.
- Verificare che il numero di serie e il codice del prodotto indicati sull'etichetta del prodotto sul retro dell'hardware dell'ODV siano coerenti con la conferma dell'ordine.

9.2 Identificazione dell'ODV

L'utente può identificare i componenti dell'ODV come descritto di seguito:

- **Hardware:** il nome del modello è contrassegnato sulla parte anteriore dell'hardware dell'ODV e il numero del prodotto sull'etichetta del prodotto sulla parte posteriore.
- **Firmware:** l'utente può verificare la versione del firmware controllando la sezione "Configuration Page" tramite l'interfaccia amministratore EWS o utilizzando il Pannello di Controllo.
- **Documentazione di guida:** il numero di versione è stampato nei documenti.

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, il documento Common Criteria Evaluated Configuration Guide for HP Document Scanners [CCECG] contiene informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

Il Fornitore mette altresì a disposizione guide d'utente specifiche per i modelli di stampante valutati. Questi documenti aggiuntivi sono elencati nella Tabella 1-2 ("User guides") e nella Tabella 1-3 ("Hardware installation guides") di [CCECG].

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "HP Digital Sender Flow 8500 fn2 Document Capture Workstation and HP ScanJet Enterprise Flow N9120 fn2 Document Scanner with HP FutureSmart 4.11.0.1 Firmware", sviluppato da HP, Inc.

La configurazione valutata dell'ODV comprende i modelli hardware e le versioni del firmware elencate nel par. 7.3.

Il confine fisico dell'ODV è il confine fisico del prodotto HCD. Le opzioni e i componenti aggiuntivi che non sono rilevanti per la sicurezza, come i fascicolatori, non fanno parte della valutazione ma possono essere aggiunti all'ODV senza implicazioni per la sicurezza.

Nella configurazione valutata devono essere rispettati i seguenti requisiti (vedere par. 1.5.4.3 del Traguardo di Sicurezza [TDS]):

- La soluzione HP Digital Sending Software (DSS) deve essere disabilitata.
- Deve essere utilizzato un solo Administrative Computer per gestire l'ODV.
- Non devono essere installate sull'ODV soluzioni di terze parti.
- La funzionalità Device USB deve essere disabilitata.
- La funzionalità Host USB plug and play deve essere disabilitata.
- La gestione di Jetdirect Inside tramite telnet e FTP deve essere disabilitata.
- La funzionalità Jetdirect XML Services deve essere disabilitata.
- I soli metodi supportati per l'autenticazione IPsec sono i certificati X.509v3 e le chiavi pre-condivise (l'autenticazione IPsec tramite Kerberos non è supportata).
- Il protocollo IPsec Authentication Headers (AH) deve essere disabilitato.
- La funzionalità Control Panel Mandatory Sign-in deve essere abilitata (di conseguenza viene disabilitato il ruolo Guest).
- Il supporto a SNMP deve essere disabilitato.
- Il Service PIN, utilizzato da un tecnico dell'assistenza clienti per accedere alle funzioni disponibili al personale dell'assistenza HP, deve essere disabilitato.
- Le seguenti funzionalità wireless devono essere disabilitate:
 - Near Field Communication (NFC);
 - Bluetooth Low Energy (BLE);
 - Wireless station.

- Quando si utilizza Windows Sign In, il dominio Windows deve rifiutare le connessioni Microsoft NT LAN Manager (NTLM).
- Non è consentito l'uso del Pannello di Controllo da remoto.
- Non devono essere creati account Local Device Sign In (ovvero, è consentito come account Local Device Sign In solo l'account Device Administrator integrato).
- L'accesso ai seguenti servizi Web (WS) deve essere bloccato utilizzando IPsec e il Firewall di Jetdirect Inside:
 - Open Extensibility Platform device (OXPD) Web Services;
 - WS* Web Services.
- Deve essere impostata la Device Administrator Password.
- Non deve essere impostata la Remote Configuration Password.
- Non è consentito l'uso di OAuth 2.
- La funzionalità HP JetAdvantage Link Platform deve essere disabilitata.
- Non devono essere installate licenze per abilitare funzionalità oltre a quelle supportate nella configurazione valutata.
- Le funzionalità Internet Fax e LAN Fax devono essere disabilitate.
- Non è consentito l'aggiornamento del firmware mediante REST Web Services.

10.1 Ambiente operativo dell'ODV

I seguenti componenti devono essere necessariamente presenti nell'ambiente operativo dell'ODV per consentirne la corretta operatività (vedere par. 1.4.1 del Traguardo di Sicurezza [TDS]):

- Un server DNS (Domain Name System).
- Un server NTS (Network Time Service).
- Un computer client amministrativo, dotato di browser Web, connesso in rete all'ODV nel ruolo di Administrative Computer.
- Almeno uno dei seguenti server di autenticazione remota:
 - un server LDAP (Lightweight Directory Access Protocol);
 - un server controller di dominio Windows / Kerberos.
- Un server *syslog*.
- Un server WINS (Windows Internet Name Service).

I seguenti componenti possono essere opzionalmente presenti nell'ambiente operativo dell'ODV:

- Microsoft SharePoint.
- I seguenti protocolli per la connessione ai *file system* remoti:
 - FTP (File Transfer Protocol).
 - SMB (Server Message Block).
- Un gateway SMTP (Simple Mail Transfer Protocol).

11 Appendice C – Attività di test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia definito dai SAR inclusi nel PP [HCDPP], tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i test

Tutte le attività di test sono state eseguite in modalità remota dalla sede dell'LVS sul Virtual Test Laboratory (VTL) situato presso il sito del Fornitore a Boise, Idaho, USA. Lo Sviluppatore ha configurato l'ambiente di test includendo i modelli reali dell'ODV.

I Valutatori hanno verificato la configurazione dell'ambiente di test, compreso l'ODV, e hanno ritenuto che fosse coerente con la Common Criteria Evaluated Configuration Guide [CCECG] e il Traguardo di Sicurezza [TDS].

I Valutatori hanno eseguito i test da remoto utilizzando il protocollo RDP (Microsoft Remote Desktop) per connettersi all'ambiente di test.

Tutte le attività di test in modalità remota sono state svolte in conformità alle indicazioni fornite dall'Organismo di Certificazione nella Nota Informativa dello Schema 1/20 - Condizioni per l'effettuazione di test da remoto in valutazioni Common Criteria [NIS120].

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* al PP [HCDPP], che definisce una serie di casi di test mappati sugli SFR. Per soddisfare i requisiti di test del PP, i Valutatori hanno eseguito sia i casi di test automatici, sia quelli manuali, soddisfacendo così anche i requisiti per ATE_IND.1.

Prima di iniziare l'attività di test, i Valutatori hanno verificato che l'ODV fosse configurato correttamente. I Valutatori hanno anche verificato che l'ambiente di test fosse stato predisposto correttamente dal Fornitore.

I Valutatori hanno effettuato i test sui modelli fisici dell'ODV elencati nella Tabella 4, coprendo così tutte le versioni del firmware di Sistema.

| Nome dell'ODV (modelli hardware) | Versione firmware Jetdirect Inside | Versione firmware di Sistema |
|--|------------------------------------|------------------------------|
| HP ScanJet Enterprise Flow N9120 fn2 Document Scanner | JSI24110014 | 2411097_060492 |
| HP Digital Sender Flow 8500 fn2 Document Capture Workstation | | 2411097_060482 |

Tabella 4 - Modelli dell'ODV sottoposti a test

I Valutatori hanno eseguito tutti i test richiesti descritti nei PP [HCDPP] e [HCDPP-ERR] e nelle Technical Decision del NIAP applicabili elencate nel par. 2.1.1 del Traguardo di Sicurezza [TDS].

Tutti i test eseguiti dai Valutatori hanno fornito risultati coerenti con i risultati attesi.

11.3 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività, i Valutatori hanno operato sullo stesso VTL già utilizzato per le attività di test funzionali, verificando che l'ODV e l'ambiente di test fossero correttamente configurati.

Poiché per effettuare un attacco è necessaria una superficie di attacco, i Valutatori hanno deciso di esaminare se l'ODV espone tali interfacce, vale a dire porte di comunicazione di rete aperte.

Sono state eseguite scansioni di porte sulle interfacce dell'ODV accessibili ad un potenziale attaccante. I Valutatori hanno esaminato tutte le potenziali interfacce (porte TCP e UDP, IPv4 e IPv6, dell'ODV).

I Valutatori hanno verificato che solamente la porta UDP 500 (ISAKMP) è disponibile al di fuori di IPsec. Questo è il risultato atteso.

I Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.