Swedish Certification Body for IT Security

Certification Report- HP Digital Sender Flow 8500 fn1 Document Capture Workstation Firmware with Jetdirect Inside

Issue: 1.0, 2015-May-26

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary 3

2 Identification 4

3 Security Policy 5
3.1 Auditing 5
3.2 Cryptography 5
3.3 Identification and Authentication 5
3.4 Data Protection and Access control 6
3.5 Protection of the TSF 7
3.6 TOE Access Protection 7
3.7 Trusted Channel Communication and Certificate Management 7
3.8 User and Access Management 7

4 Assumptions and Clarification of Scope 8
4.1 Usage Assumptions 8
4.2 Environmental Assumptions 8
4.3 Clarification of Scope 8

5 Architectural Information 9

6 Documentation 10

7 IT Product Testing 11
7.1 Test Configuration 11
7.2 Developer Testing 11
7.3 Evaluator Testing Effort 11
7.4 Evaluator Penetration Testing 11

8 Evaluated Configuration 12

9 Results of the Evaluation 13

10 Evaluator Comments and Recommendations 14

11 Glossary 15

12 Bibliography 16

Appendix A QMS Consistency 17

1 Executive Summary

The Target of Evaluation, TOE, is the firmware providing the functionality of a document capture workstation (i.e., scanner) with the exception of the operating system and the crypto module implementation. The product is the HP Digital Sender Flow 8500 fn1 Document Capture Workstation Firmware with Jetdirect Inside.

The evaluated security features include administration, user identification and authentication, and IPSec protection network communication.

The implementation of the cryptographic module is outside the scope of evaluation, but the effect of cryptographic function calls from the TOE has been verified. All Universal Serial Bus (USB) Type-A ports are disabled in the evaluated configuration.

This Security Target claims conformance to:

- PP2600.2: IEEE Std 2600.2-2009; "2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B" (with NIAP CCEVS Policy Letter #20). Version 1.0 as of December 2009; demonstrable conformance.
- PP2600.2-SCN: SFR Package for Hardcopy Device Scan Functions. Version 1.0 as of December 2009; demonstrable conformance.
- PP2600.2-SMI: SFR Package for Hardcopy Device Shared-medium Interface Functions. Version 1.0 as of December 2009; demonstrable conformance.

The evaluation has been performed by atsec information system AB in their premises in Danderyd, Sweden. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL2, augmented by ALC_FLR.2 Flaw reporting procedures.

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

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

EAL 2 + ALC_FLR.2.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2014009
Name and version of the certified IT product	HP Digital Sender Flow 8500 fn1 Document Capture Workstation Firmware with Jetdirect Inside
Security Target Identification	Hewlett-Packard Digital Sender Flow 8500 fn1 Document Capture Workstation Firmware with Jetdirect Inside Security Target, 2014-02-26, Document version 1.3
EAL	EAL 2 + ALC_FLR.2
Sponsor	HP Company
Developer	HP Company
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2015-05-26

3 Security Policy

The security functionality of the TOE includes:

- Auditing of security relevant functions
- Cryptography
- Identification & authentication via the Control Panel or IPSec
- Data protection and access control
- Protection of the TSF
- TOE access protection
- Trusted channel communication and certificate management
- User and access management

3.1 Auditing

The TOE performs auditing of security relevant functions. Both the Jetdirect Inside and HCD System firmware generate audit records. The TOE connects and sends audit records to a syslog server for long-term storage and audit review. (The syslog server is part of the Operational Environment.)

3.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec.

3.3 Identification and Authentication

Control Panel I&A

The Control Panel interface supports both local and remote sign in methods. The following sign in methods are allowed with the evaluated configuration:

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

Local Device Sign In is only available through the Control Panel. The TOE contains a local user database for defining non-administrative (U.NORMAL, by default) device user accounts used to support the Local Device Sign In mechanism. Each device user account contains the following security attributes:

- Access Code (8 digits)
- Display Name
- Permission Set

The Access Code is a number that serves as both the login user identifier and the authentication secret. Each user's Access Code is unique from all other Local Device users. In the evaluated configuration, the Access Code length must be 8 digits.

The Display Name is a unique name assigned to the account by the administrator. This name is a security attribute because it is used in audit records to identify the user. (The Access Code is not written in the audit records.)

The Permission Set defines/determines a user's access to many of the TOE's functions.

Like Local Device Sign In, the remote sign in methods are only used by the Control Panel. The TOE receives authentication credentials from the Control Panel users and passes the credentials to the remote sign in method. The remote sign in method returns an authentication decision to the TOE. This decision is then enforced by the TOE by granting or denying access to the Control Panel user.

In the case of LDAP, the user name and password entered at the Control Panel are used to bind to the LDAP server. The user must have a valid and active LDAP account in order to successfully bind using this method.

In the case of Kerberos, the user name and password entered at the Control Panel are used to authenticate with the Windows domain controller. The user must have a valid and active Windows domain account in order to successfully bind using this method.

IPsec I&A

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

- Administrative Computer (U.ADMINISTRATOR)

IPsec uses IP addresses and X.509v3 certificates via the IKE protocols (IKEv1 and IKEv2) to identify and authenticate, respectively, a remote computer.

The User Identity of a remote computer is its IP address. The TOE's internal firewall maintains lists (IPsec/Firewall address templates) of IP addresses of remote computers that can connect to the TOE as an Administrative Computer. If a client computer has an unrecognized IP address that is not defined in the IPsec/Firewall as an Administrative Computer, then the remote computer is not allowed to connect to the TOE. Similarly, if the remote computer presents an invalid or unknown (unrecognized CA) X.509v3 certificate, the IPsec mutual authentication mechanism will fail.

The TOE also uses IP addresses and X.509v3 certificates via the IKE protocols to connect to and identify other trusted IT products. The Administrative Computer can access the EWS (HTTP) interface, Web Services interface (OXPd and WS-*), and SNMP interface.

3.4 Data Protection and Access control

- Permission Sets - For Control Panel users, the TOE uses a user's User Role (as determined by each user's Permission Set) to determine a user's access to many TOE functions. Only U.ADMINISTRATOR can create, modify, and delete Permission Sets.
- Common access control - Scan jobs are not stored on the TOE for later retrieval. Therefore only the U.NORMAL user who creates the job can read or delete it. In addition, U.ADMINISTRATOR can delete any active job.
- TOE function access control - The TOE controls Control Panel access to TOE functions through the use of Permission Sets. The home screen sign in process assigns the Permission Set to the authenticated user's session. This session Permission Set becomes the user's User Role. Access to each TOE device function is configurable in a Permission Set by an administrator. A user can perform any function permitted in the session Permission Set. Control Panel applications (e.g., Scan) use the user's Permission Set to determine which of the application's functions should be allowed or disallowed for the user.

- Residual Information Protection - Objects that are deleted in the TOE are made unavailable to TOE users preventing TOE users from recovering the contents of deleted objects.

3.5 Protection of the TSF

- Restricted Forwarding of Data to external interfaces - The TOE does not allow forwarding of data to an external interface. The TOE contains only one external interface in the evaluated configuration and that interface is the Shared-medium Interface.
- TSF Self-Testing - The EWS interface allows an administrator (U.ADMINISTRATOR) to execute a set of correct operations tests, TSF Data integrity tests, and integrity tests of TSF executable code.
- Reliable Timestamps - The TOE contains a system clock which is used to generate reliable time stamps.

3.6 TOE Access Protection

Inactivity Timeout - The TOE supports an inactivity timeout for Control Panel sessions. If a logged in user is inactive for longer than the specified period, the user is automatically logged off of the system. The inactivity period is managed by the administrator via EWS (HTTP) or with WS-* web services.

3.7 Trusted Channel Communication and Certificate Management

The TOE supports IPsec with X509v3 certificates to protect data transferred over the Shared-medium interface, along with certificate management for adding, replacing, and deleting certificates

3.8 User and Access Management

The TOE supports the following types of users; administrators and users. These users have the following management capabilities:

- Administrators - manage the security functionality of the device and manage users.
- Users - manage user data which they have access to.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

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

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

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

4.2 Environmental Assumptions

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

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

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

A.USER.PC.POLICY - User computers are configured and used in conformance with the organization's security policies.

4.3 Clarification of Scope

These are the threats to TOE is designed to meet:

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

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

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

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

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

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

5 Architectural Information

The TOE is the firmware of an enterprise document capture workstation designed to be shared by many human users. It performs the functions of scanning and sending of documents. It can be connected to a local network through the embedded Jetdirect Inside's built-in Ethernet.

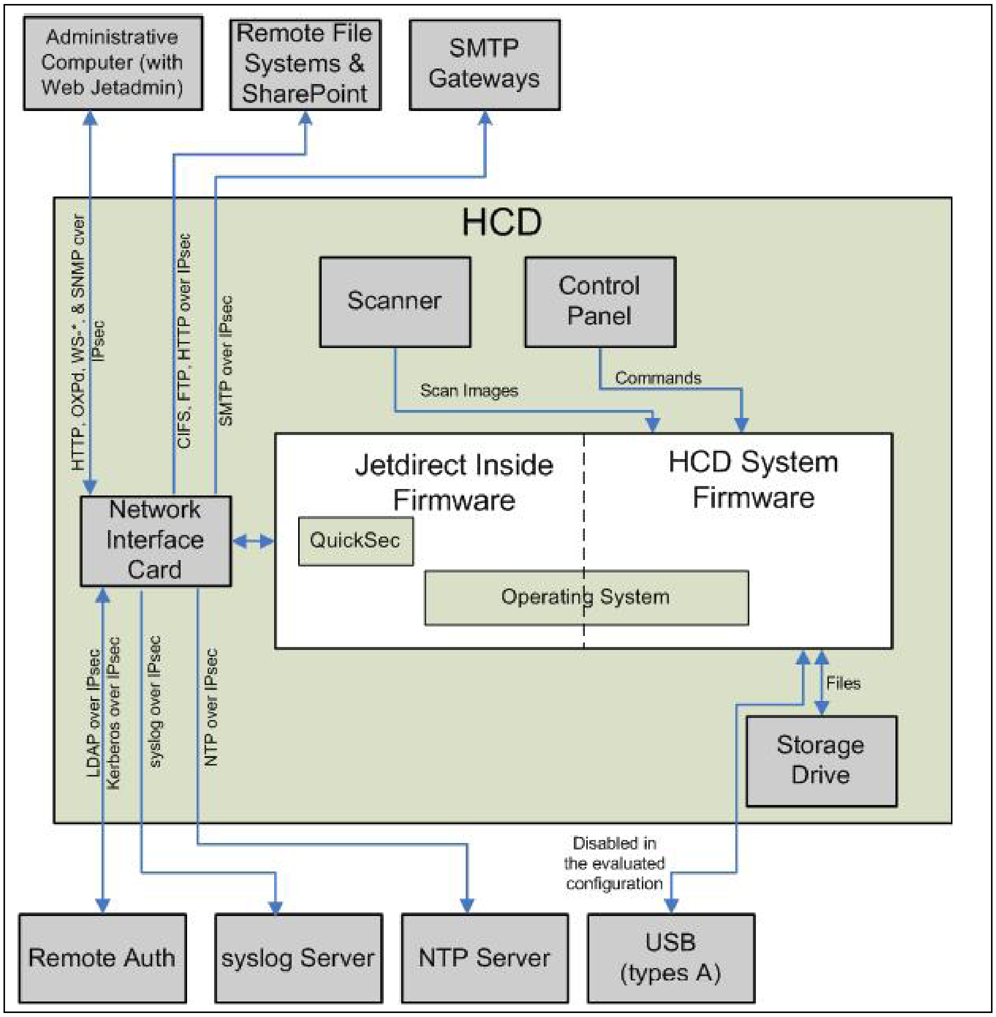

Figure 1: HCD physical diagram

Figure 1 shows a high-level physical diagram of an HCD with the unshaded areas inside the HCD representing the TOE and the shaded areas indicating components that are part of the Operational Environment.

6 Documentation

The following documents are included in the scope of the TOE:

- Common Criteria Evaluated Configuration Guide for HP Digital Sender Flow 8500 fn1 Document Capture Workstation, Version Edition 1, 11/2014
- HP Digital Sender Flow 8500 fn1 User Guide, Edition 1, 4/2013

7 IT Product Testing

7.1 Test Configuration

The test configuration is setup in two different ways: using IPv4 addressing and using IPv6 addressing. When performing the setup of the test configuration, the authentication and digital sending features must be configured using IPv4 or IPv6 addressing. Also, all connections to the interfaces of the device (e.g. EWS, SNMP) must be done using IPv4 or IPv6 addressing.

7.2 Developer Testing

Testing was performed by the developer at the HP site in Boise, Idaho, USA. The tested TOE was consistent with the information stated in [ST]. The evaluator notes that all testing is performed manually, there are no fully automated tests. All tests were passed successfully.

The developer performed functional tests to verify that the claimed security functionality works as intended. The test cases contain steps to test the successful execution of actions on the interfaces, as well as the failure of invalid actions. It is also tested if illegal information is leaked out on an interface, by observing the network traffic.

7.3 Evaluator Testing Effort

The evaluator performed the independent testing at the atsec Evaluation Laboratory in Stockholm, Sweden. The independent testing conducted uses a sample of the test cases provided by the developers and a set of test cases devised by the evaluator.

The evaluator configured the TOE and the testing environment to be identical to the developer's test environment.

The evaluator decided to repeat a sample of the developer test cases. The sample was chosen to cover all interfaces and TOE security functions with at least one test case. The focus was on security functionality on the subsystem level. The evaluator noted that not all TSFIs were covered by the developer tests. Additional evaluator test cases were therefore devised to fill this gap and cover all TSFIs and TOE security functions.

The evaluator testing was therefore performed for all TOE security functions and TSFIs, covered by at least one test case for each.

7.4 Evaluator Penetration Testing

Vulnerability testing was performed against the TOE interfaces that are accessible to a potential attacker. I.e., the IPv4 and IPv6 TCP and UDP ports of the TOE. Since an attack requires an attack surface, the evaluator decided to start by examining if the TOE exposes such interfaces, i.e., open ports.

The TOE and environment was configured according to [ST] and [CCConfigGuide].

The evaluator examined all potential interfaces, i.e., all IPv4 and IPv6 UDP and TCP ports. The evaluator determined that only UDPv4/v6 port 500 (ISAKMPD) is available outside of IPsec. This is the expected result.

8 Evaluated Configuration

The Target of Evaluation runs on the HP Digital Sender Flow 8500 fn1 Document Capture Workstation hardware:

- DCW Firmware version: 2304061_439465
- Jetdirect Inside version: JDI23400008.FF

Common Criteria Evaluated Configuration Guide for HP Digital Sender Flow 8500 fn1 Document Capture Workstation [CCConfigGuide] list requirements that must be met to achieve the evaluated configuration.

9 Results of the Evaluation

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	Pass
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security Problem Definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Use of a CM system	ALC_CMC.2	Pass
Part of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedure	ALC_FLR.2	Pass
Development	ADV	Pass
Security Architecure description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Sampling	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Vulnerability analysis	AVA_VAN.2	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

AES - Advanced Encryption Standard
AH - Authentication Header (IPsec)
ASCII - American Standard Code for Information Interchange
CA - Certificate Authority
CBC - Cipher Block Chaining
CIFS - Common Internet File System
DCW - Document Capture Workstation
DNS - Domain Name System
ESP - Encapsulating Security Payload (IPsec)
EWS - Embedded Web Server
FTP - File Transfer Protocol
HCD - Hardcopy Device
HMAC - Hashed Message Authentication Code
HTML - Hypertext Markup Language
HTTP - Hypertext Transfer Protocol
IEEE - Institute of Electrical and Electronics Engineers, Inc.
IKE - Internet Key Exchange (IPsec)
IP - Internet Protocol
IPsec - Internet Protocol Security
ISAKMP - Internet Security Association Key Management Protocol (IPsec)
LCD - Liquid Crystal Display
LDAP - Lightweight Directory Access Protocol
MAC - Message Authentication Code
NTLM - Microsoft NT LAN Manager
NTP - Network Time Protocol
OXP - Open Extensibility Platform
OXPd - OXP device layer
PIN - Personal Identification Number
SFR - Security Functional Requirement
SHA - Secure Hash Algorithm
SMTP - Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SOAP - Simple Object Access Protocol
SSH - Secure Shell
TOE - Target of Evaluation
USB - Universal Serial Bus
WINS - Windows Internet Name Service
XML - Extensible Markup Language

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 22.0, 2014-12-12, 14FMV9859-38:1, FMV/CSEC

[ST] Hewlett-Packard Digital Sender Flow 8500 fn1 Document Capture Workstation Firmware with Jetdirect Inside Security Target, Hewlett-Packard , document Version 1.3, 2015-02-26

[CCConfigGuide] Common Criteria Evaluated Configuration Guide for HP Digital Sender Flow 8500 fn1 Document Capture Workstation, Version Edition 1, 11/2014

[UserGuide] HP Digital Sender Flow 8500 fn1 User Guide, Edition 1, 4/2013

Appendix A QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2014-09-24:

QMS 1.16.2 valid from 2014-07-07

QMS 1.17 valid from 2014-11-20

QMS 1.17.1 valid from 2014-12-02

QMS 1.17.2 valid from 2015-01-13

QMS 1.17.3 valid from 2015-01-29

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.17.3”.

The certifier concluded that, from QMS 1.16.2 to the current QMS 1.17.3, there are no changes with impact on the result of the certification.