Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0566-2014

for

Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware

from

Hewlett-Packard Company

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0566-2014

Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware

from	Hewlett-Packard Company
PP Conformance:	IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B, IEEE Std 2600.2-2009, 26 February 2010, BSI-CC-PP-0058-2010 with NIAP CCEVS Policy Letter #20
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.2

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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 certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 27 January 2014

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Joachim Weber
Head of Division

L.S.

SOGIS Recognition
Agreement

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware has undergone the certification procedure at BSI.

The evaluation of the product Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware was conducted by atsec information security GmbH. The evaluation was completed on 5 November 2013. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Hewlett-Packard Company.

The product was developed by: Hewlett-Packard Company.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

[6] Information Technology Security Evaluation Facility

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Hewlett-Packard Company
11311 Chinden Blvd, MS 200
Boise, ID 83714
USA

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of evaluation (TOE) is the Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with JetDirect Inside Firmware (where MFP is an abbreviation for Multifunction Printer) and its associated guidance documentation. The TOE is thereby defined as the firmware inside of the Hewlett-Packard LaserJet MFPs, which are enterprise network multifunction products designed to be shared by many client computers and users. It provides the functions for the copying, faxing, printing, and scanning of documents. These hardcopy devices (HCDs), as they are called in the protection profile [7], are self-contained units that include a processor, memory, networking, hard drive, scanner, and print engine as well as the TOE.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B, IEEE Std 2600.2-2009, 26 February 2010, BSI-CC-PP-0058-2010 with NIAP CCEVS Policy Letter #20 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
TSF01	Auditing
TSF02	Identification and Authentication
TSF03	Data Protection and Access Control
TSF04	Protection of the TSF
TSF05	TOE Access Protection
TSF06	Trusted Channel Communication
TSF07	Management

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 1.5.4.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configuration of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040 and M9050 with Jetdirect Inside Firmware

The TOE is available for the following evaluated hardcopy device (HCD) models along with the respective evaluated firmware (TOE) version numbers for each model.

- HP Color LaserJet CM3530 MFP and CM3530fs MFP / MFP Firmware version: 20130128 53.194.1 / Jetdirect Inside version: V.43.16.FF
- HP Color LaserJet CM6030 MFP and CM6030f MFP / MFP Firmware version: 20130128 52.215.5 / Jetdirect Inside version: V.43.16.FF
- HP Color LaserJet CM6040 MFP and CM6040f MFP / MFP Firmware version: 20130128 52.215.5 / Jetdirect Inside version: V.43.16.FF
- HP LaserJet M9040 MFP / MFP Firmware version: 20130128 51.214.5 / Jetdirect Inside version: V.43.16.FF
- HP LaserJet M9050 MFP / MFP Firmware version: 20130128 51.214.5 / Jetdirect Inside version: V.43.16.FF

This evaluation only covers the HP LaserJet MFP Models CM3530, CM6030, CM6040, M9040, and M9050 with Jetdirect Inside. The following corresponding user guidance is provided with the TOE:

- HP Color LaserJet CM3530 MFP Series User Guide [9]
- HP Color LaserJet CM3530 MFP Embedded Web Server User Guide [10]
- HP LaserJet MFP Analog fax Accessory 300 fax Guide [11]
- HP Color LaserJet CM6030 and CM6040 MFP Series Embedded Web Server [12]
- HP Color LaserJet CM6030 and CM6040 MFP Series User Guide [13]
- HP LaserJet MFP Series Analog fax Accessory 500 fax Guide [14]
- HP Jetdirect Print Servers Administrator's Guide, Firmware V.36 and Firmware V.38 [15]
- HP LaserJet M9040/M9050 MFP Embedded Web Server User Guide [16]
- HP LaserJet M9040/M9050 MFP User Guide [17]
- Practical IPsec Deployment for Printing and Imaging Devices [18]
- Security Lock Adapter Installation Guide [19]

In addition, the sponsor provided the following documentation as administrator and user guidance specific to the TOE:

- Common Criteria Evaluated Configuration Guide for HP LaserJet MFPs v1.2 [20]
- Common Criteria User Operational Guide for HP LaserJet MFPs v1.2 [21]
- Common Criteria Administrator Operational Guide for HP LaserJet MFPs v1.1[22]

The TOE (firmware and guidance documentation) is available for distribution via online download only from the developer's website Software Download Depot (SDD). On the download website, a SHA-256 checksum is provided along with instructions on how to use it for verification of the integrity of the download packages. The checksums are repeated in this certification report.

Customers are required to register with HP and sign into a secure website (HTTPS) to access the pages containing the TOE download. Customers can check the digital signature of the secure HP website.

The TOE is delivered to the customer from an HP system, called a Kiosk. Users can receive access credentials by sending an email requesting the access credentials to ccc-hp-enterprise-imaging-printing@hp.com. Using these credentials, customers can sign in the Kiosk download site that is protected using the HTTPS protocol. Three download packages are available:

- Common Criteria Certification for HP Color LaserJet CM3530 MFP Series
- Common Criteria Certification for HP Color LaserJet CM6030/CM6040 MFP Series
- Common Criteria Certification for HP LaserJet M9040/M9050 MFP Series

Each of these packages contain the corresponding firmware files as well as the corresponding documentation.

The packages consist the following ZIP files, their integrity is protected by the following hash values:

- cljcm3530mfp_ccc_fw_and_guidance_Z7550-10520.zip, which has a SHA256 hash sum of: 05d81fbb1fca68fd188169269b1e562b4d2f6dcf975e19d8d705164651116956
- cljcm6030-40mfp_ccc_fw_and_guidance_Z7550-10518.zip, which has a SHA256 hash sum of: b26e4f34b5a6c6f79e46116a12628dbcf00e84b189ed67ed31c149078eb86bab
- ljm9040-50mfp_ccc_fw_and_guidance_Z7550-10519.zip, which has a SHA256 hash sum of: a5056d56147221164b9e6a9e9b26af23db01f30a2e89148644f40049db8af452

The HP download site instructs the user to verify the SHA256 hashsums of the downloaded packages to the ones provided on that website.

The consumer can follow the instructions provided in [20] chapter 3, section "Verifying LaserJet MFP is running Common Criteria Certified Firmware". [20] describes the firmware versions that need to be installed for the evaluated configuration.

The guidance documents for the TOE are labeled as being applicable to the TOE.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the issues that are summarized in the ST [6] in chapter 7 and detailed in the ST [6] in chapter 6.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The topics that are of relevance are the objectives which have to be met by the the envirioment. Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The TOE is the firmware for an enterprise network multifunction product designed to be shared by many client computers and human users. It performs the functions of copying, faxing, printing, and scanning of documents. It can be connected to a local network through the HP Jetdirect Inside built-in Ethernet and to an analog phone line using its internal analog fax modem.

The Administrative Computers are client computers that connect to the TOE using IPsec with X.509v3 certificates for both mutual authentication and for protection of data from disclosure and alteration. These computers can administer the TOE using the Embedded Web Server (EWS), simple Network Management Protocol (SNMP), and Printer Job Language (PJL) interfaces. The HTTP-based EWS administrative interface also supports the Digital Sender Module Protocol (DSMP) used to read and write XML-based device objects, and the HTTP-based certificate uploading of X.509v3 certificates. The SNMP interface allows administrators to remotely manage the TOE using SNMP-based administrative applications like the HP Web Jetadmin application.

The PJL interface allows administrators to password protect administrative data with the PJL Password while managing protected data.

The evaluated configuration supports the following SNMP versions:

- SNMPv1 read-only
- SNMPv2c read-only
- SNMPv3

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

The TOE supports an optional analog telephone line connection for sending and receiving faxes. The Control Panel uses identification and authentication to control access for sending analog faxes. Since the fax protocol does not support authentication of incoming analog fax phone line users, anyone can connect to the analog fax phone line, but the only function an incoming fax phone line user can perform is to transmit a fax into the HCD.

The TOE also supports remote file systems for the storing of scanned documents. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate. The TOE supports the File Transfer Protocol (FTP) and the Common Internet File System (CIFS) protocol for remote file system connectivity.

The TOE can be used to email scanned documents. The TOE supports protected communications between the TOE and Simple Mail Transfer Protocol (SMTP) gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutual authenticate with the SMTP gateway. The TOE can only protect the email up to the SMTP gateway.

Remote authentication servers can be used with the TOE. The TOE supports both LDAP and Kerberos. The TOE uses IPsec with X.509v3 certificates to protect LDAP communications. It uses the Kerberos protocol for protecting Kerberos communications.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of a touch sensitive LCD screen and several physical buttons that are attached to the HCD. It is the interface device that a user uses to communicate to the HCD 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. The Scanner is the part of the HCD that converts hardcopy documents into an electronic format. The Print Engine converts an electronic format into hardcopy. The Hard Disk (a.k.a. hard drive) provides persistent storage for documents. The hard drive contains a section called Job Storage which is a user-visible file system where stored jobs such as certain types of fax jobs, certain types of print jobs, and certain types of copy jobs are stored/held until deleted/released by a user, or depending on the job type, stored until the HCD is rebooted if no user action is taken.

The TOE supports the auditing of security relevant functions. It contains an internal fixed-size audit log file for storing audit events and also forwards the audit events to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between the HCD and the syslog server and to mutually authenticate the HCD and syslog server.

The Jetdirect Inside Firmware and HCD System Firmware components comprise the TOE. Though they are shown as two separate components, they both run in the same instance of the operating system. Both firmware components contain an Embedded Web Server (EWS). The two firmware components communicate with each other through these two web servers.

The Jetdirect Inside firmware includes SNMP, IPsec/Firewall, and the management functions for managing these network-related features. The Jetdirect Inside firmware also controls the HCD's Ethernet network interface.

The TOE controls the overall functions from the Control Panel to the hard drive to the print jobs.

6 Documentation

The evaluated documentation as outlined in chapter 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

Test Configuration

The TOE with each model of MFP specified in the ST [6] (CM3530, CM6030, CM6040, M9040 and M9050) was tested in each of the following configurations:

- Test Configuration "A" - This test configuration is used for running test cases using IPv4 addressing. When using this test configuration, the authentication and digital sending features must be configured using IPv4 addressing. Also, all connections to the interfaces of the HCD (e.g. EWS, SNMP) must be done using IPv4 addressing. The instructions provided in [20] must be used.
- Test Configuration "B" - This test configuration is used for running test cases using IPv6 address. When using this test configuration, the authentication and digital sending features must be configured using IPv6 addressing. Also, all connections to the interfaces of the HCD (e.g. EWS, SNMP) must be done using IPv6 addressing. The instructions provided in [20] must be used.

Developer Testing

The developer performed functional developer tests in several sessions. All functional tests were performed on a TOE configuration consistent with the [6]. With respect to the actual test results of the functional developer tests, no deviations from the expected results were identified.

The test approach chosen by the developer is based on the TOE Security Functionality (TSF) as described in the Security Target [6]. For the security functionality, the developer prepared test cases to verify the correct behaviour of the TOE with respect to those security requirements.

The functional tests were performed at the level of subsystems of the TSF. As a result of the evaluator's assessment of test coverage, additional test cases were added to the test plan by the developer to cover all interfaces and subsystems to the TSF identified in the functional specification of the TOE that had not already been triggered by tests.

All tests were run by the developer within two test sessions and compliance of actual test results with those expected were noted in the test plan by either a "Pass" or with the log message conveying the test is passed.

All test results from all tested platforms show that the expected test results are identical to the actual test results.

Evaluator Testing

The evaluator re-ran a sub-set of the developer tests and witnessed the rest of the functional test suite.

The evaluator witnessed installation and configuration of the TOE following the instructions given in [20] and [6]. The evaluator ran the entire test suite successfully. The evaluator executed additional test cases. These additional tests were based on mainly varying input parameters of already existing test cases.

All tests were performed on the same TOE configuration already used by the developer and thus consistent with the ST.

The actual test results of the functional testing as well as independent testing matched the expected test results and no deviations were observed.

Evaluator Penetration Testing

The evaluator defined a penetration test framework and produced penetration tests to verify the vulnerabilities. None of the penetration test were successful. In addition, the evaluator used a port scanner called "Nmap" to scan the open ports and a information gathering tool called "PREADA" to scan the TOE for known vulnerabilities. No applicable vulnerabilities were detected.

None of the evaluator's penetration tests were successful.

No exploitable vulnerabilities considering the claimed attack potential Basic were identified.

8 Evaluated Configuration

The TOE is available for the evaluated hardcopy device (HCD) models along with the respective evaluated firmware (TOE) version numbers for each model as described in the ST [6] and in chapter 2 of this report. It covers only these configurations. Furthermore, version numbers for each model accompanied by guidance documentation as specified in chapter 1 of [20].

Furthermore, chapter 1.5.3.3 of the ST [6] describes the evaluated configuration. The following components are considered part of the operational environment and, therefore, beyond the scope of this evaluation: X.509v3 certificate generation, HP Web Jetadmin administrative tool, HP Printer Drivers for client computers (for submitting print job requests from Network Client Computers), Kerberos server, LDAP server, Remote file systems, SMTP gateway, syslog server, Web browser, HCD hardware.

In addition, [20] which gives the following requirements that must be met to achieve the evaluated configuration:

Requirements for the Administrator

User Names/Passwords/PINs

The TOE must meet the following user name/password/PIN requirements:

- The Device Password (also called the EWS Password or Administrator Password) must be configured to at least eight characters.
- The Fax PIN must be configured to exactly 8 digits and must not begin with zero.
- The Fax PIN must not be deleted.
- The Job PIN applied to a private stored job must be exactly four digits.
- The PIN for a user PIN account must be exactly eight digits.
- User name of a user PIN account must not contain the following: ampersand (&); left angle bracket (<); right angle bracket (>); straight quotation mark ("); apostrophe (')
- The user name for a user PIN account must not exceed 25 characters.
- A Kerberos user name must not exceed 25 characters.
- LDAP user names must not exceed 25 characters.
- The File System Password must be at least eight characters.
- The Bootloader Password must be at least eight digits.
- The PJL Password must be at least 9 digits and between 100000000 and 2147483647.

- The PJL Password must not be deleted.
- The SNMPv1/v2 Get community name must be at least eight characters.
- The SNMPv1/v2 Set community name must be at least eight characters.
- The SNMPv3 authentication passphrase must be at least eight characters.
- The SNMPv3 privacy passphrase must be at least eight characters.

Third-party software

The evaluated configuration must not include any third-party solutions or applications installed.

Audit Logs

- Only authorized administrators have access to the audit logs on the LaserJet MFP, on the Syslog server, and any other backups that might exist.
- The administrator of the LaserJet MFP must periodically review the audit logs on the Syslog server.

Timestamps for Audit Records

- The administrator must perform the timestamp verification test periodically.
- The administrator must periodically check the system clock for drift from actual time.

Data Integrity Self Test

After initially configuring the TOE, the administrator must set a data integrity reference point and periodically perform the data integrity self-test to verify the configuration and authenticated data have not changed.

Requirements for the Operating Environment

Network Accessible Only to Authorized Administrators

A non-production network accessible only to authorized administrators must be available and the MFP placed on that network at the following times:

- when configuring the TOE to the evaluated configuration,
- when retrieving the audit log stored on the TOE,
- when performing any recovery or maintenance tasks that require the TOE to be taken out of the evaluated configuration.

Certificate Authority

A trusted Certificate Authority (CA) capable of generating and signing Jetdirect Identity Certificates must be available. The CA must also be able to issue Identity Certificates to computers authorized to communicate with the TOE.

HP Web Jetadmin

HP Web Jetadmin (WJA) must be installed on a computer that has been designated as an Administrator Computer for configuring, managing, and monitoring the TOE.

Supported Web Browsers

A supported web browser is required to communicate with the TOE's Embedded Web Server (EWS) to configure, manage and monitor the TOE. The following Web browsers are supported:

- Konqueror 3.5 or later.
- Microsoft Internet Explorer 6.0 or later.
- Mozilla Firefox 1.0 or later.
- Opera 9.0 or later.
- Safari 1.0 or later.

Linux Computer with sha256sum Tool Installed

A computer that runs the Linux operating system with the sha256sum tool installed must be available to to verify the integrity of the Software Depot package download.

Syslog server

A syslog server configured to receive log messages on TCP port 514 must be available.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B, IEEE Std 2600.2-2009, 26 February 2010, BSI-CC-PP-0058-2010 with NIAP CCEVS Policy Letter #20 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_FLR.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in chapter 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

For other obligations and notes for the usage of the TOE please see also chapter 8 of this report.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CIFS	Common Internet File System
DSMP	Digital Sender Module Protocol
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EWS	Embedded Web Server
FTP	File Transfer Protocol
HCD	Hardcopy Device
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MFP	Multifunction Product
PIN	Personal Identification Number
PJL	Printer Job Language
PP	Protection Profile
SAR	Security Assurance Requirement
SDD	Software Download Depot
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
WJA	Web Jetadmin
XML	Extensible Markup Language
ZIP	A File Format Specification

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 1, September 2007

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Hewlett-Packard LaserJet MFP Models CM3530, CM6030, CM6040, M9040, and M9050 with Jetdirect Inside Firmware Security Target BSI-DSZ-CC-0566-2014, Version 2.2, Date 2013-10-23, Hewlett-Packard

[7] IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B, IEEE Std 2600.2-2009, 26 February 2010, BSI-CC-PP-0058-2010 with NIAP CCEVS Policy Letter #20, November 11, 2010

[8] Evaluation Technical Report, Version 6.3, Date 2013-12-16, Certification ID: BSI-DSZ-CC-0566, atsec, (confidential document)

[9] HP Color LaserJet CM3530 MFP Series User Guide, Edition 2, 10/2008

[10] HP Color LaserJet CM3530 MFP Embedded Web Server User Guide, Edition 1, 4/2008

[11] HP LaserJet MFP Analog fax Accessory 300 fax Guide, Edition 1, 04/2008

[12] HP Color LaserJet CM6030 and CM6040 MFP Series Embedded Web Server, Edition 1, 2/2008

[13] HP Color LaserJet CM6030 and CM6040 MFP Series User Guide, Edition 1, Date April 2008

[14] HP LaserJet MFP Series Analog fax Accessory 500 fax Guide, Edition 1, 4/2011

[15] HP Jetdirect Print Servers Administrator's Guide (Firmware V.38), Edition 8, 02/2008, and HP Jetdirect Print Servers Administrator's Guide, HP Jetdirect Firmware V.36, Edition 7, 5/2007

[16] HP LaserJet M9040/M9050 MFP Embedded Web Server User Guide, Edition 1, 9/2007

[17] HP LaserJet M9040/M9050 MFP User Guide, Edition 1, Edition 2, 10/2009

[18] Practical IPsec Deployment for Printing and Imaging Devices, Date June 2008

[19] Security Lock Adapter Installation Guide, Date 2009-05-20

[20] Common Criteria Evaluated Configuration Guide for HP LaserJet MFPs, Version 1.2, Date April 2013

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[21] Common Criteria User Operational Guide for HP LaserJet MFPs, Version 1.2, Date April 2013

[22] Common Criteria Administrator Operational Guide for HP LaserJet MFPs, Version 1.1, Date April 2013

This page is intentionally left blank

C Excerpts from the Criteria

CC Part 1:

Conformance Claim Release 2 = chapter 9.4

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	**Assurance Components**
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.