Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0478-2008

for

Xerox WorkCentre 5030/5050 Multifunction Systems
System Software Version 5.003.07.000

from

Xerox Corporation

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-0478-2008

Multifunction System

Xerox WorkCentre 5030/5050 Multifunction Systems
System Software Version 5.003.07.000

from	Xerox Corporation
Functionality:	product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.3

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 19 August 2008
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all Evaluation Assurance Levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this agreement.

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

2.2 International Recognition of CC - Certificates

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 February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: 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.

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 Xerox WorkCentre 5030/5050 Multifunction Systems, System Software Version 5.003.07.000 has undergone the certification procedure at BSI.

The evaluation of the product Xerox WorkCentre 5030/5050 Multifunction Systems, System Software Version 5.003.07.000 was conducted by CSC Deutschland Solutions GmbH. The evaluation was completed on 30 July 2008. The CSC Deutschland Solutions GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Xerox Corporation

The product was developed by: Xerox Corporation

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

[6] Information Technology Security Evaluation Facility

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

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

For the meaning of the assurance levels and the confirmed strength of functions, 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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 Xerox WorkCentre 5030/5050 Multifunction Systems, System Software Version 5.003.07.000 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// 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] Xerox Corporation
1350 Jefferson Road
Rochester, NY 14623
USA

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) are the Xerox WorkCentre 5030/5050 Multifunction Systems (Xerox WorkCentre model 5030 or 5050). The TOE is a Multifunction Device (MFD) that consists of a printer, copier, scanner, FAX (when purchased by the consumer), and email as well as all Administrator and User guidance. The difference between the two models is their printing speed. The TOE consists of the whole MFD (complete Hardware together with the Software which is installed on the Hardware).

The MFD provides copy and print services as well as the scan to email, network scan and FAX options. The optional Xerox Embedded Fax accessory provides local analog FAX capability over Public Switched Telephone Network (PSTN) connections, if purchased by the consumer.

The MFD stores temporary image data created during a print, network scan or scan-to-email job on an internal Hard Disk Drive (HDD). This temporary image data consists of the original data submitted and additional files created during a job.

The TOE has an Image Overwrite function that overwrites files created and stored on the HDD during print, network scan or scan-to-email jobs. This overwrite process will be activated at the completion of each print, network scan, or scan to email job (Immediate Image Overwrite (IIO)), once the MFD is turned back on after a power failure or on demand of the MFD system administrator (On Demand Image Overwrite (ODIO)). Copy and FAX jobs are not written to the HDD and therefore need not to be overwritten.

The TOE does not allow information to flow between the PSTN port of the optional FAX processing board (if installed) and the network controller (which covers the information flow to and from the internal network). Data and/or commands cannot be sent to the internal network via the PSTN. A direct connection from the internal network to external entities by using the telephone line of the TOE is also denied.

The TOE requires a system administrator to authenticate before granting access to system administration functions. The system administrator has to enter a PIN at either the web user interface or the local user interface. The PIN will be obscured with asterisks as it is being entered. Identification of the system administrator at the local user interface is implicit – the administrator will identify themselves by pressing the “Access” hard button. Identification of the system administrator at the web user interface is explicit -- the administrator will identify themselves by entering the username “admin” in the authentication dialog window. Only authenticated system administrators can enable or disable the Image Overwrite function, enable or disable the On Demand Image Overwrite function, change the system administrator PIN, and start or cancel an On Demand Image Overwrite operation.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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.3.

The Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

There are no Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE.

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

TOE Security Function	Addressed issue
Image Overwrite (TSF_IOW)	The TOE implements an Image Overwrite Security Function to overwrite temporary files created during the printing, network scan, or scan-to-email process.
Information Flow (TSF_FLOW)	The TOE does not allow communication between the optional FAX processing board and the network controller and prevents therefore an interconnection between the PSTN and the internal network.
Authentication (TSF_AUT)	The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions.
Security Management (TSF_FMT)	The TOE provides some administrative functions to the system administrator.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The claimed TOE's Strength of Functions 'basic' (SOF-basic) for specific functions as indicated in the Security Target [6], chapter 8.6 is confirmed.

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

This certification covers the following configurations of the TOE: The Image Overwrite Security Package is installed and Immediate Image Overwrite (IIO) and On Demand Image Overwrite (ODIO) are enabled on the TOE. IIO and ODIO must not be disabled.
The Xerox Embedded Fax accessory is an optional part of the TOE which can be ordered by the customer. It provides local analog FAX capability over PSTN connections, when purchased and installed. Only in this case the TOE provides the Security Function "Information Flow (TSF_FLOW)". If the FAX option is not installed this Security Function is not present and not needed as it is separated from and does not influence the other Security Functionality.

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:

Xerox WorkCentre 5030/5050 Multifunction Systems,
System Software Version 5.003.07.000

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Xerox WorkCentre	5030 / 5050	
2	SW	System Software	5. 003.07.000	Installed on MFD
3	SW	Network Controller Software	1.08.535.01	Installed on MFD
4	SW	UI Software	005.03.007	Installed on MFD
5	SW	SIP Software	50.06.00	Installed on MFD
6	SW	IOT Software	23.54.00	Installed on MFD
7	SW	DADH Software	12.15.00	Installed on MFD
8	SW	Finisher Software	09.21.00	Installed on MFD
9	SW	FAX Software	02.28.03	Installed on MFD
10	SW	Printer and Fax Driver		CD
11	SW	All optional software kits the customer purchased; The evaluated configuration includes at least the IIO option kit.	part number 604E32560	CD
12	DOC	WorkCentre 5030/5050 Quick Reference Guide	part number 604E39140	Paperform
13	DOC	User guidance	part number 538E11390	CD
14	DOC	Administrator guidance	part number 538E11400	CD
15	DOC	Secure Installation and Operation of Your WorkCentre™ 5030/5050	Version 1.6 April 16, 2008	Download from Xerox-Webpage: http://www.xerox.com/security

Table 2: Deliverables of the TOE

The TOE is assembled and packed according to the order form of the Customer. Xerox Authorized Representatives deliver the device to the customer site. There Xerox Authorized Representatives will install the product according to the installation instructions.

A customer system administrator can ensure that they have a TOE by printing a configuration sheet and comparing the version numbers reported on the sheet to table 2 above or in the Security Target [6].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- The image information of the different types of jobs the MFD can handle is considered as confidential user information. Therefore, the TOE must protect this information according to the following rules:
  Temporary document image data from a print, network scan or scan-to-email job must be overwritten on the HDD immediately after that job is completed, once the MFD is turned back on after a power failure or if the system administrator has invoked the On Demand Image Overwrite function. Document image data of copy and FAX jobs must not be written to the HDD.
- The Security Function “Information Flow (TSF_FLOW)” restricts the information flow between the PSTN port of the optional FAX board (if installed) and the internal network by implementing a store-and-forward principle. The TOE does not allow information to flow between the PSTN port of the optional FAX processing board (if installed) and the network controller (which covers the information flow to and from the internal network). Data and/or commands cannot be sent to the internal network via the PSTN. A direct connection from the internal network to external entities by using the telephone line of the TOE is also denied.
  If the FAX board is not installed, an information flow is not possible and needs not to be restricted.
- The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions. The following security management functions are provided by the TOE:
  - Enable or disable the Immediate Image Overwrite function (IIO) (only via local user interface)
  - Enable or disable the On Demand Image Overwrite function (ODIO) (only via local user interface)
  - Change of the System Administrator PIN (only via local user interface)
  - Invocation of ODIO (via local user interface or web user interface)
  - Cancellation (Abort) of ODIO (via local user interface or web user interface)

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 following topics are of relevance:

- Monitored network to which the TOE is connected to
- Secure installation and configuration of the TOE
- Monitored office environment in which the TOE is located
- Trained and trustworthy TOE administrators

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The following figure shows decomposition of the TOE into six subsystems.

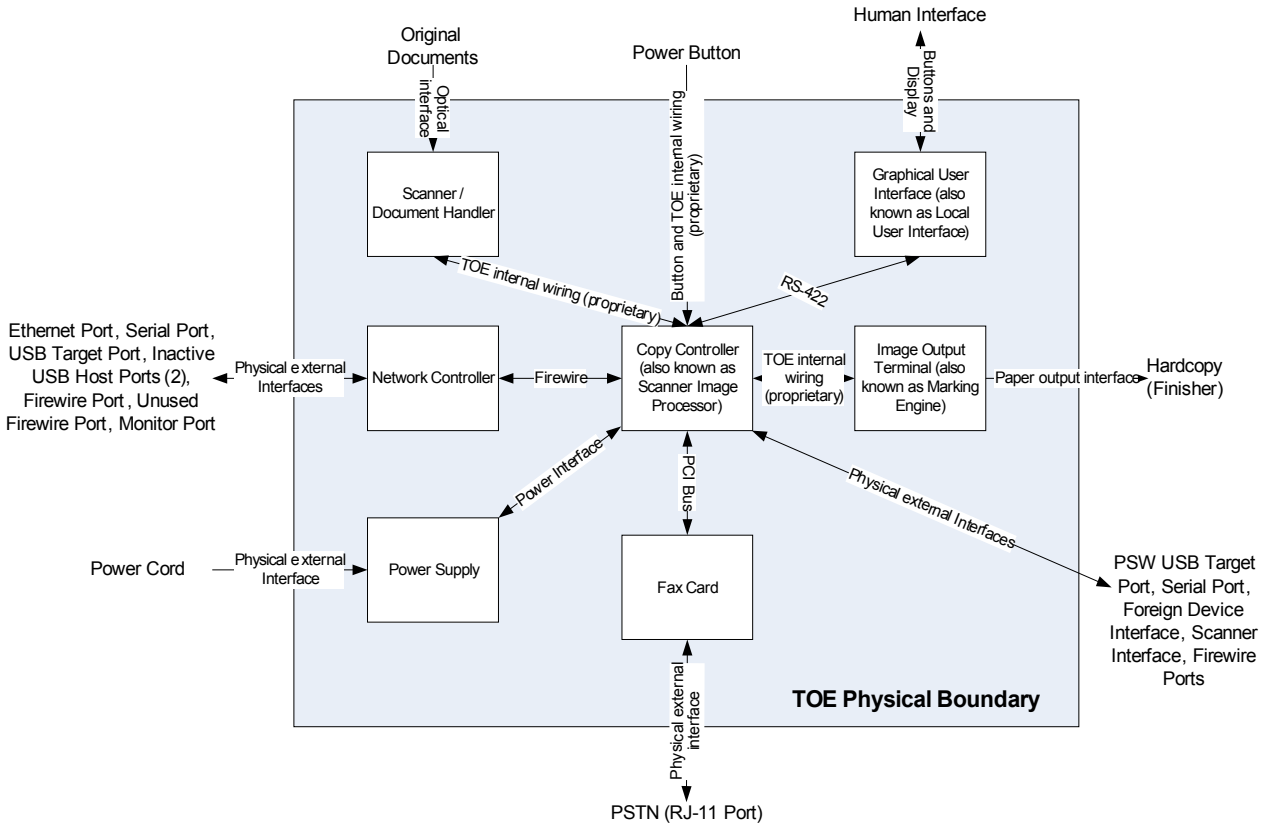

Figure 1: Architecture of the TOE

The TOE consists of the subsystems Scanner/Document Handler, Network Controller, Power Supply, FAX Card, Copy Controller (also known as Scanner Image Processor), Graphical User Interface (also known as Local User Interface) and the Image Output Terminal (also known as Marking Engine). The TOE has several external and internal interfaces as depicted in the figure.

6 Documentation

The evaluated documentation as outlined in table 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

7.1 TOE Test Configuration

The LAN interface of the network controller of the TOE is connected to a local LAN. All other test systems are also connected to this LAN. The TOE is furthermore connected to the PSTN to be able to send and receive facsimiles.

By using a serial Null-Modem connection, the evaluator was able to access the Linux-based operating system of the network controller. The evaluator uses a terminal server for this purpose because the TOE was not located in the office rooms of the evaluator. The terminal server is a Windows 2003 server with a serial interface and Tutty1 v0.58.1 as serial terminal software. The evaluator uses the remote desktop tool of Windows to access the terminal server.

The File- and FTP-Server was set up to test the scan-to-network features and to have a file transfer ability to and from the Linux-based operating system. This server runs under Linux. File services are provided by Samba, the FTP-Server used was vsftpd.

The Email-Server was set up to test the scan-to-email features. This server runs under Linux. Email services (only SMTP) are provided by postfix.

The evaluator PC runs under Windows XP. The TOE printer driver and the TOE as system printer are installed.

7.2 Developer Tests

The developer tested all TOE Security Functions in combination with the different user interfaces (local user interface or web user interface) and in combination with the different types of jobs (print, copy, fax, …).

The depth of testing was on the level of the external interfaces as required for EAL 2.

The TOE passed all developer tests. This means the verification of the complete and correct implementation of all TOE Security Functions and all TOE Security Functional Requirements was successful.

7.3 Independant Evaluator Tests

Due to the fact that the TOE is a device with an overall SOF claim “basic”, the evaluator does not select a very rigorous testing strategy. Therefore, the evaluator decides to test all Security Functions and all Security Functional Requirements with little to medium rigor.

The approach to select and define the test subset is to take the developer tests into account, modify some of the tests and define some additional tests in order to fulfill the test strategy requirements. The evaluator does not repeat all tests of the developer tests but only selected.

Due to the fact that the TOE itself must not be modified for the tests, only the tools available at the Linux operating system of the TOE can be used. The external connections to the TOE were realized by browsers (here: Internet Explorer 7 and Firefox 2.0.0.14). The serial connection was established by Tutty (see above). Print jobs were started using the Xerox PCL6 Printer Driver for Windows XP, available at the Xerox web site. For receiving and sending facsimiles from and to the TOE, a conventional digital FAX machine was used.

The TOE passed all evaluator tests. This means the verification of the complete and correct implementation of all TOE Security Functions and all TOE Security Functional Requirements was successful.

The depth of testing was on the level of the external interfaces as required for EAL 2.

7.4 Penetration Tests

According to the requirements of EAL 2 the developer did a research for common known vulnerabilities for this product or product type. The developer did also a penetration test using a penetration testing tool.

Additionally, the evaluator verified the results and conclusions of the developer and performs also penetration tests using penetration testing tools.

The vulnerability tests of the evaluator are based on the intended operational environment. Therefore the evaluator assumes that an attacker does not have direct physical access to the TOE. So, only remote attacks were performed. This means only the network protocols as logical interfaces of the TOE were tested. For this purpose, the evaluator activated all network protocols the TOE supports.

The evaluator performed some network vulnerability scans using the vulnerability scanner Nessus version 3.2.0. The scanner identified some potential vulnerabilities. After an analysis of the given facts and the output of the scanner, all the remarks could be identified as false positives. So, no vulnerability could be identified.

For verification of the developer SOF analysis the evaluator performed a brute force attack the tool Brutus (www.hoobie.net/brutus) against the web user interface in order to break PIN mechanism. It could be demonstrated that a brute force against this interface and function will not succeed due to improper performance of the TOE.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- The Image Overwrite Security Package is installed and Immediate Image Overwrite (IIO) and On Demand Image Overwrite (ODIO) are enabled on the TOE. IIO and ODIO must not be disabled.
- The Xerox Embedded Fax accessory is an optional part of the TOE which can be ordered by the customer. It provides local analog FAX capability over PSTN connections, when purchased and installed.
  If the FAX option is installed and enabled, the TOE does not allow communication between the optional FAX processing board and the network controller and prevents therefore an interconnection between the PSTN and the internal network. If the optional FAX board is not installed, an information flow from or to the FAX port is not possible at all.
  The Security Functionality provided by the TOE concerning the FAX option is separated from and does not influence the other Security Functionality. If the FAX option is not installed the associated Security Functionality (TSF_FLOW with dedicated SFRs, see Security Target [6]) is not present and not needed.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] 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.

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

- All components of the class ASE
- All components of the EAL2 package as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by
  ALC_FLR.3
- The following TOE Security Functions fulfil the claimed Strength of Function : basic Authentication (TSF_AUT)

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 operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, the following aspects need to be fulfilled when using the TOE:

- There is no physical access to the TOE for an attacker.
- The minimum length of the PIN is 8 characters.
- The network the TOE is connected to is monitored regarding attacks against the TOE or other network equipment.
- IIO is installed and enabled.
- The TOE has to be installed and configured according to the guidance document “Secure Installation and Operation of Your WorkCentre™ 5030/5050” [11].

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

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

FAX Facsimile

HDD Hard Disk Drive

IIO Immediate Image Overwrite

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LAN Local Area Network

MFD Multifunctional Device

ODIO On Demand Image Overwrite

PP Protection Profile

PSTN Public Switched Telephone Network

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0478-2008, Version 1.0, Revision 1.18, 15 April 2008, „Xerox WorkCentre 5030/5050 Multifunction Systems Security Target“, Xerox Corporation

[7] Evaluation Technical Report BSI-DSZ-0478-2008, Version 1.0, 30 July 2008, CSC Deutschland Solutions GmbH (confidential document)

[8] WorkCentre 5030/5050 Quick Reference Guide, Part Number 604E39140, Xerox Corporation

[9] User guidance, Part Number 538E11390, Xerox Corporation

[10] Administrator guidance, Part Number 538E11400, Xerox Corporation

[11] Secure Installation and Operation of Your WorkCentre™ 5030/5050, Version 1.6, 16 April 2008, Xerox Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.