Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0516-2009

for

Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems System Software Version 21.113.02.000

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-0516-2009

Multifunction Device

Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687
Multifunction Systems
System Software Version 21.113.02.000

from	Xerox Corporation
PP Conformance:	None
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 (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, 30 April 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

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 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

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

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 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 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

2.2 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 January 2009 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 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 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems, System Software Version 21.113.02.000 has undergone the certification procedure at BSI.

The evaluation of the product Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems, System Software Version 21.113.02.000 was conducted by CSC Deutschland Solutions GmbH. The evaluation was completed on 09 April 2009. 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 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 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems, System Software Version 21.113.02.000 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, New York 14623
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) consists of the Xerox WorkCentre 5632/5638/5645/5655/ 5665/5675/5687 Multifunction Systems, System Software Version 21.113.02.000.

The TOE is a Multifunction Device (MFD) that provides copy, print, scan-to-email, network scan (including “scan to mailbox”) and optionally FAX services.

The difference between the 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 stores temporary image data created during a print, network scan or scan to email, and LanFAX 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. All partitions of the HDD used for spooling temporary files are encrypted. The encryption key is created dynamically on each power-up.

A standard component of the TOE is the Image Overwrite Security package. The Image Overwrite function overwrites temporary document image data as described in DoD Standard 5200.28-M at the completion of each print, network scan, scan to email, or LanFAX job, once the MFD is turned back on after a power failure or on demand of the MFD system administrator. Copy jobs are not written to the hard drive and do not need to be overwritten. Copy/Print, Store and Reprint jobs are written to the hard drive so that they may be reprinted at a later time; therefore, they will be overwritten when a full on-demand image overwrite is performed. Embedded FAX jobs are written to flash memory and are overwritten at the completion of each job, or on demand of the MFD system administrator.

The optional Xerox Embedded Fax accessory provides local analog FAX capability over Public Switched Telephone Network (PSTN) connections and also enables LanFax jobs, if purchased by the consumer. A separate non-volatile memory resource is dedicated to embedded fax, and the image files written to this memory are zeroed at the completion of a fax job.

The system administrator must authenticate by entering a PIN prior to being granted access to the system administration functions. While the system administrator is typing the PIN number, the TOE displays an asterisk for each digit entered to hide the value entered.

All models of the TOE support both auditing and network security. The system administrator has to enable and configure the network security support. The network security support is based on SSL. When SSL support is enabled on the device, the following network security features can be enabled/configured: HTTPS support (for both the device’s web user interface (WebUI) and secure network scan data transfer); system administrator download of the device’s audit log; IPSec support for print jobs; secure network device management through SNMPv3, and specification of IP filtering rules. Scan-to-email and FAX data are not protected from sniffing by the IPSec or SSL support. The transmission of LanFax data over the Ethernet connection is protected by IPSec, but the transmission over the PSTN is not. Note that for the MFD configuration, IPSec and SNMPv3 can only be activated if SSL has been enabled and an SSL-based certificate has been loaded into the TOE via the Web UI.

The TOE provides user identification and authorization based on either local or remote access control lists as configured by the system administrator.

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 TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.3. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Function	Addressed issue
TSF_IOW	Image Overwrite
TSF_FLOW	Information Flow Security
TSF_AUT	System Authentication
TSF_NET_ID	Network Identification
TSF_FAU	Security Audit
TSF_FCS	Cryptographic Support
TSF_FDP_SSL	User Data Protection – SSL
TSF_FDP_FILTER	User Data Protection – IP Filtering
TSF_FDP_IPSec	User Data Protection – IPSec
TSF_NET_MGMT	Network Management Security
TSF_FMT	Security Management
TSF_EXP_UDE	User Data Protection - AES

Table 1: TOE Security Functions

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.2 – 3.4.

The evaluated configuration covered by this certification is described in detail in chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, 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:

Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems, System Software Version 21.113.02.000

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Xerox WorkCentre	5632/5638/5645/5655/ 5665/5675/5687	
2	SW	System Software	21.113.02.000	Installed on MFD
3	SW	Network Controller Software	050.60.50812.P33v1	Installed on MFD
4	SW	UI Software	020.11.030	Installed on MFD
5	SW	IOT Software	91.02.65	Installed on MFD
6	SW	SIP Software	20.11.30	Installed on MFD
7	SW	DADH Software (Options) Normal Mode Quiet Mode	 16.28.00 25.18.00	Installed on MFD
8	SW	FAX Software	02.28.033	Installed on MFD
9	SW	Finisher Software (Options) 1K LCSS 2K LCSS HCSS HCSS with BookletMaker High Volume Finisher (HVF) HVF with BookletMaker	 01.27.00 03.40.00 13.40.00 24.16.00 04.03.51 03.06.06	Installed on MFD
10	SW	Scanner Software (Options) 5632/5655/5665/5675/5687 Models 5638/5645 Models	 04.22.00 17.05.00	Installed on MFD
11	DOC	System Administration CD1 [9]	538E11430 June 12th, 2007	CD
12	DOC	Xerox IUG CD 2 [10]	538e11441 September 14th, 2007	CD
13	DOC	Secure Installation and Operation of Your WorkCentre 5632/5638/ 5645/ 5655/5665/5675/5687 [11]	1.4 March 20th, 2009	Download from Xerox-Webpage: http://www.xerox.com/security
14	DOC	WorkCentre 5632/5638/5645/ 5655/5665/5675/5687 Quick Use Guide [12System Software 21.113.02.000]	604P19210	Paperform

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.

The TOE is labelled with the model name and model number (e.g. Xerox WorkCentre 5632). The customer can compare the information given on the physical batch on the TOE to the model numbers given in table 2 above or in the Security Target [6].

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 the information given in table 2 above or in the Security Target [6].

All guidance documents are labelled with their title, a unique product number and / or with a version number and a date. Details on the correct versions of the guidance documents are given in the table above or within 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:

- Data that is temporarily stored in the TOE shall be encrypted.
- Data that is temporarily stored in the TOE shall be overwritten when it is no longer needed or on demand of the system administrator.
- Communication with the TOE shall be protected from disclosure and manipulation.
- Only authorised users shall be able to use the TOEs Security Functionality.
- The TOE shall enable authorised administrators to manage the TOE Security Functionality.
- The TOE shall audit security relevant events.
- The TOE shall provide a reliable separation between the internal network and the PSTN.

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:

- The network to which the TOE is connected is monitored
- Correctly and accurately functioning network identification and authentication mechanisms
- Protection from disclosure or modification of IPv4 traffic to and from the TOE
- 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.

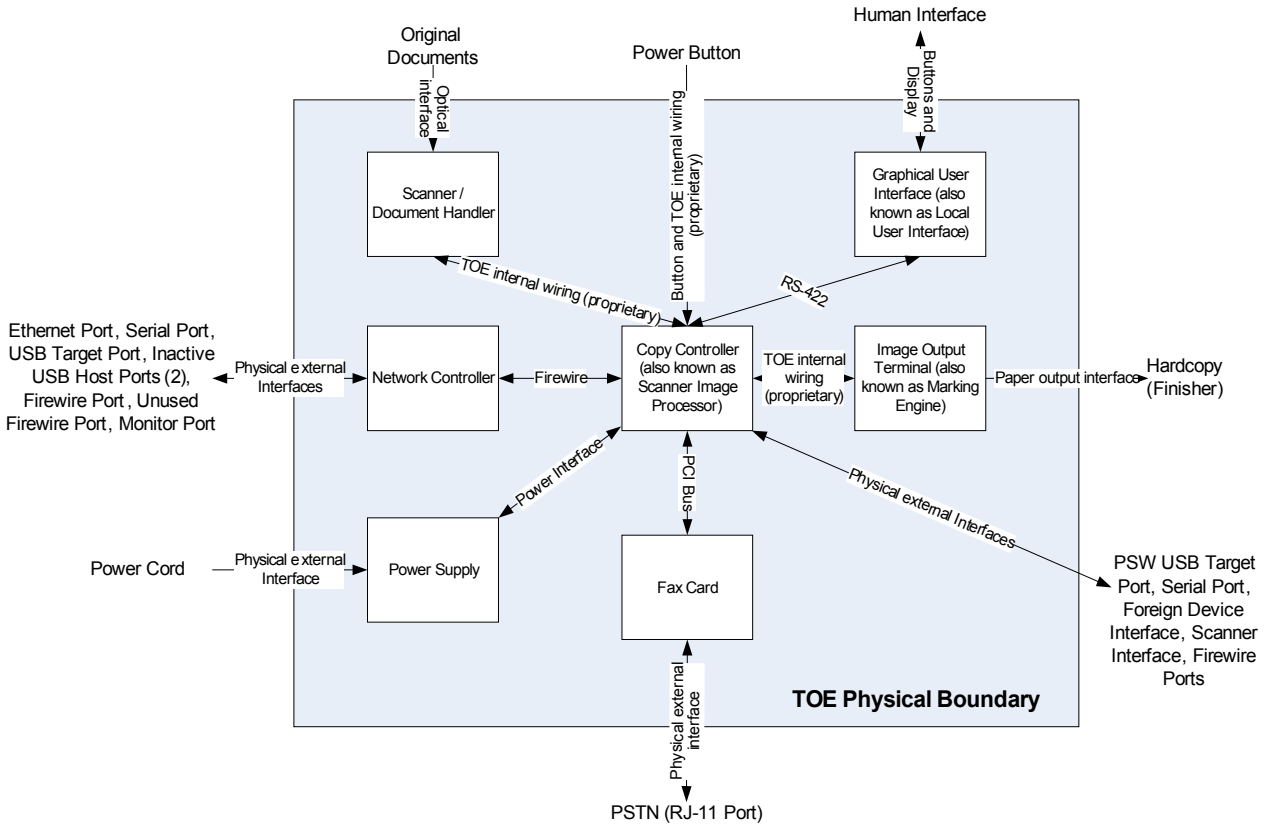

Figure 1: Architecture of the TOE

The copy controller provides all of the functions necessary to implement a digital copier, and works together with the fax card to implement embedded fax functionality.

The network controller provides both network and direct-connect external interfaces, and enables print, email, network scan and LanFAX functionality.

The embedded FAX service uses the installed embedded fax card to send and receive images over the telephone interface.

The purpose of the scanner / document handler is to provide mechanical transport of hard copy originals and to convert hard copy originals to electronic data.

The graphical user interface (GUI) detects soft and hard button actuations, and provides text and graphical prompts to the user. The GUI is sometimes referred to as the local user interface (LUI) to distinguish it from the web user interface, which is exported by the web service that runs in the network controller.

The image output tray / marking engine performs copy/print paper feeding and transport, image marking and fusing, and document finishing.

The power supply provides power to the hardware of the device.

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 was connected to a local LAN. All other test systems were also connected to this LAN. The TOE was 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 used a terminal server for this purpose because the TOE was not located in the office rooms of the evaluator. The terminal server was a Windows 2003 Server with a serial interface and Tutty v0.58.1 as serial terminal software. The evaluator used the remote desktop tool of Windows to access the terminal server.

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

The active directory provided the account directory required by the TOE to identify the users. This directory contained the user accounts of the evaluators. This machine was set on a VMWare virtual machine.

The HTTP(S)- and SNMP-server was required to demonstrate the scan-to-mailbox feature and as destination for SNMP traps. This server ran under Windows 2003 server. HTTPS was provided by Internet Information Services 6.0. SNMP-server was NetSNMP. This server was also a VMWare virtual machine.

The evaluator PC ran under Windows XP. The TOE printer driver and the TOE as system printer were installed. The Windows XP was installed on a VMWare virtual machine.

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 Functional Requirements was successful.

7.3 Independent Evaluator

Due to the fact that the TOE was certified according to EAL2+, which indicates an attack potential of “Basic”, the evaluator did not select a very rigorous testing strategy. Therefore, the evaluator decided to test all Security Functional Requirements with little to medium rigour.

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

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

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

7.4 Penetration Tests

According to the requirements of AVA_VAN.2 the evaluator did a research for common known vulnerabilities for this product or product type. The evaluator found some potential vulnerabilities which were further examined by penetration tests. The tests included network scans, tests of the login mechanisms and verification of the correct operation at the technical limits (e.g. print file size) of the TOE.

The results of the penetration tests showed that there is no exploitable vulnerability in the TOE for attackers possessing only basic attack potential.

8 Evaluated Configuration

In the evaluated configuration covered by this certification the following obligations and hints have to be considered:

- There is no physical access to the TOE for attackers.
- The minimum length of the administrator PIN is 8 alphanumeric characters.
- Image Overwrite Security accessory is installed and enabled.
- The FAX option, if purchased by the consumer, is installed and enabled.
- The following security functions are set up and enabled:
  - Disk Encryption
  - IP Filtering
  - Audit Log
  - SSL
  - SNMP
  - IPSec
  - Trusted Certificate Authorities
- Access on the device services network scanning, scan-to-email and Embedded Fax are locked to everyone but authenticated users.

- IPSec is available only with IPv4, and is not available for either the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport. IPSec also does not protect the IPv6 protocol.
- IP Filtering is available only with IPv4, and is not available for either the Ipv6 protocol, the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport.

Moreover, the details given in the document „Secure Installation and Operation of Your WorkCentre™ 5632/5638/5645/5655/5665/5675/5687" related to the previously listed aspects have to be regarded. The document can be obtained on the Xerox homepage http://www.xerox.com/security.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The component ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- 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 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 vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the following TOE Security Functions:

- TSF_FCS – Cryptographic Support (algorithms see below)
- TSF_FDP_SSL – User Data Protection – SSL (RSA-1024, RC4-128)
- TSF_FDP_IPSec – User Data Protection – IPSec (TDES-168, MD5, SHA-1)
- TSF_NET_MGMT – Network Management Security (MD5, DES-64)
- TSF_EXP_UDE – User Data Protection – AES (AES-128)

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.

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

AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DES	Data Encryption Standard
DoD	Department of Defense
EAL	Evaluation Assurance Level
FAX	Facsimile
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
LAN	Local Area Network
LUI	Local User Interface
MD5	Message Digest 5 Algorithm
MFD	Multifunction Device
PP	Protection Profile

PSTN	Public Switched Telephone Network
RSA	Rivest, Shamir, & Adleman (public key encryption technology)
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TSF	TOE Security Functionality

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 - An 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 - A set consisting of all hardware, software, and firmware of the 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. 2, September 2007

[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 in the BSI Website

[6] Security Target BSI-DSZ-0516-2009, Revision 1.21, April 08th, 2009, “Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target”, Xerox Corporation

[7] Evaluation Technical Report, Version 1.0, April 09th, 2009, CSC Deutschland Solutions GmbH, (confidential document)

[8] Configuration list for the TOE, Version 1.5, April 08th, 2009, “WorkCentre 5632/5638/5645/5655/5665/5675/5687 CI List for Evaluation Evidence” , Xerox Corporation (confidential document)

[9] System Administration CD1, Version 538E11430, June 12th, 2007, Xerox Corporation

[10] Xerox IUG CD 2, Version 538e11441, September 14th, 2007, Xerox Corporation

[11] Secure Installation and Operation of Your WorkCentre 5632/5638/5645/ 5655/5665/ 5675/5687, Version 1.4, March 20th, 2009, Xerox Corporation

[12] WorkCentre 5632/5638/5645/5655/5665/5675/5687 Quick Use Guide, Version 604P19210, Xerox Corporation

C Excerpts from the Criteria

CC Part1:

Conformance Claim (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 A.

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 decompositon.

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-

Assurance Class	Assurance Components
	level design presentation
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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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.