Certification Report

EAL 3+ Evaluation of Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-124-CR
Version: 1.0
Date: 26 November 2010
Pagination: i to iii, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratory located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 26 November 2010, and the security target identified in Section 5 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- Xerox is a trademark of Xerox Corporation in the United States and/or other counties.
- Windows is a registered trademark of Microsoft Corporation.

TABLE OF CONTENTS

Executive Summary

Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems (hereafter referred to as Xerox 5632/5638/5645/5655/5665/5675/5687), from Xerox Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation

Xerox 5632/5638/5645/5655/5665/5675/5687 is a family of multi-function devices that include copy, print, scan-to-email[1], network scan[2], and FAX functionality. The product incorporates security features such that temporary files created for these processes are encrypted and then overwritten as the processes complete. Users are required to provide a valid username and password or Common Access Card and PIN to access the product processes.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 4 November 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Xerox 5632/5638/5645/5655/5665/5675/5687, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[3] for this product provide sufficient evidence that it meets the EAL 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.* The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Xerox 5632/5638/5645/5655/5665/5675/5687 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product

[1] Scanned files are emailed to the user.

[2] Scanned files are routed to a directory.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems (hereafter referred to as Xerox 5632/5638/5645/5655/5665/5675/5687), from Xerox Corporation.

2 TOE Description

Xerox 5632/5638/5645/5655/5665/5675/5687 is a family of multi-function devices that include copy, print, scan-to-email[4], network scan[5], and FAX functionality. The product incorporates Image Overwrite Security whereby temporary files created for these processes are overwritten either on demand or as processes complete. Partitions of the hard drive used to store the temporary files are encrypted using CAVP-validated cryptography. Users must provide a valid username and password or Common Access Card and PIN to access the product processes.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Xerox 5632/5638/5645/5655/5665/5675/5687 is identified in Section 5 of the Security Target (ST).

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Xerox 5632/5638/5645/5655/5665/5675/5687:

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	990
Advanced Encryption Standard (AES)	FIPS 197	1471, 1472
Rivest Shamir Adleman (RSA)	FIPS 186-2	719
Secure Hash Algorithm (SHA-1)	FIPS 180-2	1331

[4] Scanned files are emailed to the user.

[5] Scanned files are routed to a directory.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target
Version: 1.0
Date: October 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

Xerox 5632/5638/5645/5655/5665/5675/5687 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

6 Security Policy

Xerox 5632/5638/5645/5655/5665/5675/5687 implements the following security policies:

- an overwrite policy for the overwrite of temporary files created for the print, network scan, scan-to-email, and FAX processes;
- an information flow control policy that prevents data and commands from entering the network via the FAX board;
- encryption policies for the protection of temporary files stored on the hard drive and for the protection of audit data output by the TOE;
- an access control policy whereby users cannot access TOE processes without a valid username and password, or Common Access Card and PIN; and
- an access control policy that restricts IP addresses permitted to communicate with the TOE.

In addition, Xerox 5632/5638/5645/5655/5665/5675/5687 implements policies pertaining to security audit, identification and authentication, and security management.

Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Xerox 5632/5638/5645/5655/5665/5675/5687 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE has been delivered and installed by Xerox-authorized representatives using Xerox delivery and installation guidance. The TOE has been configured by the system administrator in accordance with the administrator and user guidance delivered with the TOE.

- One or more system administrators are assigned to manage the TOE. Procedures exist for granting a system administrator access to the system administrator password for the TOE.

- The system administrators are not careless, willfully negligent or hostile, and will follow the instructions provided in the administrator and user guidance delivered with the TOE.

- All of the systems that communicate with the TOE are under the same management and physical control as the TOE, and are covered by the same management and security policy as the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed in a standard office environment. Because the TOE is under observation by office personnel, unauthorized physical modifications to the TOE and unauthorized attempts to connect to the TOE via its physical interfaces are not possible.

- The network that the TOE is connected to is monitored for unapproved activities and/or attempts to attack network resources.

- All remote products that communicate with the TOE implement the communications protocol in accordance with industry standard practice and work as advertised.

- The IT environment will provide the TOE with the following services: Network Time Protocol; Identification and Authentication; and Authorization.

7.3 Clarification of Scope

Xerox 5632/5638/5645/5655/5665/5675/5687 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The Xerox 5632/5638/5645/5655/5665/5675/5687 comprises two configurations: Single Board Controller (SBC) and Multi Board Controller (MBC). The software/firmware components of each are listed below. The administrator can confirm their product configuration by printing a configuration sheet and checking against the evaluated configuration list.

Software/Firmware Item	MBC	SBC
System Software	021.120.060.00015	025.054.060.00015
Network Controller Software	061.100.08402	061.060.08402
UI Software	020.014.063	025.061.063
IOT Software	092.011.000	092.011.000
SIP (Copy Controller) Software	020.063.000	025.058.000
DADH Software (Options)		
• DADH 75	016.028.000	016.028.000
• DADH 100	020.019.000	020.019.000
• DADH 100 Quiet Mode	025.018.000	025.018.000
Paper Feeder Software	000.040.000	000.040.000
High Capacity Feeder Software	000.010.009	000.010.009
• Finisher Software (Options)		
• 1K LCSS	001.031.000	001.031.000

Software/Firmware Item	MBC	SBC
• LCSS	003.053.000	003.053.000
• HCSS	013.040.000	013.040.000
• HCSS with BookletMaker	024.016.000	024.016.000
• High Volume Finisher (HVF)	004.003.072	004.003.072
HVF with BookletMaker	003.002.005	003.006.006
FAX Software	003.009.009	003.009.009
Scanner Software (Options)		
• 32, 38, 45, 55 PPM	017.005.000	017.005.000
• 65, 75, 87 PPM	004.022.000	004.022.000

9 Documentation

The Xerox Corporation documents provided to the consumer are as follows:

- System Administration CD 1, version 538E11432, December 16th, 2008; and
- Xerox IUG CD 2, version 538E11443, December 16th, 2008.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Xerox 5632/5638/5645/5655/5665/5675/5687, including the following areas:

Development: The evaluators analyzed the Xerox 5632/5638/5645/5655/5665/5675/5687 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Xerox 5632/5638/5645/5655/5665/5675/5687 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Xerox 5632/5638/5645/5655/5665/5675/5687 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the

product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of Xerox 5632/5638/5645/5655/5665/5675/5687 configuration management system and associated documentation was performed. The evaluators found that the Xerox 5632/5638/5645/5655/5665/5675/5687 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Xerox 5632/5638/5645/5655/5665/5675/5687 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Xerox 5632/5638/5645/5655/5665/5675/5687 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Xerox Corporation for Xerox 5632/5638/5645/5655/5665/5675/5687. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Xerox 5632/5638/5645/5655/5665/5675/5687. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the Xerox 5632/5638/5645/5655/5665/5675/5687 in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[6].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of DOMUS IT Security Laboratory test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Image Overwrite: The objective of this test goal is to verify files created during the printing, network scan, scan-to-email and LanFAX processes are overwritten;

c. Identification and Authentication: The objective of this test goal is to ensure that system administrators are required to identify and authenticate themselves prior to gaining access to system administration functions;

d. Network Identification: The objective of this test goal is to verify that the TOE can prevent unauthorized use of installed network options;

e. Audit: The objective of this test goal is to ensure that the TOE generates audit logs;

f. Cryptographic Operations: The objective of this test goal is to ensure that the TOE performs the specified cryptographic operations;

g. User Data Protection – IP Filtering: The objective of this test goal is to ensure the TOE enforces the network information flow control policy controlling network traffic to and from the TOE as configured by the system administrator;

[6] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

h. Information Flow Security: The objective of this test goal is to ensure the TOE controls and restricts information flow between the PSTN port of the optional FAX processing board, if installed, and the network controller;

i. Security Management: The objective of this test goal is to determine the correct operation of the management functions provided by the TOE; and

j. User Data Protection – AES: The objective of this test goal is to ensure the TOE supports encryption and decryption of designated portions of the hard disk where temporary files are stored.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Port Scanning: The objective of this test goal is to determine if Xerox 5632/5638/5645/5655/5665/5675/5687 opens any ports that could be exploited from the network;
- Session Fixation[7]: The objective of this test goal is to determine if Xerox 5632/5638/5645/5655/5665/5675/5687 is vulnerable to the session fixation attack; and
- Denial of Service (DOS) Attack: The objective of this test goal is to determine if Xerox 5632/5638/5645/5655/5665/5675/5687 is vulnerable to a DOS attack causing the network controller to reboot.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

Xerox 5632/5638/5645/5655/5665/5675/5687 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

[7] Session fixation attacks attempt to exploit the vulnerability of a system which allows one person to fixate (set) another person's session identifier (SID).

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Xerox 5632/5638/5645/5655/5665/5675/5687 behaves as specified in its ST and functional specification and TOE design.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 + level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The evaluator found the guidance for the configuration, integration, and use of the Xerox 5632/5638/5645/5655/5665/5675/5687 to be clear. The evaluator recommends that customers follow the provided guidance documentation in order to deploy the Xerox 5632/5638/5645/5655/5665/5675/5687 in its evaluated configuration.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAX	Facsimile
IP	Internet Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September, 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September, 2007.

d. Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems Security Target, 1.0, October 2010.

e. Evaluation Technical Report Version 1.0, Xerox Corporation Xerox WorkCentre 5632/5638/5645/5655/5665/5675/5687 Multifunction Systems EAL3+, 1 November 2010.