Certification Report

EAL 4 Evaluation of WinMagic Inc.

SecureDoc Disk Encryption

Version 4.3C

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-58
Version: 1.0
Date: 4 July 2007
Pagination: i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have 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 2.2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2*. This certification report, and its associated certificate, applies 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 (CSE), 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 CSE, 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.

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 Standard 17025, General requirements for the accreditation of calibration and testing 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, a division of NUVO Network Management, located in Ottawa, Ontario.

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) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 04 July 2007, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked names: SecureDoc is a registered trademark of WinMagic Inc.

TABLE OF CONTENTS

Executive Summary

SecureDoc Disk Encryption, Version 4.3C, from WinMagic Inc., (hereafter referred to as SecureDoc) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation.

SecureDoc is a disk encryption product for use in a Windows 2000/XP/2003 environment running on a PC, workstation platform, or laptop. The SecureDoc product performs disk encryption using Advanced Encryption Standard (AES) encryption algorithm on hard disks, logical segments of disks, or removable media such as floppy disks, flash disks, and USB Drives.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 25 May 2007, 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 SecureDoc, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of SecureDoc are advised to verify that their own 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)[1] for this product provide sufficient evidence that it meets the EAL 4 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r311* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r311*.

The Communications Security Establishment, as the CCS Certification Body, declares that the SecureDoc evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

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

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is the SecureDoc Disk Encryption, Version 4.3C, from WinMagic Inc. (hereafter referred to as SecureDoc).

2 TOE Description

SecureDoc is a disk encryption product for use in a Windows 2000/XP/2003 environment running on a PC, workstation platform, or laptop. SecureDoc performs disk encryption using Advanced Encryption Standard (AES) encryption algorithm on hard disks, logical segments of disks, or removable media such as floppy disks, flash disks and USB Drives.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SecureDoc is identified in Section 5 of the ST.

The following Government of Canada approved algorithms were evaluated for correct implementation in SecureDoc: AES; SHA-1,256, 384, 512; HMAC; and RNG. As part of the CC evaluation effort, the evaluator made use of results generated under the Cryptographic Module Validation Program (CMVP), namely AES (certificate #359); SHA (certificate #434); HMAC (certificate #158); and RNG (certificate #172). In addition, the cryptographic module implemented in the TOE, SecureDoc Cryptographic Engine version 4.5, passed NIST FIPS 140-2 validation and received certificates #698 for Level 2 and #699 for Level 1.

4 Security Target

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

Title: SecureDoc Disk Encryption Version 4.3C Security Target
Version: Version 1.11
Date: 14 May 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r311*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r311*, incorporating all final CC interpretations. SecureDoc 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 4 conformant with all the security assurance requirements in the EAL 4 package.

6 Security Policy

SecureDoc implements the following Security Policies:

- Access Control implements a set of rules that determines what kind of access an authenticated user has to a security-relevant object;
- Identification and Authentication requires a user to authenticate at pre-boot prior to any other actions involving encryption/decryption access of protected data;
- Cryptographic Keys Management denies access to cryptographic keys and encrypted data unless the user is successfully authenticated and has appropriate privileges; and
- Audit Security will track and save security related transactions and save them in a protected storage area. The audit log is restricted and can only be viewed by authorized users. The audit information provides a time stamp as to when the transaction was filed, and the event information of the transaction.

Full details on the SecureDoc security policy can be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SecureDoc should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of SecureDoc.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

The selection of personnel for administrative roles with respect to the deployment of the TOE and use in the organization must include a proper background check of the individual or be justified by mitigating circumstances that provide the organization with the assurance that administrators will demonstrate competence in their duties and not deliberately misuse or subvert the TOE for non-secure, fraudulent or other improper purposes.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which electromagnetic emissions countermeasures are mandatory or recommended by the environment system's responsible authority;

- The physical environment allows users to enter passwords without being directly observed by other users or potential threat agents; and

- The sensitivity of information assets under protection by the TOE in its environment do not exceed that for which the symmetric encryption algorithms supported by the TOE (256-bit AES) are recommended by the environment system's responsible authority.

For more information about the TOE security environment, refer to section 3 of the ST.

7.3 Clarification of Scope

SecureDoc is a disk encryption software product. The TOE relies upon the underlying operating system, tokens, smart cards, biometrics, and Trusted Platform Module (TPM) within the IT Environment for the following security functional requirements:

- FPT_STM.1 - Reliable time stamps; and

- FIA_UAU.5 - Multiple authentication mechanisms

8 Architectural Information

SecureDoc is composed of the following functional layers:

- The **application layer** delivers the functionality to the user and contains all visible interfaces. All executables belong to this layer, which comprises the following subsystems:

  User Authentication
  Disk and File Encryption
  Installation and Maintenance

- The **low-level components layer** incorporates most critical and sensitive functions like media conversion, encipherment, access control, etc. This layer also manages interfaces to hardware media: hard drives, floppies, flash drives and tokens.
  The subsystems included in this layer are:

  Cryptographic Engine
  Disk Access

- The **intermediate layer** serves as an interface between the application layer and the low-level component layer. Its goal is to deliver the functionality in the form of general operations performed by applications. In addition, the intermediate layer delivers some non-security or supplementary functions shared by applications.

9 Evaluated Configuration

SecureDoc is a disk encryption product for use in a Windows 2000/XP/2003 environment running on a PC, workstation platform, or laptop. For the purposes of this evaluation, the evaluated configuration of the TOE consisted of Version 4.3C of the TOE installed on a HP tablet PC with Windows XP Tablet PC Edition 2005, Service Pack 2.

10 Documentation

SecureDoc documents provided to the consumer are as follows:

- SecureDoc Enterprise Edition Client Manual Version 4.3;
- Readme for SecureDoc Version V4.3C for Windows 2000/XP/2003; and
- SecureDoc Disk Encryption Setup Guide.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of SecureDoc, including the following areas:

Configuration management: An analysis of the SecureDoc development environment and associated documentation was performed. The evaluators found that the SecureDoc configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of SecureDoc during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed SecureDoc functional specification, high-level design, low-level design, and a subset of the implementation representation; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined SecureDoc user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to

securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of SecureDoc design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

Vulnerability assessment: The evaluators analyzed the administrator guidance to ensure the absence of ambiguities that could result in inadvertent misuse of SecureDoc. Meanwhile, the strength of function claim in the ST was validated through independent evaluator analysis. Further, the evaluators examined the developer's vulnerability analysis for SecureDoc and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators performed independent vulnerability analysis, including a review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer had considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL4 consists of the following activities: assessing developer tests in terms of coverage and depth, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR) [2].

The evaluator assessed SecureDoc's test documentation for both coverage and depth. The evaluator found that the developer's test documentation was sufficient to demonstrate that security functions perform as specified, and that the security functionality has been systematically tested against the functional specification and high-level design.

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

12.2 Independent Functional Testing

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

The tests focused on the following areas, based upon the security functional requirements in the ST and the security functions defined in the functional specification:

- Cryptographic Support;
- Identification and Authentication;
- Session Control;
- Access Control;
- Protection of the TOE Security Functions;
- Audit;
- Fault Tolerance; and
- Security Management.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the test procedures and results. All independent functional tests yielded the expected results.

12.3 Independent Penetration Testing

During the evaluation, the evaluator developed independent penetration tests based on the SecureDoc vulnerability analysis, as well as the functional specification, high-level design, low-level design, implementation representation, guidance documentation, and installation guidance.

The penetration tests focused on:

- Direct access to underlying data storage for TSF data;
- Bypass attempts by manipulating the configuration file;
- Tampering of crucial TOE components; and
- Network access to data storage under protection.

No exploitable vulnerabilities were uncovered during the independent penetration testing.

12.4 Conduct of Testing

SecureDoc was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the WinMagic Inc.'s facility in Mississauga, Ontario, and the ITSET facility at DOMUS IT Security Laboratory located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and independent functional tests yielded the expected results, giving assurance that SecureDoc behaves as specified in its ST and functional specification. The penetration testing resulted a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in SecureDoc Disk in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

Over the course of the evaluation, the evaluators noted that the TOE is a mature and easy-to-use product, supported by a well-established development team. The evaluators also observed that the TOE documentation is complete, accurate and highly professional in presentation.

The data objects must be configured to reside on the disk/partition/USB-drive under protection by SecureDoc. If they are situated on another unprotected drive, or exposed in a network by sharing the encrypted disk/partition, the encryption services of SecureDoc are not designed to protect them from unauthorized access.

It is also well advised to have a state of the art virus-checking program to ensure viruses are not introduced and to follow best practices to secure the network to protect against network attacks. The systems under the protection of SecureDoc should be regularly patched with latest security updates. Only software approved by the system administrator should be installed on the platform that SecureDoc is protecting to prevent the importation of Trojan horses or other destructive software.

Further consultation with specific application user manuals may be necessary to extend this list for a specific environment.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
AES	Advanced Encryption Standard
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Hash Message Authentication Code
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
RNG	Random Number Generator
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TPM	Trusted Platform Module

16 References

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

a) Common Criteria for Information Technology Security Evaluation, Version 2.2, September 2004.

b) Common Methodology for Information Technology Security Evaluation, Version 2.2, September 2004 .

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) SecureDoc Disk Encryption Version 4.3C Security Target, Version 1.11, 24 April 2007

e) Evaluation Technical Report for EAL4 Evaluation of SecureDoc Disk Encryption Version 4.3C, Version 0.8, 25 May 2007