Certification Report

EAL 1 Evaluation of SecureDoc Disk Encryption

Version 2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 1999-LGS-01
Version: 1.02
Date: April 18, 2000
Pagination: i to iii, 1 to 9

DISCLAIMER

The IT product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 0.6, for conformance to the Common Criteria for IT Security Evaluation, Version 2.0. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, is either expressed or implied.

FOREWORD

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

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the ISO Guide 25, 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.

By awarding a certificate, a certifying body asserts, to some degree of confidence, that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification-like document that defines and scopes the evaluation activities. The consumer of certified IT products should review the ST, in addition to the certification report, in order to gain an understanding of any assumptions made during evaluation, the IT product's intended environment, its security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. The ST associated with this Certification Report (CR) is identified by the following nomenclature:

SecureDoc™ Disk Encryption V.2.0
Security Target
Common Criteria EAL 1
Version 1.4
Dated: July 15, 1999

This Certification Report is associated with the Certificate of Product Evaluation dated August 27, 1999.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SecureDoc Disk Encryption, version 2.0 for Windows 95/98 and Windows NT, from WinMagic Inc., is the Target of Evaluation (TOE) for this EAL 1 evaluation. The SecureDoc 2.0 Disk Encryption product controls access to disk partitions or entire disks by encryption (DES, Triple DES, or CAST5) using keys assigned to established user accounts. Once SecureDoc has been installed and keys and user accounts have been created, a user need only log on to the platform and request access to a file. SecureDoc works at the BIOS level to identify and authenticate the user via a password mechanism. Based upon the identity of the user, SecureDoc will determine if the user has been assigned the key to decrypt the disk or partition on which the file resides. If the user has been assigned the key, SecureDoc will use the key to transparently decrypt the disk or partition and make the original text of the file available to the user.

The threats that are countered by SecureDoc include: unauthorized access to information or resources (via encryption); corruption of the encryption process due to loss of power or an operating system fault; and denial of access resulting from users forgetting their passwords and thus not having access to their encryption keys.

SecureDoc's use of the DES, Triple-DES and CAST5 algorithms and associated key lengths was validated under the Cryptographic Module Validation Program (CMVP). The Common Criteria evaluation verified that no plaintext remained in areas of disk media encrypted using SecureDoc. The cryptography, however, was not validated to FIPS 140-1, meaning that the ability of cryptography to withstand a concerted attack effort is unknown and cannot be inferred from the algorithm validation effort.

The Common Criteria Evaluation Facility (CCEF) conducting the evaluation was Information Technology Security Laboratory, DOMUS Security, a division of LGS Group, Inc. The evaluation was completed on July 23, 1999. Cryptographic validation was performed under the CMVP by the same facility and was completed on April 6, 2000.

The evaluation of SecureDoc Disk Encryption has determined that the TOE can be trusted to a level of assurance of **EAL 1**, to conform to the requirements of the *Security Target* (ST) [5]. The TOE is CC Part 2 conformant (functional requirements from CC Part 2 only) and CC Part 3 conformant (assurance requirements from CC Part 3 only).

The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS). The Canadian CCS has established a Certification Body that is managed by the Communications Security Establishment (CSE). The evaluation was performed using the Common Criteria (CC) [1] and applied using the *Common Methodology for Information Technology Security Evaluation* (CEM) [3,4].

The scope of the evaluation is defined by the ST, which identifies assumptions made during the evaluation, the IT product's intended environment, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers of SecureDoc are advised to verify that their own environment is consistent with the ST [5], and to give due consideration to the comments, observations and recommendations stated in this report.

The information contained in this document is supported by evidence contained in the detailed *Evaluation Technical Report* (ETR) [6] and algorithm validation report [9].

1 Identification of Target of Evaluation

The evaluated product is SecureDoc™ 2.0 Disk Encryption for Windows 95/98 and NT, with no SecureDoc upgrades or service patches.

2 Security Target

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

SecureDoc Disk Encryption V.2.0
Security Target
Common Criteria EAL 1
Version 1.4
Dated: July 15, 1999

3 Security Policy

SecureDoc provides access control to entire disks and partitions through encryption. One of three algorithms, DES, Triple DES, or CAST, can be selected as the encryption algorithm when keys are generated. SecureDoc by default uses Triple DES as the encryption algorithm. Only administrators can generate keys for disk and disk partition encryption.

SecureDoc allows the administrator to create an emergency backup key database. This database can be used at any time by entering the name of the database at Boot Logon. Boot Logon prompts the administrator for their login password following the entry of the key database name.

Keys can be exported from SecureDoc in key files. SecureDoc associates a password with the key file. The key file cannot be imported unless the correct password is entered.

An administrator can set access profiles for disks or partitions. Available access restrictions are write only if encrypted, read and write access, and no access. SecureDoc has two control features for the profile: "Alert" and "Lock". The "Alert" setting will result in warning messages being displayed when the specified drive is accessed contrary to the restriction; "Lock" disallows the access. Partitions with NT File System format cannot be configured for read-only access. Disk "Lock" cannot be applied to the root drive containing the system files.

SecureDoc has two roles: an Administrator role and a User role. Operators in the Administrator role can create key databases; generate, import and export keys; create user accounts; change user database names; and customize SecureDoc such as setting the minimum password length. Operators in the User role can read and write to encrypted

disks for which they have been given access and can change their password. They cannot generate new keys, export or import them.

At the SecureDoc Control Center, the user is prompted for a database name and its associated password. If the password is incorrectly entered five times consecutively, the system is locked and must be re-booted.

When the PC boots up with Boot Logon installed, the user is prompted for a database name and password. (The only time the database name and path are entered at this screen is when the key database file is not on the C:\ drive, but instead is stored on a floppy diskette.) The password associated with this database must then be entered. If the password is incorrectly entered three times consecutively, the system is locked and must be re-booted.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For SecureDoc to be used securely, it should be installed following the guidelines outlined in the User's Manual, *SecureDoc Ver. 2.0 For Windows 95/98/NT User's Guide* [7]. The sensitivity of the information assets protected by SecureDoc should not exceed the sensitivity for which at least one of the three implemented cryptographic algorithms, DES, Triple DES, and CAST5, is recommended by the consumer's organisational security policy.

4.2 Environmental Assumptions

It is assumed that administrators of SecureDoc can be trusted by the organization to perform their administrative tasks securely. It is also assumed that keystrokes used for entering a password cannot be observed either by another user or threat agent or be recorded by a video camera. Passwords should only be provided to authorized users.

4.3 Clarification of Scope

The evaluation verified that no plaintext remained in areas of disk media encrypted using SecureDoc. SecureDoc's use of the DES, Triple-DES and CAST5 algorithms and associated key lengths were validated under the Cryptographic Module Validation Program (CMVP). Specifically, the DES and Triple-DES algorithms were validated to FIPS 46-3 and FIPS 81. The same CMVP approved laboratory, using test vectors provided by the Canadian CCS certification body, validated the CAST5 algorithm. The cryptography, however, was not validated to FIPS 140-1 meaning that the ability of cryptography to withstand a concerted attack effort is unknown and cannot be inferred from the algorithm validation effort.

To fully protect all information, all applications, and the operating system with SecureDoc, the entire hard disk should be encrypted and Boot Logon should be installed. If, however, only a partition of the disk is encrypted, all sources of sensitive information (temporary files, paging files, etc.) should be located in folders on the protected partition. In the case of the entire disk not being encrypted, there is the potential for attacks on the operating system.

If an emergency backup key database is not created and the key database on the platform is destroyed or corrupted, encrypted information cannot be recovered.

5 Architectural Information

SecureDoc has a dynamic link library, "SecurDoc.DLL", which interfaces to all SecureDoc components including the SecureDoc Control Center. The SecureDoc Control Center provides administrative services including key database creation, key export and import, user account creation, name and password changes and profile creation and deletion.

"SecurDoc.DLL" is the interface for another SecureDoc component, "SecurDoc.SYS". "SecurDoc.SYS" is a device driver that performs the encryption and decryption when an operator reads files from, or writes files to, an encrypted disk or partition.

SecureDoc also has a Boot Logon component to authenticate users before the operating system is loaded. This allows the entire hard disk and all of its contents, such as the Windows start-up files, to be encrypted. Boot Logon interfaces directly with the BIOS and the BIOS controls the I/O devices. Boot Logon authenticates the user to the PC or system on which SecureDoc resides.

6 Documentation

SecureDoc™ Version 2.0 Disk Encryption product comes with a copy of their user manual, *SecureDoc Ver. 2.0 For Windows 95/98/NT User's Guide* [7]. The manual provides installation information, user guidance and administrator guidance.

7 ITS product testing

Developer testing is not required for EAL1. The evaluator approach to testing was to functionally test each and every security function of SecureDoc that was specified in the Security Target. A hex reader, ZipZap 7.15, was utilized to verify that data was not in readable plaintext format. The executable of SecureDoc available both on CD-ROM and at their website were tested.

The evaluator installed SecureDoc and verified that the installation coincided with the documentation provided by WinMagic. The process included the creation of a key backup diskette. The various administrator functions were tested, including the import, export and deletion (via zeroization) of cryptographic keys, creating users, encrypting disk partitions, and creating each type of access profile (which set the conditions under which read and write operations are permitted for a disk partition). The various methods of logging into and out of SecureDoc were tested to ensure that individuals could not gain unauthorized access to protected files. Numerous tests were run to ensure that a user could not access any disk partitions except for those that were encrypted by a key assigned to that user.

In addition to the above tests, the ability of SecureDoc to successfully complete encryption operations on a disk partition was tested, by powering down the PC in the middle of an encryption operation in one case, or by removing a floppy diskette during an encryption operation to that diskette. In these cases, it was verified that the encryption operations were successfully completed once either power was restored (in the first case) or once the diskette was returned to the floppy drive.

Validation of the cryptographic algorithms was performed as a related but separate activity under the CMVP program. The same laboratory (and staff) that performed the CC evaluation also performed the algorithm validations.

8 Evaluated Configuration

The SecureDoc™ Version 2.0 Disk Encryption product has been developed to run on Microsoft Windows 95 or 98 and Microsoft Windows NT version 4.0 and designed to be used on a PC or workstation. SecureDoc was evaluated on a PC running Microsoft Windows NT version 4.0.

SecureDoc was evaluated both with Boot Logon installed and without Boot Logon installed. An emergency backup key database, which was stored on a floppy diskette, was created in both cases. SecureDoc has a Wizard, which is used to install and configure the product. The guidance provided in the user manual and online was followed in the installation of SecureDoc for evaluation.

9 Results of the Evaluation

The security functionality for SecureDoc™ Version 2.0 Disk Encryption product that was specified in the Security Target, *SecureDoc Disk Encryption V.2.0 Security Target Common Criteria Version 1.4* [5], was found to be correctly implemented in the product to the Common Criteria EAL1 level of assurance.

10 Comments, Observations and Recommendations

10.1 Comments and observations

The following observations were noted during the course of the evaluation.

After installing SecureDoc, the administrator requires a default user name in order to change the administrator password, which was not provided. WinMagic has issued an addendum with the SecureDoc product, which indicates the default user name to be used is the key database file name, without the file name extension.

When the PC boots up with Boot Logon installed, the user is prompted for the name of the key database file and its associated password. If the default database file on the C:\ drive is to be used, the operator will press the 'Enter' key in response to the key database file name prompt and then enter the password in the password field. If the key database file to be used is on a floppy diskette or token, the full path and name of the key database must be entered at the file name prompt and the password for this database must be entered in the password field

During the course of testing, it was discovered that a request to generate more than eight keys could be made, that appeared to be contrary to the User Guide, which stated that eight is the maximum number of keys that can be stored in one key database. However, while names could be created for these keys, they could not actually be saved to disk.

10.2 Recommendations

It is recommended that the sensitivity of the information protected by SecureDoc be of a degree by which DES, Triple DES, or CAST5 is sufficient, as determined by the consumer's security policy, to provide adequate confidentiality. It is also recommended that the guidance provided in *SecureDoc Ver. 2.0 For Windows 95/98/NT User's Guide* concerning password selection, creation of an emergency key database, and trial usage is followed.

It is recommended that an administrator use full disk encryption with Boot Logon to ensure that plain-text information (files, applications, operating system) is **not** available from the disk; this is the most secure option.

If only part of the disk is encrypted, special care must be taken to ensure that no copies of plain-text information are accidentally made available. All files such as:

- text files and cookies (*.txt),
- document files (*.doc),
- compressed files (*.zip),
- information files (*.inf),

- data files (*.dat),
- database files (e.g. *.mdb),
- temporary files (those in the *Microsoft* "TEMP" folder), and
- files in the *Microsoft* Recycle Bin

should be located on a protected partition.

Finally, an administrator should create an emergency backup key database to be used in case the key database on the platform is destroyed.

11 Glossary

This section expands upon abbreviations and acronyms, and defines vocabulary used in a special way to help increase the readability of this report.

Abbreviation	Description
CC	Common Criteria
CB	Certification Body
CCEF	Common Criteria Evaluation Facility
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Evaluation Methodology
CMVP	Cryptographic Module Validation Program
CR	Certification Report
CSE	Communications Security Establishment
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Functional Specification
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
NTFS	Network Transfer File System
PALCAN	Program for the Accreditation of Laboratories Canada
PCR	Preliminary Certification Report
ST	Security Target
TOE	Target of Evaluation

Word	Explanation
CAST/CAST5:	Symmetric cryptographic algorithm developed by Carlisle Adams and Stafford Tavares.

Disk Profile:	An access control used by administrators to restrict or limit a user's access to a disk. The profile can be one of the following: no restrictions, write only if the disk is encrypted, read only access, or no access at all.

12 References and bibliography

This section lists all documentation used as source material in the compilation of this report:

1. Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998;

2. Canadian Common Criteria Evaluation and Certification Scheme (CCS), Technical oversight, CCS#4, Version 0.82 - Draft;

3. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, 11 January 1997;

4. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation methodology, Version 0.6, January 1999;

5. Domus Security Division, LGS Group Inc., SecureDoc Disk Encryption V.2.0 Security Target Common Criteria Version 1.4, 15 July 1999;

6. Domus Security Division, LGS Group Inc., Evaluation Technical Report, Document CC-3151-008-ETR, 23 July 1999;

7. WinMagic Inc., SecureDoc Ver. 2.0 For Windows 95/98/NT User’s Guide, 1999;

8. WinMagic Inc., SecureDoc Ver 2.0 Informal Functional Specification (ADV_FSP.1) Release 1.2, 22 July 1999.

9. Domus Security Division, LGS Group Inc., Draft Report on Conformance Testing of Triple-DES, DES and CAST128 in Version 2.0 of WinMagic Inc.'s SecureDoc Disk Encryptor, LGS, 6 April 2000.