UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P227

SafeBoot Device Encryption for PC
Version 5.0

Issue 1.0

May 2006

UK Certification Body,
CESG, Hubble Road,
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor / Developer	**SafeBoot N.V.**
Product and Version	**SafeBoot Device Encryption for PC Version 5.0**
Description	SafeBoot Device Encryption for PC is a personal computer hard disk encryption system.
CC Part 2	**Conformant**
CC Part 3	**Conformant**
EAL	**EAL 4**
CLEF	**BT**
Certifier	**CESG**
Date authorised	23 May 2006

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 [a] - [c]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [d], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations .

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of SafeBoot Device Encryption for PC Version 5.0 to the Sponsor, SafeBoot N.V., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

SafeBoot Device Encryption for PC Version 5.0.

4. The Developer was SafeBoot N.V.

5. SafeBoot Device Encryption for PC is a disk encryption system for personal computers running the Microsoft Windows XP Professional or Windows 2000 Professional operating systems. It prevents data stored on a PC's hard disk from being accessed by an unauthorised person. SafeBoot Device Encryption for PC takes control of a user's hard disk away from the resident operating system, encrypting data written to the disk and decrypting data read from the disk.

6. SafeBoot Device Encryption for PC Client consists of a boot operating system (the SafeBoot OS), a Basic Input Output System (BIOS) hook, Windows drivers, a system tray application and a set of Windows Dynamic Link Libraries (DLLs).

7. The evaluated subset and configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

8. The TOE is SafeBoot Device Encryption for PC Client software installed on a single client PC. The IT environment consists of the PC and its operating system, either Microsoft Windows XP Professional or Microsoft Windows 2000 Professional. Included within the IT environment (but outside the scope of this evaluation) in order to facilitate correct operation of the TOE are the following SafeBoot Device Encryption for PC entities – SafeBoot Administrator, SafeBoot Server, and the SafeBoot Object Directory, all at version 5.0. These entities are connected remotely over a TCP/IP network.

9. SafeBoot Device Encryption for PC has three configuration modes, determined at setup by the SafeBoot Administrator, specifying the types of hard disk encryption employed - full, partial or none. Full encryption is the only mode considered under this evaluation.

10. The implementation of the cryptographic algorithms used by the TOE to encrypt data on the hard disk are out of scope of this evaluation, although the calls to these algorithms are considered.

11. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Protection Profile Conformance

12. There is no claimed compliance to any protection profiles.

Security Claims

13. The Security Target [d] fully specifies the TOE's security objectives, the Organisational Security Policies (OSPs) which these objectives support and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

14. The TOE security policies are detailed in the Security Target [d].

Strength of Function Claims

15. **The minimum Strength of Function (SoF) was SoF-Medium**. The strength of function claim applies to the password authentication mechanism only. **The Certification Body has determined that these claims were met.**

16. For the TOE to be used in a CC compliant mode it must be configured for use with a minimum password length of five characters and to lock after ten unsuccessful entry attempts. The SafeBoot administrators guide [j] provides further details.

17. The TOE uses a variety of cryptographic keys and algorithms. It should be noted that none of these have been included in this evaluation and no claims have been made about their strength of functions in this context.

Evaluation Conduct

18. The Certification Body monitored the evaluation which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in April, 2006, were reported in the ETR [i].

Conclusions and Recommendations

19. The conclusions of the Certification Body are summarized in the Certification Statement on page 2.

20. **Prospective consumers of SafeBoot Device Encryption for PC Version 5.0 should understand the specific scope of the certification by reading this report in**

conjunction with the Security Target [d]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

21. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

22. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

23. **Certification is not a guarantee of freedom from security vulnerabilities**; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

24. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

25. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.**

26. The TOE is delivered to customers either on CD or as a download from the SafeBoot FTP server. Secure delivery is ensured by procedures for checking that modification to files has not taken place in transit. MD5, SHA1 and SHA256 hashes are created during the release process, from release images of the TOE (including documentation). Hashes are maintained by the Product Manager who distributes them via email when requested by customers.

27. A text file on the CD contains detailed instructions on how to verify its contents. This is done by using the hash values, obtained from SafeBoot via email, with the hash tool provided on the SafeBoot website or alternatively using a third party tool.

28. Correctly matching hash values indicate that the TOE contents, as delivered on the CD or downloaded by FTP, and the security of the TOE have not been compromised during delivery.

Installation and Guidance Documentation

29. A description of the installation and configuration procedures is contained in the Quickstart Guide [k] and in Section 17 of the administration guide [j]. **It is important that instructions in the administrators guide [j] are followed to ensure that the TOE runs in the evaluated configuration.**

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is uniquely identified as: SafeBoot Device Encryption for PC Version 5.0.

31. The image on both CD and the SafeBoot FTP server is identified as:

DE 5.0.0.0 B5000.

32. The TOE consists of the SafeBoot Device Encryption for PC Client software installed on a single PC/laptop.

TOE Documentation

33. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

34. Relevant documentation is included within the TOE image on the CD or downloadable from the SafeBoot FTP server.

TOE Scope

35. The TOE consists of the SafeBoot Device Encryption for PC Client software that is part of the SafeBoot Device Encryption for PC Version 5.0. The application software is physically bounded by the PC on which the software is installed.

36. The SafeBoot Device Encryption for PC software also comprises an Administration Server consisting of SBAdmin, SBServer and the SafeBoot Object Directory. The Administration server was used during evaluation to test the client interfaces. As such, the Administration Server was exercised during testing to provide assurance as to its effectiveness and to provide assurance of its support for the security of the TOE. However, it should be noted that the Administration Server was not within the scope of the EAL4 evaluation.

37. The cryptographic functions (AES, SHA-1 and DSA) used in the TOE are out of scope and were not considered during the evaluation.

TOE Configuration

38. The TOE should be configured in accordance with the administrators guide [j].

39. SafeBoot Device Encryption for PC Client may be configured in one of three possible encryption modes: full, partial or none. Further details are provided in the administrators guide [j]. Only the full encryption mode is valid for Common Criteria compliant operation. This is defined as follows:

- Passwords must be restricted to a minimum of five characters
- Passwords must be invalidated after ten unsuccessful logon attempts
- Partitions on the hard disk must be fully encrypted

- Users must be forced to logon
- The SafeBoot Device Encryption Client screen saver must be enabled, with password protection.

Environmental Requirements

40. Details of the TOE's environmental configuration are summarised above under 'TOE Scope'.

41. The Security Target [d] includes a number of assumptions about the environment. These include authentication of trusted users; administration of the TOE and the security of its data.

42. The TOE's IT environment includes the SafeBoot Administration Server which enables generation of the SafeBoot Device Encryption PC Client installation set and remote administration of the security functions of the TOE.

Test Configuration

43. The diagram below shows the test configuration. Details of the machines used during testing are as detailed:

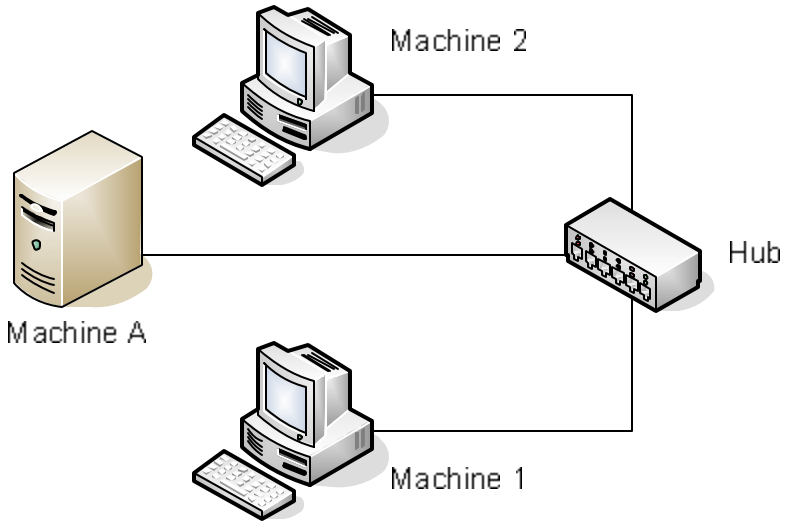
TOE – SafeBoot Device Encryption for PC Client

- Machine 1 – Dell Dimension 2400, Intel Celeron 2.6 GHz, 256 MB RAM, 40GB HDD; running Windows XP Professional with SP2 then Windows 2000 with SP4.
- Machine 2 – HP Compaq D530C, Intel Pentium 4 2.66GHz, 256MB RAM, 9GB HDD; running Windows XP Professional with SP2.

IT environment – Administration Server

- Machine A – Toshiba Tecra M2, Intel Centrino 1.6GHz, 512MB RAM, 7GB HDD; running Windows XP Professional with SP1.

44. The latest service packs were applied to both client machines. Later patches and hot fixes were not installed, they were deemed to be unnecessary as the TOE has no dependencies on functions in the areas they cover.



45. Machine A acts as the remote PC running the SafeBoot Administration Server, which consists of SBAdmin, SB Server and the SafeBoot Object Directory. These are connected to the SafeBoot Device Encryption PC client machine over a network using the TCP/IP protocol.

46. In the context of this evaluation the Administration Server has been used to provide a human-user interface to the TOE management interface (via TCP/IP network connection). It has been exercised during evaluation testing so as to provide a degree of assurance that it supports the security of the TOE.

IV. PRODUCT SECURITY ARCHITECTURE

47. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

48. SafeBoot Device Encryption for PC is a Personal Computer (PC) security system that prevents the data stored on a PC's hard disk from being read or used by an unauthorised person. The SafeBoot Device Encryption for PC takes the control of a user's hard disk away from the resident operating system, encrypting the data written to the disk and decrypting the data read from the disk. The TOE is the SafeBoot Device Encryption PC client installed on the PC/laptop to be protected.

49. The IT environment of the TOE consists of a PC running either Microsoft Windows 2000 Professional or Windows XP Professional operating systems. The TOE (SafeBoot Device Encryption PC client) runs on this machine.

50. Also included in the IT environment, but outside the scope of the evaluation is the Administration Server which comprises the SafeBoot Administrator (SBAdmin), the SafeBoot Server (SBServer) and the SafeBoot Object Directory. These components run on a remote PC, or PCs, connected to the client over a TCP/IP network.

51. The Admin Server was used during evaluation to test the SafeBoot Device Encryption PC Client. The Security Target [d] provides further details.

52. The TOE depends on the operating system for domain separation, time stamps and the Microsoft GINA API (MSGINA).

Design Subsystems

53. The security functionality is partitioned into the following subsystems:

- Bootcode – provides a pre-boot environment for access control and user authentication
- Int13 Hook – handles encryption and decryption of the hard disk until Windows is loaded
- Windows Encryption Driver – handles all disk access, encrypting and decrypting as appropriate when Windows is loaded
- Client Status Monitor – provides a Windows tray icon to activate the screen saver, show status and force synchronisation
- Disk Manager – is used by SafeBoot Device Encryption for PC applications to access and manage the physical disks
- Client Manager – manages aspects of the client machine that relate to SafeBoot Device Encryption for PC, including synchronisation with the server
- SafeBoot GINA (SBGINA) – allows SafeBoot Device Encryption for PC to provide its token-based access control

- SafeBoot Device Encryption screen saver – after a period of inactivity the screen saver will activate and lock the TOE; SBGINA will prompt a user to unlock the TOE
- Password Token – uses a password to secure user's encryption keys
- Audit – writes audit events to an audit log.

Hardware and Firmware Dependencies

54. The TOE runs on a standard IBM compatible personal computer.

TOE Interfaces

55. SafeBoot Device Encryption for PC Client provides a logical interface exposing the following services:
    - Data input – to all driver functions
    - Data output – from all driver functions
    - Control input – from TCP/IP interface, IPC interface, GUI
    - Status output – return codes from driver functions, Show Status GUI option.

56. The Data Input and Output services provide interfaces to the encryption and decryption functions.

57. The Control input provides a secure management interface through which the SafeBoot Device Encryption for PC Client is configured by the Administration Server.

58. SafeBoot Device Encryption for PC Client also provides a Graphical User Interface (GUI) to the user.

User Access Control

59. Users are required to authenticate themselves by providing a valid identifier and password via the SafeBoot Device Encryption for PC Client logon screen before gaining access to the PC's data.

60. A PC may be locked by activating the SafeBoot Device Encryption Client screen saver. Subsequent unlocking will require authentication by the user.

User Authentication

61. Provides the user password authentication mechanism by checking a password against a securely stored value associated with the user. This functionality is provided by the SafeBoot OS.

Management of the TOE by a User

62. Uses the password authentication mechanism to enable a user to change his password as part of the logon process.

Hard Disk Encryption

63. The hard disk of the TOE is encrypted to prevent unauthorised access to the TOE.

Hard Disk Encryption Key Management

64. Manages the generation and destruction of hard disk encryption keys. The key is stored encrypted, and is decrypted as required.

Administrative Access Control and Secure Management

65. Concerns the management of the TOE via the administration secure management interface over a secure session using authenticated message exchange.

Audit

66. The TOE maintains an audit log listing the events that have occurred on the TOE. The audit function is active whilst the TOE is operational.

Self Protection of the TOE

67. Concerns the functions that protect the TOE to help maintain its integrity in the event of hardware failure or communications link failure.

V. PRODUCT TESTING

IT Product Testing

68. Developer testing covered all aspects of the functional specification including the design subsystems identified in section IV above. The subsystems - BootCode, Client Status Monitor Tests, Client Manager, SafeBoot GINA, SafeBoot Device Encryption client screen saver and Audit have user interfaces or use external interfaces of the TOE. Tests exercising these were performed at the external interfaces of the TOE via mouse, keyboard and network.

69. The subsystems with no external interfaces i.e. Int13 Hook, Windows Encryption Driver, Disk Manager and Password Token, were tested implicitly by testing the above.

70. The Evaluators performed independent functional testing on the TOE between 6 March and 10 March 2006 and between 27 March and 29 March at the BT CLEF in Fleet. A sample of 41% of developer tests were repeated. Some tests were deemed to be operating system independent and were not performed on both operating systems. Each TSF was covered by at least one test. The actual test results were consistent with the expected test results.

71. The Evaluators performed penetration testing which confirmed the SoF claimed in the Security Target [d] for the password authentication mechanism.

Vulnerability Analysis

72. The developers carried out their own vulnerability analysis on the TOE, including searches on the Internet and found no vulnerabilities. The evaluators have examined the developers work and concur with their findings.

73. The Evaluators conducted their own search for known vulnerabilities in the public domain, but no relevant vulnerabilities were identified.

Platform Issues

74. The TOE was tested on the hardware platforms specified above under 'Test Configuration', with each test being performed on the platforms specified.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.0, December 2005.

[d] SafeBoot Device Encryption for PC Version 5 Common Criteria Security Target,
SafeBoot N.V.,
Version 1.0, 19 May 2006

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2005-08-004, Version 2.3, August 2005.

[i] Evaluation Technical Report,
BT,
LFS/T493/ETR, Issue 1.0, 3 April 2006.

[j] SafeBoot 5 Device Encryption Guide
SafeBoot, Version 2006/09, 31 March 2006

[k] SafeBoot Device Encryption Quickstart Guide
SafeBoot, Version 2006/03, 21 March 2006

VIII. ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, PC, HTML, ... or standard Common Criteria abbreviations such as TOE, TSF, ... (See Common Criteria Part 1 [e], Section 2.3)

BIOS	Basic Input Output System
DLL	Dynamic Link Library

[This page is intentionally blank]