Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0553-2012

for

SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7

from

Utimaco Safeware AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0553-2012

SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7

from	Utimaco Safeware AG
PP Conformance:	None
Functionality:	product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 18 June 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

It includes assurance levels beyond EAL4 resp.E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7 has undergone the certification procedure at BSI.

The evaluation of the product SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 9 May 2012. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Utimaco Safeware AG

The product was developed by: Utimaco Safeware AG

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

[6] Information Technology Security Evaluation Facility

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5 Publication

The product SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Utimaco Safeware AG
Germanusstraße 4
52080 Aachen

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the product SafeGuard Enterprise Device Encryption, Version 5.60 provided by Utimaco Safeware AG. The TOE is a software that prevents unauthorized access to clear text of data stored on mobile or stationary block devices. This is achieved by data encryption which is completely transparent to users.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 6.3.

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

TOE Security Function	Addressed issue
Power On Authentication (POA)	POA is a mechanism of the TOE to check the user's authenticity before the operating system on a PC is booted from its boot device.
Protection of Data on Protected Devices	After a successful authentication the cryptographic keys needed to boot the PC are determined out of the user's key ring stored in TSF data. The user's key ring is compiled from one or more key tables after a successful logon to Windows. An access to any encrypted device is only possible if the cryptographic key used for encryption of that specific device is known. Hence, the TOE security function ensures that data provided by authorised users are protected when being stored on encrypted devices and when the PC is not in operation or the device is detached from a PC in operation.
Secure Server-Based Administration	The administration of the TOE is done in the administration server. The TOE retrieves its administration data from the administration server over a network connection. Besides the TOE installation, uninstallation and user password change, there is no administration function available at the client side for the TOE. The local administration data (TSF data) is secured by symmetric encryption. Only a successful identification and authentication grants access to the TSF data.
Random Number Generation and Key Generation	During installation of the TOE and initial encryption of local block devices a deterministic random number generator (DRNG) is used for the generation of the cryptographic keys.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 7.1.

The claimed TOE's Strength of Functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6] and [9], chapter 2.3 is confirmed. The rating of the

Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 4.2, 4.3 and 4.4.

This certification covers the configurations of the TOE as specified in chapter 8.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

SafeGuard Enterprise – Device Encryption, Version 5.60 for Microsoft Windows XP Professional and Microsoft Windows 7

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	SafeGuard® Enterprise 5.60.0.192 – Version 5.60.0.192 – Application for Windows XP / Vista / Windows 7	2011	DVD
2	DOC	SafeGuard Enterprise, Product version: 5.60 - Installation guide [10] Guidance for the installation of the TOE	4/2011	DVD
3	DOC	SafeGuard Enterprise, Product version: 5.60 - Administrator help [11] Guidance for the administrators of the TOE	4/2011	DVD
4	DOC	SafeGuard Enterprise, Product version: 5.60 - User Help: SafeGuard Enterprise (managed) + Sophos SafeGuard (standalone) [12] User’s Guide for operating SafeGuard Enterprise and SafeGuard Enterprise	4/2011	DVD
5	DOC	SafeGuard Enterprise, Product version: 5.60 - Manual for certification-compliant operation [13] User's Guide Enhancement for secure operation	11/2011	DVD

Table 2: Deliverables of the TOE

The delivery of the TOE is secured in a way that any user can determine the authenticity of the software package received. This is outlined in the Security Target [6] and [9], chapter 3.5, and in the installation guide [10].

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Access Control:
  The TOE controls access to block devices (hard disk partitions, floppy disks, USB memory sticks, memory cards, compact flash etc.). Each block device is treated as a whole, i.e. there is no specific access control to any subset of data (directories, files) on a block device. For each user known to the TOE and each block device under control of the TOE it can be defined if the user has access to the block device or not.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- The TOE is properly installed and configured regarding the required settings for the security attributes.
- All authorised individuals protect their passwords and PINs.
- Untrusted software is not placed on the PC's hard disk and not executed while the computer is operated.
- Administrators can be trusted and the administration server is operated in a secure environment.
- Authorised users do not actively or negligently compromise the security of the computer on which the TOE is installed.
- The computer secured by the TOE shall not fall under temporary and undetected physical control of an attacker. If a token or a smart card is used for authentication, the assumption extends to the token or the smart card and smart card reader.
- If a token or smart card is used for user authentication it is assumed that the device implements secure storage of the user's private key through its hardware and firmware/operating system, and that it requires a PIN before any operation using this key can be performed.

Details can be found in the Security Target [6] and [9], chapter 3.3, 4.2 and 6.4.

5 Architectural Information

The TOE consists of the following main components:

- [C1] "Power On Authentication" component, performing boot control and user identification and authentication;
- [C2] Real mode kernel for device encryption on BIOS level and TSF data management;
- [C3] Windows 32-bit filter driver for device encryption;
- [C4] Administration component including remote administration interface and local administration tools;

During their examination the evaluators got the following overview showing the decomposition of the TOE into subsystems:

Subsystems of the main component [C1]: Power On Authentication component

- *[S1.1] Modified Master Boot Record*
- [S1.2] POA User Interface Application
- [S1.3] POA Cryptographic Subsystem

Subsystems of the main component [C2]: Real mode kernel for device encryption on BIOS level and TSF data management

- [S2.1] Real Mode Encryption Driver

Subsystems of main component [C3]: Windows 32-bit filter driver for device encryption

- *[S3.1] Windows 32-bit Filter Driver Frame*
- [S3.2] Windows 32-bit Crypto Modules

Subsystems of main component [C4]: Administration component including remote administration interface and local administration tools

- [S4.1] Initialization Subsystem
- [S4.2] Administration Server Interface
- [S4.3] User and Password Synchronisation Subsystem
- [S4.4] Device Encryption Controller Subsystem
- *[S4.5] Event Subsystem*
- [S4.6] Status User Interface
- *[S4.7] Auditing Subsystem*

Please note that the italic marked subsystems don’t provide any explicit security function.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

Tests of the Developer

The test configuration consists of a TOE installed according to the installation guidance [10] as well as the user guidance documents [12] and [13]. The tests are exercised on three operating system versions by the developer: for the operating system "Microsoft Windows XP Service Pack 3" ("XP " in short), using the operating system "Microsoft Windows 7 32-bit" (“Win7-32” in short) and “Microsoft Windows 7 64-bit” (“Win7-64” in short) . The configuration of the TOE is the same for all three operating systems

The TOE is tested by the developer in the normal operational state which is reached after the installation according to the installation guidance for the three different operating systems XP, Win7-32 and Win7-64. Hence the test approach consists of the interaction with the TOE using the user reachable interfaces and so stimulating the security functions. Some test cases stimulate the security functions according to their normal using and the error-free situations are tested. Other test cases stimulate the security functions under failure provoking circumstances and the correct reaction of the TOE is checked.

For the check of the cryptographic algorithms additional test tools are used. These test tools are implemented using a different crypto implementation – implemented independently from the TOE implementation – to find evidence about the correctness of the TOE's implementation of the cryptographic mechanism.

Overall the developer introduces 26 different test cases for the coverage and depth analysis. The actual test results of all test cases documented by the developer are "Tested and OK". This shows that the execution of each test case was successful and all actual test results were as the expected ones. Therefore the overall developer testing result is "OK".

Independent Evaluator Tests

Since there are no different configurations of the TOE the evaluators' testing addresses the TOE as defined by the denotation SafeGuard Enterprise Device Encryption, Version 5.60. The test configuration consists of a TOE installed according to the installation guidance [10] as well as the user guidance documents [12] and [13]. Since the dedication of the TOE is intended for the two different operating systems Microsoft Windows XP Professional Service Pack 3 (XP) and Microsoft Windows 7 Enterprise 64-bit (Win7-64) the tests were conducted twice, once for each operating system. Please note that the use of these two different operating system platforms corresponds with the information about the operating system platform in the Security Target [6] and [9].

From the evaluators' point of view these two different operating system versions are not different configurations for the TOE itself in the sense of the CC. Since the TOE is used in the same manner on both operating systems and in particular the same security functions are active as well as during the installation of the TOE no different configurations have to be performed. Except for a different look-and-feel - which is not based on the TOE itself - no differences of both installations exist.

The developer delivered test cases for the TSF that the TOE operates as specified. The evaluators decided to re-conduct all developer test cases used by the developer for the argumentation regarding the test coverage of the functional specification except one test case which addresses the explicit test of the random number generator during machine key generation for the following reasons:

- The use of the random number generator and of the key generation is implicitly tested in every case a new block device is initially encrypted. For the initial device encryption process a new cryptographic key is generated. For the key generation the random number generator of the TOE is used. The evaluators tested the randomness of the seeding of the random number generator. The evaluators did not verify the structure of the API return values. The evaluators assume that the involved internal functionality will not be changed.
- The developer provided a separate document regarding the quality assessment of the random number generator.

- The developer provided a source code fragment providing evidence about the usage of the random number generator in the context of the key generation.

The test subset conducted by the evaluator consists of a few additional tests, more precisely of enhancing four test cases, and therefore it refers to the actual test cases describing the TSF.

The independent testing took place on 19.8.2011 – 18.11.2011 at the evaluators' site.

For two specific aspects the developer provided additional test tools to find evidence about the correct functionality of the security functions. The first test tool KeytestSGN contains a second implementation of the security functionality to access the key hierarchy stored in a PKCS#12 archive. The other test tool CryptoTestVBE realizes a second implementation of the cryptographic mechanism used for the encryption/decryption of the user data. By the successful application of both test tools during testing evidence is provided that the respective cryptographic functionality implemented in the TOE works as specified.

8 Evaluated Configuration

There are no different configurations of the TOE. The TOE is defined by the denotation SafeGuard Enterprise Device Encryption, Version 5.60.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4
- The following TOE Security Functions fulfil the claimed Strength of Function : medium SF1 (Power On Authentication), SF4 (Random Number Generation and Key Generation).

In order to assess the Strength of Function the scheme interpretations AIS 20 (see [4]) were used.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- AES in CBC mode of operation and block size 128 bits, key size 128 and 256 bits
- AES-256 in Key Wrap mode (RFC 3394) with block size 128 bits, key size 256 bits
- RSAES-PKCS1-v1_5 with CRT option, modulus size 1024, 1536, 2048 or 4096 bits
- PKCS #12 using SHA-1 as pseudorandom function and 3-key-Triple- DES as encryption function (Identifier: pbeWithSHAAnd3-KeyTripleDES-CBC, OID: 1.2.840.113549.1.12.1.3)

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The determination of the existence of a watermarked file on the encrypted device is not considered as violating the security objectives of the TOE, hence not considered as vulnerability here. However it could be stated that the cryptographic mechanism used to protect the integrity and confidentiality of the user data doesn’t provide protection against Watermarking attacks.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AES Advanced Encryption Standard

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DOC	Document
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PKCS	Public-Key Cryptography Standards
POA	Power On Authentication
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
RSAES	RSA Encryption Scheme
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0553-2012, Version 2.40.03, 19.04.2012, Security Target – SafeGuard Enterprise - Device Encryption, version 5.60, Utimaco Safeware AG, file name: SGN_EAL4_ST.pdf (confidential document)

[7] Evaluation Technical Report, Version 1.4, 02.05.2012, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list for the TOE (confidential documents)
Configuration List for Evaluation Documentation, SafeGuard Enterprise - Device Encryption Version 5.60, Version 7, 01.12.2011, file name: SGN_EAL4_cfgList.pdf
Configuration List for source code and binary files, Utimaco Safeware AG, Version 1, May 23, 2011, file name: SGN_EAL4_cfgList_source.pdf

[9] Security Target BSI-DSZ-0553-2012, Version 1.00.00, 02.05.2012, Security Target – SafeGuard Enterprise - Device Encryption, version 5.60, Utimaco Safeware AG, file name: SGN_EAL4_ST_L.docx (sanitised public document)

[10] SafeGuard Enterprise - Installation guide, Product version: 5.60, Sophos Group, April 2011, file name: sgn_56_ig_eng_installation.pdf

[11] SafeGuard Enterprise, Product version: 5.60 – Administrator help, Sophos Group, April 2011, file name: sgn_56_h_eng_admin_help.pdf

[12] SafeGuard Enterprise Product version: 5.60 – User help, Sophos Group, April 2011, file name: sgn_56_h_eng_user_help.pdf

[13] SafeGuard Enterprise, Product version: 5.60 - Manual for certification compliant operation, Sophos Group, November 2011, file name: sgn_cg_eng_certification.pdf

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

“The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.