Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0536-2010

for

Apple Mac OS X 10.6

from

Apple Inc.

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-0536-2010

Operating System

Apple Mac OS X 10.6

from	Apple Inc.
PP Conformance:	“Controlled Access Protection Profile” (CAPP) Version 1.d, 8 October 1999
Functionality:	Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.3

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 (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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, 8 January 2010

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

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 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

---

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

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

2.2 International Recognition of CC - Certificates

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 January 2009 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 web site: 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.

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 Apple Mac OS X 10.6 has undergone the certification procedure at BSI.

The evaluation of the product Apple Mac OS X 10.6 was conducted by atsec information security GmbH. The evaluation was completed on 10 December 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Apple Inc.

The product was developed by: Apple Inc.

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

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 may evolve over time, the resistance of the

[6] Information Technology Security Evaluation Facility

certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Apple Mac OS X 10.6 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] Apple Inc.
1 Infinite Loop
Cupertino, CA 95041
USA

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 operating system Apple Mac OS X 10.6, delivered in two different types: Apple Mac OS X Server 10.6 and Apple Mac OS X 10.6.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Controlled Access Protection Profile, Version 1.d as of 1999-10-08; providing demonstrable conformance.

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 EAL3 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Function	Addressed issue
Audit	The TOE has the ability to audit user actions and store the records in an audit trail that is protected from unauthorized access. The administrator has the ability to select which events get audited.
User Data Protection	The TOE provides a discretionary access control mechanism to protect user objects such as files, directories, and message queues. Resources are cleared of previous information before a user allocates them.
Identification and Authentication	All users are identified and authenticated before they can access any system service.
Residual Data Protection	It is ensured, that all previously allocated memory is cleared before is it allocated to a user process. File system objects are created with all fields initialized at creation time, overwriting the existing information. Additionally, an end of file marker prevents users from accessing data beyond the current file boundary. Other objects that use memory are cleared upon allocation.
Secure Communication	The TOE can be accessed using the SSHv2 protocol, which provides cryptographically-protected network access. Confidentiality and integrity protection are provided by the SSHv2 protocol, which ensures that data is not modified or disclosed.
Security Management	A set of administrative functions to manage user accounts, object access rights, and the audit trail is provided.
TOE Self Protection	The TOE has several features to protect the security functions. It utilizes the security features of the hardware, including running the kernel in the most privileged state of the hardware. Memory protection and process isolation are provided to keep processes from interfering with each other and, more importantly, from interfering with the operating system. A set of diagnostic tools that can be run to ensure the correct operation of the hardware is also provided to the administrator.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 1.5.4.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. 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], chapter 3.

This certification covers the following configurations of the TOE: The evaluated configuration of the TOE is based on the software releases of Mac OS X version 10.6 that are identified above and in [10]. [10] contains further configuration instructions and operational conditions that must be met in order to operate the TOE in its evaluated configuration. For details please refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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:

Apple Mac OS X 10.6

The following table outlines the TOE deliverables:

No	Type	Identifier	Version	Build Version	Form of Delivery
1	SW / DOC	Mac OS X Server 10.6 Snow Leopard	10.6	10A433	DVD
2	SW / DOC	Mac OS X 10.6 Snow Leopard	10.6	10A432	DVD
3	DOC	Common Criteria Configuration and Administration Guide	2.1	n.a.	Electronic

Table 2: Deliverables of the TOE

The TOE is available for purchase through the Apple Store web site: http://store.apple.com/ and through the Apple retail stores. Mac OS X is delivered in two editions: Mac OS X Server 10.6 (No 1) and Mac OS X 10.6 (No 2). This report covers both editions.

Apple utilizes delivery carriers that are capable of providing tracking information. The tracking information is provided to a customer so the customer can track the order throughout the delivery process. The customer can use the tracking information to ensure the proper product was delivered. The shipping boxes also contain a bill of materials that the customer can use to verify what was delivered.

The DVD package is shrink-wrapped to ensure that the TOE has not been tampered with. Signs of tampering are evidence if the shrink-wrap has been compromised. If shipped, the shipping package in which the DVD package is sent is sealed with a single, clear, round tape seal. The seal is placed at the opening of the package. Signs of tampering are

evident if the tape has been cut, removed, re-taped, or covered. The DVD is surrounded by inflatable air bags inside the shipping box to keep it from moving around during transit.

Upon delivery, the TOE user can verify the receipt of the correct version of the TOE by checking the version marked on the package and the DVD. In addition, when the user is installing the TOE from the provided DVDs, the introduction window identifies the TOE, version and the appropriate software updates.

The TOE guidance consists of man pages and the Common Criteria Configuration and Administration Guide [10].The man pages are delivered and installed with the product, and so this delivery aspect is covered by the description of product delivery. For general user manuals, the files are managed in similar fashion to the source code; that is, individual organizations submit the files to the B&I organization for build, and the resulting document PDFs are published with a version number and document number. The Common Criteria Configuration and Administration Guide is delivered electronically from the secure web page https://www.apple.com/support/security/commoncriteria/.

The TOE version only covers the English language of the software as well as the guidance documentation.

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:

- Only those users who have been authorized to access the information within the system may access the system.
- The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information.
- The users of the system shall be held accountable for their actions within the system.

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:

- Trustworthy and compentent administration of the TOE,
- protected user credentials,
- properly installed TOE,
- protection from physical attacks,
- installed procedures for secure information and configuration handling,
- established procedures and / or mechanism for recovery without protection compromise,
- maintain configuration in way only administrative users can install software,
- installed procedures and / or mechanisms for protecting communication.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

Apple distributes the Mac OS X product with its computer systems on DVDs or in DVD images. The distributed Mac OS X product contains many software components covering a large number of different functions.

Mac OS X is distributed as two different types:

- Mac OS X
- Mac OS X Server

The TOE covers both types of Mac OS X. The restrictions required by the evaluated configuration apply equally to both types. This results in the fact that the evaluated configuration is identical for both types, with the exception of the Mac OS X server providing additional GUI interfaces for managing network services.

The TOE is a subset of the distributed Mac OS X product; the subset consists of the software packages defined in [6] section 1.5.4. The TOE includes the kernel, kernel extensions, system libraries and applications necessary to manage, support and configure the operating system.

Mac OS X is a UNIX-like operating system based on the Mach kernel and FreeBSD, which abstracts the complexity of UNIX and provides a user interface that fosters enhanced productivity and ease of use. The following figure provides an overview of the architecture of Mac OS X implemented in the TOE.

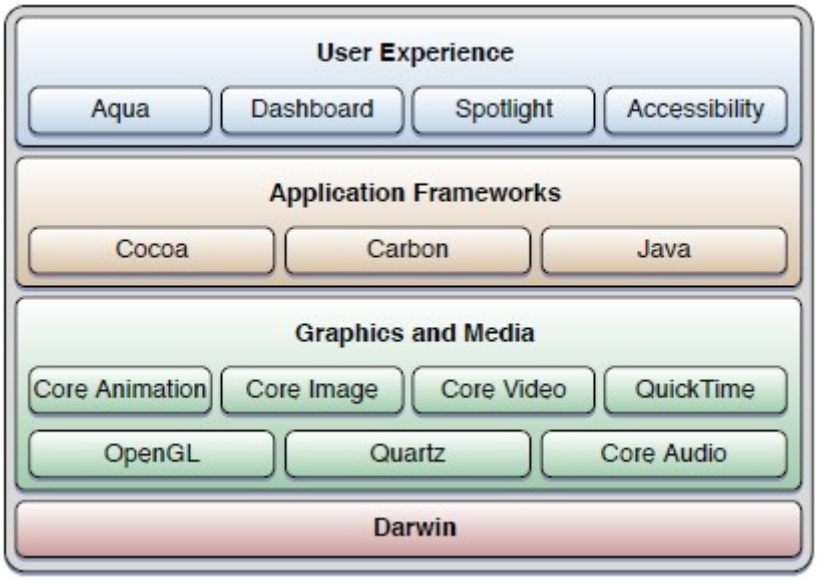

Figure : TOE Layers

The system components perform the following functions:

- User Experience – This layer provides the graphical interface to both users and administrators.
- Application Frameworks – This layer provides an application environment for users. An application environment consists of the frameworks, libraries, and services (along with associated APIs) necessary for the runtime execution of programs developed with those APIs. The application environments have dependencies on all underlying layers of system software. There are four application environments provided:
  1. Carbon – a set of programming interfaces derived from earlier Mac OS X APIs that have been modified to work with Mac OS X, especially its kernel environment.

2. Cocoa – a native set of Mac OS X APIs that access Mac OS X features using an object framework.
3. Java –development and runtime environments and an application framework that allow applications developed in Java to execute on Mac OS X.
4. BSD Commands (not shown in the picture) – a native implementation of a command line BSD command environment.

- Graphics and Media – This layer contains the graphics and windowing environment of Mac OS X. This environment is responsible for screen rendering, printing, event handling, and low-level window and cursor management. It also holds libraries, frameworks, and background servers useful in the implementation of graphical user interfaces. In addition, this layer includes a number of Carbon managers that offer low-level services to all application environments. These services include cooperative and preemptive threading, resource management, memory management, and file-system operations.
- Darwin – The base operating system environment including the kernel is the lowest layer of system software. This environment provides essential operating-system functionality to the layers above it, such as:
  - Kernel: Pre-emptive multitasking
  - Kernel: Real-time support guaranteeing low-latency access to processor resources for time-sensitive media applications
  - Kernel: Virtual memory with memory protection and dynamic memory allocation
  - Kernel: Symmetric multiprocessing
  - Kernel: Multi-user access
  - Kernel: File systems based on VFS (Virtual File System)
  - Kernel: Device drivers
  - Kernel: Networking
  - Kernel: Basic threading packages
  - Rosetta, the translator of PowerPC processor instructions to Intel x86 instructions to allow the execution of native PowerPC applications on Intel x86 hardware
  - Shell and BSD/POSIX utilities

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

7.1 Developer Testing

7.1.1 Test Approach

The majority of test the vendor employed were automated tests, which recruit themselves out of 3 different suites. Manual tests were also part of the set of tests the vendor used for testing the TOE. Summarizing:

1. ATE Test Suite – this automated test suite has been used in the Mac OS X version 10.3 evaluation.
2. Conformance Tests – the automated UNIX conformance suite of the OpenGroup.
3. Common Criteria Tests – automated tests providing additional coverage for the TOE.
4. Manual Tests – manual tests (contained by the Common Criteria Tests).

7.1.2 Test Environment and Configuration

The following table describes the vendor's test environment:

Hardware	Word size of kernel	Word size of test cases	Test suites
X86_64 with 2 CPUs 64-bit system	64 bits	64 bits	ATE, Conformance Tests, Common Criteria Tests, Manual Tests
X86_64 with 2 CPUs 64-bit system	64 bits	32 bits	ATE, Conformance Tests, Common Criteria Tests
X86_64 with 2 CPUs 64-bit system	32 bits	64 bits	Conformance Tests
X86_64 with 2 CPUs 64-bit system	32 bits	32 bits	Conformance Tests
i386 with 2 CPUs 32-bit system	32 bits	32 bits	ATE, Conformance Tests, Common Criteria Tests, Manual Tests

Table 3:Vendor Test Environment

7.1.3 Test Coverage and Depth

All TSFI and all TOE subsystems have been subject to testing.

7.1.4 Test Results

All tests passed successfully or have an appropriate explanation for their (relative) failure.

7.2 Evaluator Testing Effort

7.2.1 Test Approach

The test approach was a mixture of automated and manual tests. The automated tests employed were either specifically developed from the evaluators or adapted from publicly available test suites (the Linux Testing Project test suite in this case).

7.2.2 Test Environment and Configuration

The evaluator tested on two different machines:

- 20-inch iMac, 64bit, 2009 model, iMac9,1
- 15-inch MacBook Pro, 32bit 2008 model, MacBookPro2,2

Each of the machines has an installation of the TOE (Mac OS X Server and Mac OS X Client), which could be booted alternatively on the evaluator's discretion. The test setup used by the evaluator was:

- The iMac was used with an installation of Mac OS X Client running a 32bit or a 64bit kernel together with 32bit and 64bit user mode binaries.
- The MacBook Pro was used with an installation Mac OS X Server running a 32bit kernel together with 32bit and 64bit user mode binaries.

7.2.3 Test Depth

The tests the evaluator executed, covered the following TOE subsystems:

- ADM
- BP
- BSD
- IA
- Mach
- NA
- UA

7.2.4 Test Results

All tests ran successfully and produced the expected results.

7.3 Evaluator Penetration Testing

The evaluator used the information on potential vulnerabilities collected by the evaluators during the evaluation that should be considered in the vulnerability analysis.

- ASE: None
- ALC: None
- ADV: None
- AGD: None

- ATE: None

The evaluator took into account the ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE and came up with the following areas subject to penetration testing:

- System calls, soundness of implementation, error resilience
- Privileges such as the authorization interface, the management of disks and interfaces to device drivers.

The evaluator defined a penetration test framework and produced penetration tests to verify the vulnerabilities. None of the penetration test were successful.

The penetration was carried out using the external interfaces of the TOE, namely the various system call interfaces as well as the filesystem and an authorization service related interface stack as well as the. The subsystems subject to penetration testing are the following:

- Mach
- BSD
- IO
- ADM

The TSF under examination were the following:

- Identification and Authentication
- User Data Protection
- Mach IP Access Control
- Security Management
- TOE Self Protection

None of the evaluator's penetration tests were successful. The vulnerabilities identified by the scanner are either not applicable to the TOE or are not exploitable in the TOE.

Summarizing: No exploitable vulnerabilities were identified.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

Both editions of the TOE (Mac OS X 10.6 and Mac OS X Server 10.6) on i386 and X86_64 CPUs are covered. On X86_64, kernel and / or user programs can be executed in 64 bit and 32 bit word size. Only the English language setting is covered.

The TOE hast to be installed under following rules:

- The set of software packages forming the TOE must be installed during installation time in accordance with the installation instructions provided in the Common Criteria guidance document.
- Only local user databases for password based authentication are allowed to be used by the DirectoryService mechanism.

- The automated password quality checking mechanism is configured to meet the password quality constraints set forth in [6].
- The root account is disabled for interactive login. Administrators use the ‘sudo’ application to gain root privileges.
- The initial configuration outlined in the Common Criteria guidance document representing the evaluated configuration must be achieved before users are allowed to interact with the TOE.
- Mac OS X supports different networking protocols, including IPv4 and IPv6. Only IPv4 is supported in the evaluated configuration.
- Mac OS X supports a wide range of protocols and network services. In the evaluated configuration, the TCP/IP protocol, the NFS client, and SSH services are supported. NFS is allowed to be used in the evaluated configuration, but is not covered by security functional claims in this ST.
- Darwin offers support for multiple file systems. In the evaluated configuration, the HFS+ file system is supported.
- For SSH, the allowed cryptographic mechanisms must be in line with the specification in [6]. Specifically, the “none” cipher (no encryption), and the “none” keyed hash function (no HMAC) are not allowed in the evaluated configuration.
- Apple provides several Mac OS X software applications that are considered outside the scope of the defined TOE and thus not part of the evaluated configuration. These services may be executed under a non-root user ID without invalidating the evaluated configuration, but the evaluation does not make any security claims about these services. Services outside this evaluation include:
  - E-mail services
  - Web server services
  - Remote apple events
  - Print sharing services
  - File sharing services
  - Unencrypted base services, such as FTP or the r-utilities
  - Classic programming support (Old Macintosh OS compatibility support)
  - Mac OS X contains a watchdog timer to restart services and provide stability; however, this timer is disabled in the evaluated configuration.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 EAL3 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Controlled Access Protection Profile [7]
  demonstrable conformance
- for the Functionality: Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by ALC_FLR.3

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- the TOE Security Functionality Secure Communication, using the following:
  - generation of symmetric cryptographic keys defined by the SSH version 2.0 protocol
  - generation of asymmetric keys defined in FIPS-186-2
  - distribution of symmetric cryptographic keys: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1 specified by SSH version 2.0 protocol; diffie-hellman-group-exchange-sha1 defined by RFC 4419
  - distribution of asymmetric cryptographic keys as defined in SSH version 2.0 protocol
  - encryption and decryption: 3DES in CBC mode with 168 bit key size; AES in CBC mode with 128 bit, 192 bit or 256 bit key size; Blowfish in CBC mode with 128 bit; Arcfour in CBC mode with 128 bit key size ; CAST in CBC mode with 128 bit key size; HMAC-SHA1 with 160 bit hash size; HMAC-MD5 with 128 bit hash size as defined in SSH version 2.0 protocol
- and for other usage of encryption and decryption within the TOE.

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.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CPU Central Processing Unit

EAL Evaluation Assurance Level

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirement

SSH Secure Shell

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functions

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[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 Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0536-2010, Version 1.0, December 12th, 2009, Apple Mac OS X 10.6 Security Target, Apple Inc.

[7] Controlled Access Protection Profile (CAPP), Issue 1.d, October 8th,1999

[8] Evaluation Technical Report, Version 3, December 16th, 2009, Apple Mac OS X 10.6, atsec information security GmbH (confidential document)

[9] Snow Leopard configuration item list, 2009-09-01, CI_XBS_SnowLeopard.zip (confidential document)

[10] Guidance documentation for the TOE, Version 2.1, September 21th, 2009, Common Criteria Configuration and Administration Guide

[8] specifically

- AIS 23, Version 2, 11 March 2009, Zusammentragen von Nachweisen der Entwickler
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ 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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0536-2010

Evaluation results regarding development and production environment

The IT product Apple Mac OS X 10.6 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 8 January 2010, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_FLR.3) are fulfilled for the development and production site of the TOE:

Apple Computer
1 Infinite Loop
Cupertino, CA 95014
USA

For the site listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of this site.

This page is intentionally left blank.