

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <!-- New document created with EditiX at Mon May 16 10:30:48 CEST 2011 -->
3  <AbstractASSERTStructure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4  xsi:noNamespaceSchemaLocation="ASSERT-1r.xsd">
5      <ASSERTIssuer>
6          <Name>BSI - Bundesamt für Sicherheit in der Informationstechnik</Name>
7          <Date>2010-01-08</Date>
8      </ASSERTIssuer>
9      <ASSERTType>ASSERT-E</ASSERTType>
10     <ASSERT4Humans>
11         <OriginalDocument>http://www.commoncriteriaportal.org/files/epfiles/0536a_pdf.pdf</OriginalDocument>
12         <Description>The IT product identified in this certificate has been evaluated at an approved evaluation
13             facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to
14             the Common Criteria for IT Security Evaluation (CC), Version 3.1.
15             This certificate applies only to the specific version and release of the product in its evaluated
16             configuration and in conjunction with the complete Certification Report.
17             The evaluation has been conducted in accordance with the provisions of
18             the certification scheme of the German Federal Office for Information Security (BSI) and the
19             conclusions of the evaluation facility in the evaluation technical report are consistent with the
20             evidence adduced.
21             This certificate is not an endorsement of the IT product by the Federal Office for
22             Information Security or any other organisation that recognises or gives effect to this certificate,
23             and no warranty of the IT product by the Federal Office for Information Security or any other
24             organisation that recognises or gives effect to this certificate, is either expressed or implied
25         </Description>
26         <Keywords>APPLE</Keywords>
27         <Keywords>Apple Mac OS X 10.6</Keywords>
28         <Keywords>fromApple Inc.PP Conformance: "Controlled Access Protection Profile" (CAPP)Version 1.ds</Keywords>
29         <Keywords>Common Criteria Part 2 extended Assurance3</Keywords>
30         <Keywords>Common Criteria Part 3 conformantEAL 3 augmented by ALC_FLR</Keywords>
31     </ASSERT4Humans>
32     <SerialNumber>BSI-DSZ-CC-0536-2010</SerialNumber>
33     <Issuer(signer)>
34         <Type>Responsible Person</Type>
35         <Value>Bernd Kowalski</Value>
36     </Issuer(signer)>
37     <Validity>
38         <NotBefore>2010-01-08</NotBefore>
39     </Validity>
40     <ServiceOwner>
41         <Type>Company</Type>
42         <Name>Apple Inc</Name>
43         <Legal-Address>1 Infinite Loop, Cupertino, CA 95041, USA</Legal-Address>
44     </ServiceOwner>
45     <ServiceOwnerPublicKeyInfo>.....</ServiceOwnerPublicKeyInfo>
46     <Signature>.....</Signature>
47     <ProvidedProperties>
48         <Property>
49             <ID>Audit</ID>
50             <Description>The TOE has the ability to audit user actions and store the records
51                 in an audit trail that is protected from unauthorized access. The administrator
52                 has the ability to select which events get audited</Description>
53             <FormalSpecification>
54                 <TypeOfSpefication> Link </TypeOfSpefication>
55                 <PropertySpecification> .....</PropertySpecification>
56             </FormalSpecification>
57         </Property>
58         <Property>
59             <ID>User Data Protection</ID>
60             <Description>The TOE provides a discretionary access control mechanism to protect
61                 user objects such as files, directories, and message queues. Resources are cleared
62                 of previous information before a user allocates them.</Description>
63             <FormalSpecification>
64                 <TypeOfSpefication> Link </TypeOfSpefication>
65                 <PropertySpecification> .....</PropertySpecification>
66             </FormalSpecification>
67         </Property>
68         <Property>
69             .....
70         </Property>
71     </ProvidedProperties>
72     <CertificationProcess>
73         <ProcessID>Common Methodology for IT Security Evaluation (CEM), Version 3.1</ProcessID>
74         <ProcessDescription>EAL3 permits a conscientious developer to gain maximum assurance
75             from positive security engineering at the design stage without substantial alteration
76             of existing sound development practises. EAL3 is applicable in those circumstances where
77             developers or users require a moderate level of independently assured security, and
78             require a thorough investigation of the TOE and its development without substantial
79             re-engineering.</ProcessDescription>
80         <CertificateAgent>Atsec information security GmbH</CertificateAgent>
81         <EvaluationSetting>The evaluator tested on two different machines:
82             20-inch iMac, 64bit, 2009 model, iMac9,1

```

```

83         15-inch MacBook Pro, 32bit 2008 model, MacBookPro2,2 Each of the machines has an
84         installation of the TOE (Mac OS X Server and Mac OS X Client), which could be
85         booted alternatively on the evaluator's discretion. The test setup used by the
86         evaluator was:
87         The iMac was used with an installation of Mac OS X Client running a 32bit or
88         a 64bit kernel together with 32bit and 64bit user mode binaries.
89         The MacBook Pro was used with an installation Mac OS X Server running a 32bit
90         kernel together with 32bit and 64bit user mode binaries.</EvaluationSetting>
91     <Tasks>
92         <TaskName>Test</TaskName>
93         <TaskDescription>The tests the evaluator executed, covered the following TOE
94         subsystems:ADM, BP, BSD, IA, Mach, NA, UA</TaskDescription>
95     </Tasks>
96     <CertificateEvaluationDates>2009-12-10</CertificateEvaluationDates>
97 </CertificationProcess>
98 <CertificationResults>
99     <ResultsType>Textual</ResultsType>
100    <ResultsDescription>The Evaluation Technical Report (ETR) [9] was provided by the ITSEF
101    according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme
102    [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.
103    The Evaluation Methodology CEM [2] was used.
104    As a result of the evaluation the verdict PASS is confirmed for the following assurance
105    components: All components of the EAL3 package including the class ASE as defined in the CC
106    (see also part C of this report)
107    The components ALC_FLR.3 augmented for this TOE evaluation. The evaluation has confirmed:
108    PP Conformance:Controlled Access Protection Profile [7]demonstrable conformance
109    for the Functionality: Common Criteria Part 2 extended
110    for the Assurance: Common Criteria Part 3 conformantEAL 3 augmented by ALC_FLR.3
111    For specific evaluation results regarding the development and production environment see annex B
112    in part D of this report.The results of the evaluation are only applicable to the TOE as defined
113    in chapter 2 and the configuration as outlined in chapter 8 above.</ResultsDescription>
114 </CertificationResults>
115 <CertificationResults>
116     <ResultsType>Link</ResultsType>
117     <ResultsDescription>http://www.commoncriteriaportal.org/files/epfiles/0536b.pdf</ResultsDescription>
118 </CertificationResults>
119 <ServiceApplication>
120     <Binding>Type:SW / DOC, ID:Mac OS X 10.6 Snow Leopard, Version: 10.6, Build: 10A432, DeliveryForm: DVD</Binding>
121     <AssumptionsDependencies>Trustworthy and competent administration of the TOE,
122     protected user credentials,
123     properly installed TOE,
124     protection from physical attacks,
125     installed procedures for secure information and configuration handling,
126     established procedures and / or mechanism for recovery without protection compromise,
127     maintain configuration in way only administrative users can install software,
128     installed procedures and / or mechanisms for protecting communication.
129     Details can be found in the Security Target [6], chapter 4.2.</AssumptionsDependencies>
130 </ServiceApplication>
131 </AbstractASSERTStructure>
132

```