Federal Office
for Information Security

Certification Report

BSI-CC-PP-0067-2010

for

Operating System Protection Profile (OSPP) Version 2.0

from

Federal Office for Information Security (BSI)

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0067-2010

Common Criteria Protection Profile

Operating System Protection Profile (OSPP)
Version 2.0

developed by Federal Office for Information Security (BSI)

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
ALC_FLR.3

Common Criteria
Recognition
Arrangement

The Protection Profile 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 Protection Profile 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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile 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, 2 June 2010

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

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 as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

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.

[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 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [8]
- Procedure for the Issuance of a PP certificate by the BSI

2 Recognition Agreements

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

[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 12 February 2007 in the Bundesanzeiger dated 23 February 2007

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. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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 (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 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 resp. 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 Operating System Protection Profile (OSPP), Version 2.0 has undergone the certification procedure at BSI.

The evaluation of the Operating System Protection Profile (OSPP), Version 2.0 was conducted by the ITSEF Tele-Consulting security | networking | training GmbH. The evaluation was completed on 1 June 2010. The ITSEF Tele-Consulting security | networking | training GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Federal Office for Information Security (BSI)

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 Protection Profile as indicated.

In case of changes to the certified version of the Protection Profile, 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 Protection Profile, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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

5 Publication

The Operating System Protection Profile (OSPP), Version 2.0 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: https://www.bsi.bund.de and [4]). 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 Protection Profile. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Information Technology Security Evaluation Facility

[7] Federal Office for Information Security (BSI)
Godesberger Allee 185-189
53175 Bonn

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Operating System Protection Profile (OSPP), Version 2.0 [6] is established by the Federal Office for Information Security (BSI) as a basis for the development of Security Targets in order to perform a certification of an IT-product (TOE).

This Protection Profile defines the security functionality expected to be provided by a general-purpose operating system capable of operating in a networked environment. Unlike most other Protection Profiles, the Operating System Protection Profile (OSPP) is structured into a "base" part and a set of (optional) "extended packages". This structure was chosen to maximize adaptability for different operational environments and different operational requirements, since general-purpose operating systems may provide a wide range of different functionality.

General-purpose operating systems often operate in environments that provide centralized services that can be used by a large number of systems within an organization. It is expected that a modern general-purpose operating system provides the capability to use centralized services for the implementation of security functionality, for example, authentication servers, directory servers, certification services, or audit log servers. While most modern general-purpose operating systems implement functions such as centralized security services, they may also be able to act as the server for those services.

Co-operating with another trusted IT system to provide a security service is not restricted to the use of centralized services, but can also be accomplished in a peer-to-peer relationship. An example is a function for the authentication of a human user that is based on a token the user needs to present, for example, a smart card. In this scenario, the user authenticates to the smart card using his PIN, and the smart card authenticates the user to the operating system, for example, by presenting the user's certificate and assuring the operating system that it has the private key associated with the public key in the certificate.

Operating systems conformant to this Protection Profile are assumed to operate in an environment in which the platform on which they execute (underlying hardware, devices and firmware) is protected from physical attacks and manipulation. In addition, it is assumed that all management activities are performed by knowledgeable and trustworthy users.

OSPP Base:

The mandatory OSPP base (see [6], chapter 3), which defines the common denominator for all operating systems claiming conformance with the OSPP, describes the security functionality provided by a TOE claiming conformance with the OSPP base. The TOE has the following capabilities:

- providing the following services to different "users", which may be human users, as well as other IT systems
- simultaneously supporting multiple subjects (usually processes or address spaces), potentially operating on behalf of different users
- separating subjects operating for different users from each other
- mediating and enforcing access to operating system-defined "named objects" and allowing or disallowing such access based on well-defined rules
- verifying the identity of external users, which allows the access control policy rules to be based on security attributes the operating system associates with such users

- recording defined events with sufficient data thereby allowing a reviewer to identify the type of event, the time the event happened, and when possible, the identity of the user that caused the event
- defining aspects of the security policy that can be managed, together with rules to restrict management activities to defined users
- protecting itself including the data/objects it relies on from tampering with also in terms of bypassing the security policy

The TOE provides the following security functionality:

- **Auditing**: Security relevant events are audited. Audit records are stored in an audit trail in persistent storage unless they are transmitted to a trusted centralised audit server. Local storage used for the audit trail must be protected form unauthorised access by users or subjects. A policy must be defined.
- **Cryptographic services**: The TOE provides secure network protocols (SSH, TLS and IPSEC).
- **User data protection**: Discretionary access control implies that the access control settings on a specific named object can be defined individually for each user/subject. The TOE uses an information flow policy that defines how network data received are treated by the filter mechanism.
- **Identification and authentication**: Identification and authentication of a user is required when the operating system grants a service protected by the security policy based on the identity of a user. The methods used for user identification and authentication may differ for different types of users. The TOE shall provide identification and authentication services by allowing locally- and remotely-performed identification and authentication. At a minimum, the TOE provides the mechanisms user-ID/password- and software token-based authentication.
- **Management for security mechanisms**: For all security functions the TOE must provide management mechanisms. The authority to perform management of aspects of security functions is based on dedicated management rules.
- **Trusted channel**: The TOE shall establish a trusted channel to a remote trusted IT system. The communication between the TOE and the remote trusted IT system must ensure that the data exchanged between the TOE and the remote trusted IT system is sufficiently protected, ensuring authenticity, integrity and confidentiality of the exchanged TSF data.

Co-operating trusted systems: A TOE that uses remote trusted systems for the support of its security policy must define in its Security Target which parts of the security policy are enforced with the support of a remote trusted IT product and any assumptions on the functionality of such remote trusted IT systems.

The optional **extended packages** (EP) [7] are:

OSPP Extended Package – Labeled Security (Packet Abbreviation: LS)

This EP defines systems protecting information in multi-level environments.

Multi-level security is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. A multi-level-secure security policy has two primary goals. First, the controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization. Second, the controls must prevent individuals from declassifying information.

The security functionality of this package applies to all users and all untrusted subjects, as well as all named objects of the TOE.

The information flow control defined in this extended package is based on the Bell-La Padula model.

OSPP Extended Package – Integrity Verification (Packet Abbreviation: IV)

The OSPP base defines that the code of the TSF is protected against modification using TOE protection mechanisms. However, an administrator cannot verify whether the code is unchanged when compared to the vendor-provided copy.

This extended package defines the functionality to perform integrity verification. The mechanism must be usable to verify the TSF code, TSF data, and user data.

OSPP Extended Package – Advanced Audit (Packet Abbreviation: AUD)

The OSPP base requires the TOE to provide audit functionality that stores audit data locally irrespectively whether the audit data originates locally or from other remote trusted IT systems, and provides simple local audit management interfaces.

This extended package defines functionality for the TOE to operate as an audit server that gathers and stores audit data from remote trusted IT systems, and allows for more sophisticated analysis of audit data.

Please note that the TOE must offer the functionality outlined here, but there is no requirement that the administrator must enable this functionality.

OSPP Extended Package – General Purpose Cryptography (Packet Abbreviation: CRYPTO)

The OSPP extended package for general purpose cryptography specifies cryptographic services the TOE provides to a user. These cryptographic services can be used for unspecified purposes by the user.

OSPP Extended Package –Advanced Management (Package Abbreviation: AM)

The management policy defined in the OSPP base makes no specific requirements. The policy allows the commonly-found model in which administrators own all rights for administering the TOE, while regular users have no administrative rights except for their own data. The administrator is allowed to configure the system, including modification of settings that have an impact on security functionality. The user, on the other hand, cannot perform any configuration that has an impact on the security policy.

While the OSPP base does offer the ST author the freedom to specify more comprehensive management policies, this extended package specifies definition of mechanisms and interfaces that are well-suited to administration in more complex environments, covering, for example, the following needs:

- In larger environments, an all-or-nothing approach to administrative rights is insufficient. Usually, specific groups of users have different, specific tasks with respect to administering the system. For example, it is unwise to grant a group of users that shall only administer the audit facility, administrative rights that go beyond administering the audit settings.

- A help desk organization might provide support for normal users in a large environment, including resetting user passwords. Therefore, help desk personnel should have the right to set and reset user passwords, but not to administer other properties of the system.
- Users might need the ability to delegate all or a subset of their own administrative rights for their own data to other users, in case of vacation or other absence. However, the TOE security policy might need to deny the delegation of certain rights and prevent any privilege escalation.

OSPP Extended Package – Extended Identification and Authentication (Packet Abbreviation: EIA)

The OSPP base defines minimum identification and authentication (I&A) functionality that every general-purpose operating system must provide. Additional identification and authentication mechanisms can be provided by the TOE.

The OSPP extended package for extended I&A mechanisms requires the TOE to perform identification and authentication based on additional credentials. The extended I&A mechanism may be used independently, or it may be used concurrently with the identification and authentication mechanism defined for the OSPP base.

In addition to supporting the new set of credentials, the TOE shall allow to define an identification and authentication policy that is independent of the policy defined for the OSPP base. This OSPP extended package does not predefine any specific policy, but requires the ST author to specify such a policy. The additional identification and authentication policy must allow the TOE to operate as a central identification and authentication server supporting other remote trusted IT systems. This identification and authentication policy integrates with the user-subject binding of the remote trusted IT system, in that the TOE effectively provides the identification and authentication policy decisions that must be enforced by the remote trusted IT system. For this policy, no special user-subject binding is defined locally. It is nevertheless possible that this extended identification and authentication policy supports the locally-enforced policy and therefore integrates with the locally-enforced user-subject binding user-subject binding as defined by FIA_USB.2 of the OSPP base.

This OSPP extended package allows the ST author to specify the additional identification and authentication policy decisions to be enforced remotely and (optionally) locally. As such, the extended package allows the definition of an identification and authentication server that provides services to remote trusted IT systems.

If the extended identification and authentication services of the TOE are applied to remote trusted IT systems, the following sequence of data flow is considered:

- The remote trusted IT system obtains credential information from the user (which may be a human or other technical user) trying to perform identification and authentication. Currently, this OSPP extended package does not make any requirements as to how the remote trusted IT system obtains these credentials.
- These credentials are transmitted to the TOE, which performs operations to validate the credentials as defined by the identification and authentication policy.

This validation is subject to the security requirements set forth by this OSPP extended package.

- The TOE provides the result back to the remote trusted IT system that made the request. The remote trusted IT system is now required to enforce identification and authentication based on the reply obtained from the TOE. The enforcement of the identification and authentication decision is outside of TOE control and cannot be defined in the ST (this does not apply when this identification and authentication policy is also used locally, where the SFRs defined in the OSPP base specify the enforcement side).

OSPP Extended Package – Trusted Boot (Packet Abbreviation: TB)

As outlined in the "OSPP Extended Package – Integrity Verification", integrity protection requires an anchor, as the TSF are stored in a modifiable environment. The anchor specified in the "OSPP Extended Package – Integrity Verification" contains the parts of the TSF data including the stored TSF code implementing the TSF functions that are loaded and executed before integrity verification is active. To achieve a higher level of trust, the size of the trust anchor must be limited to components that are part of a non-modifiable environment, such as hardware or software/firmware stored in read-only memory. Therefore, all TSF code and TSF data loaded and executed by the underlying platform before the TSF-provided integrity mechanism is initiated must be verified for integrity by the trust anchor before they are loaded. The integrity verification provided by the non-modifiable environment must be invoked before the TSF code and TSF data are loaded and executed.

If "Extended Package – Trusted Boot" is used in an ST, the "Extended Package – Integrity Verification" has to be claimed additionally in order to fulfill the dependency of these packages.

OSPP Extended Package – Virtualization (Packet Abbreviation: VIRT)

The OSPP base defines security requirements for general-purpose operating systems. A general-purpose operating system allows subjects to interact with each other through well defined communication channels; however, the operational environment of one subject is protected from any other subject. The OSPP extended package for virtualization adds requirements for the complete separation of compartments in which subjects execute their code.

This OSPP extended package is defined for operating systems that provide functions for the management and separation of compartments. The TOE shall allow execution of multiple, separated compartments on a single trusted system. Each compartment can behave like a single platform separated from other compartments. The TOE enforces this separation and controls communication between compartments, as well as communication with external entities, in accordance with a defined policy. As such, compartments are a different set of active entities in addition to the subjects defined in the OSPP base.

The following implementations of virtualization functionality provided with general-purpose operating systems are covered by this extended package:

- Hardware virtualization: Hardware virtualization utilizes the hardware, mainly the processor support of a hypervisor state, in addition to the supervisor and user states. The hypervisor state is utilized by a component of the TOE to provide an isolated operating space for itself and to provide operating spaces to other untrusted entities. These untrusted entities can utilize the supervisor and user states of the processor. For this implementation, a compartment is a separated entity capable of executing a standard operating system.

- Operating system functionality virtualization: The operating system compartmentalizes the user space to provide strict isolation of the user space compartments. Within these compartments, processes can communicate as usual. However, processes located in different compartments are not allowed to perform any communication. This implementation defines a compartment as a collection of processes (i.e., subjects as defined in the OSPP base) that are isolated from other collections of processes according to the policy defined for the virtualization mechanism.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], chapter 5.1.1. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Protection Profile [6], chapter 5.

These assumptions, threats and organisational security policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the operational environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [6], chapter 6.

The Protection Profile [6] requires a Security Target based on this PP or another PP claiming this PP, to fulfill the CC requirements for demonstrable conformance.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of security functional requirements to be implemented by a TOE. It covers the following issues:

- Auditing
- Cryptographic services
- User data protection
- Identification and authentication
- Management for security mechanisms
- Trusted channel

These TOE Security Functional Requirements (SFR) are outlined in the PP [6], chapter 8. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Security Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
ALC_FLR.3

(for the definition and scope of assurance packages according to CC see part C or [1], part 3 for details).

4 Results of the PP-Evaluation

The Evaluation Technical Report (ETR) [5] 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) [8] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE.

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Operating System Protection Profile (OSPP), Version 2.0 [6] including its extended packages [7] as defined in chapter 1 of this report. This certificate covers both the OSPP base (as defined in [6]) and the extended packages [7].

5 Obligations and notes for the usage

The OSPP allows the definition of functional extensions that can be optionally claimed by an ST in addition to the OSPP base. As such, the OSPP defines the following components:

- The OSPP base specifies the conformance claim, security problem definition, security objectives, and security functional requirements that are to be implemented by every general-purpose operating system. The OSPP base is mandatory and defines the common denominator for all operating systems claiming conformance with the OSPP.
- An OSPP extended package specifies the security problem definition, security objectives, and security functional requirements for mechanisms that may be implemented in addition to the OSPP base. Usually, an OSPP extended package defines an extension that is either desired or implemented by several general-purpose operating systems. However, the functionality specified in an OSPP extended package is not commonly found among general-purpose operating systems. OSPP extended packages can optionally be added to the OSPP base functionality when writing an ST.

The ST author may choose from the set of OSPP extended packages when deriving an ST. To avoid fragmentation of security functionality into OSPP extended packages that are too small to be practical, an OSPP extended package shall define a set of functional requirements that address one or more general security problems.

The OSPP is defined as and extensible framework. The current set of OSPP extended packages can be enhanced with newly-developed or updated OSPP extended packages. Those will then be part of a re-evaluation and re-certification of the OSPP base. Therefore, this framework invites anybody interested in specifying an aspect of general-purpose operating systems to author an OSPP extended package and commit it to the OSPP forum, where the OSPP is managed. Using this approach, there will always be a valid set of OSPP base and extended packages, which are compliant to each other. Dependencies on other OSPP extended packages can be specified.

The following information must be given as part of the ST derived from the OSPP.

- Conformance claim
  When specifying conformance to the OSPP, the ST must specify any OSPP extended packages with which the ST shall conform to. In addition, the ST must claim conformance to any OSPP extended packages that are dependencies of the OSPP extended packages claimed by the ST.
- SFR reference with OSPP extended package reference
  When specifying the SFRs as part of the ST, a reference to the OSPP base or OSPP extended package abbreviation must be given in order to facilitate a direct mapping of the SFR, specifically considering iterations. This requirement shall support ST authors and evaluators to ensure that no SFR from the OSPP base or an OSPP extended package the ST claims conformance to is left uncovered.
- Mandatory information given by OSPP extended packages
  The following information must be given for each OSPP extended package to allow the extended package to be embedded into the framework of the OSPP.
  - Extended package identification
    The following information must be given to identify an OSPP extended package:
    - Extended package name in narrative English
    - Abbreviation of the extended package name to allow easy and unambiguous reference to the extended package
    - Version of the extended package
    - Owner of the extended package; that is, who is in charge of performing authoritative changes
  - Extended package composition rules
    To specify how the OSPP extended package can be used together with other OSPP extended packages, the following information must be provided:
    - A list of dependent OSPP extended packages with their respective versions.
    - A list of disallowed OSPP extended packages with their respective versions.

    Note that the extended package must not exclude the OSPP base or any portion of it; however, extended packages are bound to a version of the OSPP.

    If an existing extended package must be changed to accommodate another extended package (the “current” extended package), the author of the current extended package is requested to approach the owner of the existing extended package to agree on the required modifications.

  - Specification of OSPP extended packages
    The OSPP extended packages may define many aspects as an addition to the OSPP base. Specification includes the following information:
    - Package introduction
    - Dependencies on other OSPP extended packages
    - Security problem definition
    - Security objectives
    - Security functional requirements
    - Refinements to Security Assurance Requirements
      Note that specification of higher or extended Security Assurance Requirements is not allowed; the entire OSPP in intended to be covered by the mutual recognition agreement (CCRA), and the OSPP base shall ensure this.

- Specification restricted to the OSPP base
  - The OSPP base exclusively defines the following properties:
    - Conformance claims to other Protection Profiles
    - Conformance type (either strict or demonstrable)
    - Conformance claim to the EAL including any augmentation

An OSPP extended package may define refinements to assurance components. Refinements may provide guidance on how to satisfy the assurance requirements specifically for the SFRs in the extended package. However, one of the core requirements for OSPP is to keep the Protection Profile and all its modules covered under the mutual recognition agreement (CCRA). Therefore, no OSPP extended package shall add an SAR or modify the level of an SAR that would exceed the boundary set by the mutual recognition agreement. Note that refinements are allowed operations for SFRs and SARs, and such refinements can well be used to guide the evaluator on how to evaluate aspects specific for the functionality defined in a package. Especially for SARs, refinements should be used; extended assurance components must be avoided.

The ST author has to pay attention to all application notes provided in the PP. The ST author can use the extended packages in any combination together with the OSPP base. If the “Extended Package – Trusted Boot” is used in an ST, the “Extended Package – Integrity Verification” has to be claimed additionally in order to fulfill the dependency of these packages.

6 Protection Profile Document

The Operating System Protection Profile (OSPP), Version 2.0 [6] and its extended packages [7] are being provided within separate documents as Annex A of this report.

7 Definitions

7.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
EP	Extended Package
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OSPP	Operating System Protection Profile
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

7.2 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.

8 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, Revision 3, July 2009

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

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

[5] Evaluation Technical Report, Version 2.0, 01.06.2010, Evaluation Technical Report BSI-CC-PP-0067 for Operating System Protection Profile, Tele-Consulting GmbH (confidential document)

[6] Common Criteria Protection Profile, Operating System Protection Profile, Version 2.0, 2010-06-01, Federal Office for Information Security (BSI)

[7] Operating System Protection Profile Extended Packages:

OSPP Extended Package – Advanced Management, Version 2.0, 2010-05-28
OSPP Extended Package – Advanced Audit, Version 2.0, 2010-05-28
OSPP Extended Package – Integrity Verification , Version 2.0, 2010-05-28
OSPP Extended Package – Labeled Security, Version 2.0, 2010-05-28
OSPP Extended Package – General Purpose Cryptography, Version 2.0, 2010-05-28
OSPP Extended Package – Extended Identification and Authentication, Version 2.0, 2010-05-28
OSPP Extended Package – Trusted Boot, Version 2.0, 2010-05-28
OSPP Extended Package – Virtualization, Version 2.0, 2010-05-28

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

[8] specially

- AIS 32, Version 5, 17 Mai 2010, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

„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 D.”

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-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

Assurance Class	Assurance Components
	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: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	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	1	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 d1ue 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: Operating System Protection Profile (OSPP) [6] and its extended packages [7] provided within separate documents.

This page is intentionally left blank.