Federal Office
for Information Security

Operating System Protection Profile

Common Criteria

Common Criteria Protection Profile

BSI-CC-PP-0067

Version 2.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of contents

1 Protection Profile Introduction....9
1.1 Protection Profile reference....9
1.2 TOE overview....9
1.2.1 TOE type....10
1.2.2 Hardware / software / firmware supporting the TOE....10
1.3 Structure of the Protection Profile....11
1.4 Terminology....12
1.4.1 Users....12
1.4.2 Groups....12
1.4.3 Subjects....13
1.4.4 Resources....14
1.4.5 Objects....14
1.4.6 Security attributes....15
1.4.7 Trusted users / subjects....15
1.4.8 Security policy....16
1.4.9 Storage object types....16
1.5 References....16
2 OSPP Framework....17
2.1 Mandatory information given by the ST....17
2.1.1 Conformance claim....17
2.1.2 SFR reference with OSPP extended package reference....17
2.2 Mandatory information given by OSPP extended packages....18
2.2.1 Extended package identification....18
2.2.2 Extended package composition rules....18
2.2.3 Specification of OSPP extended packages....18
2.3 Specification restricted to the OSPP base....18
3 OSPP Base Introduction....20
3.1 TOE overview....20
3.1.1 Auditing....20
3.1.2 Cryptographic services....21
3.1.3 User data protection....22
3.1.4 Identification and authentication....23

3.1.5 Management of security mechanisms....25
3.1.6 Trusted channel....26
3.2 Co-operating trusted systems....27
3.3 TOE boundary....28
4 Conformance Claims....30
4.1 Conformance with CC parts 2 and 3....30
4.2 Conformance with Packages....30
4.3 Conformance with other Protection Profiles....30
4.4 Conformance Statement....30
4.5 Conformance required by OSPP Extended Packages....30
5 Security Problem Definition....31
5.1 Threats....31
5.1.1 Assets....31
5.1.2 Threat Agents....31
5.1.3 Threats countered by the TOE....32
5.2 Organizational Security Policies....32
5.3 Assumptions....32
5.3.1 Physical aspects....33
5.3.2 Personnel aspects....33
5.3.3 Procedural aspects....33
5.3.4 Connectivity aspects....33
6 Security Objectives....34
6.1 Security Objectives for the TOE....34
6.2 Security Objectives for the Operational Environment....35
6.3 Rationale for Security Objectives....36
6.3.1 Security Objectives coverage....36
6.3.2 Security Objectives sufficiency....37
7 Extended Components Definition....42
7.1 FCS_RNG Generation of random numbers....42
7.1.1 Family Behaviour....42
7.1.2 Component leveling:....42
7.1.3 Management....42
7.1.4 Audit....42
7.1.5 FCS_RNG.1 Random number generation....42

7.1.6 Rationale....42
7.2 FDP_RIP.3 Full residual information protection of resources....42
7.2.1 Component leveling....42
7.2.2 Management....42
7.2.3 Audit....43
7.2.4 FDP_RIP.3 Full residual information protection of resources....43
7.2.5 Rationale....43
7.3 FIA_USB.2 Enhanced user-subject binding....43
7.3.1 Component leveling....43
7.3.2 Management....43
7.3.3 Audit....43
7.3.4 FIA_USB.2 Enhanced user-subject binding....43
7.3.5 Rationale....44
8 Security Requirements....45
8.1 Security functionality provided by remote trusted IT systems....45
8.1.1 Example: Access control policy....46
8.2 Security Functional Requirements....48
8.2.1 FAU_GEN.1 Audit data generation....48
8.2.2 FAU_GEN.2 User identity association....50
8.2.3 FAU_SAR.1 Audit review....50
8.2.4 FAU_SAR.2 Restricted audit review....50
8.2.5 FAU_SEL.1 Selective audit....50
8.2.6 FAU_STG.1 Protected audit trail storage....51
8.2.7 FAU_STG.3 Action in case of possible audit data loss....51
8.2.8 FAU_STG.4 Prevention of audit data loss....51
8.2.9 FCS_CKM.1(SYM) Cryptographic key generation....52
8.2.10 FCS_CKM.1(RSA) Cryptographic key generation....53
8.2.11 FCS_CKM.1(DSA) Cryptographic key generation....53
8.2.12 FCS_CKM.2(NET) Cryptographic key distribution....54
8.2.13 FCS_CKM.4 Cryptographic key destruction....54
8.2.14 FCS_COP.1(NET) Cryptographic operation....54
8.2.15 FDP_ACC.1(PSO) Subset access control....55
8.2.16 FDP_ACC.1(TSO) Subset access control....56
8.2.17 FDP_ACF.1(PSO) Security attribute based access control....56

8.2.18 FDP_ACF.1(TSO) Security attribute based access control....57
8.2.19 FDP_IFC.2(NI) Complete information flow control....57
8.2.20 FDP_IFF.1(NI) Simple security attributes....57
8.2.21 FDP_ITC.2 Import of user data with security attributes....59
8.2.22 FDP_RIP.2 Full residual information protection....60
8.2.23 FDP_RIP.3 Full residual information protection of resources....60
8.2.24 FIA_AFL.1 Authentication failure handling....60
8.2.25 FIA_ATD.1(HU) User attribute definition....60
8.2.26 FIA_ATD.1(TU) User attribute definition....61
8.2.27 FIA_SOS.1 Verification of secrets....61
8.2.28 FIA_UAU.1 Timing of authentication....61
8.2.29 FIA_UAU.5 Multiple authentication mechanisms....61
8.2.30 FIA_UAU.7 Protected authentication feedback....62
8.2.31 FIA_UID.1 Timing of identification....62
8.2.32 FIA_USB.2 Enhanced user-subject binding....63
8.2.33 FMT_MSA.1(PSO) Management of object security attributes....63
8.2.34 FMT_MSA.1(TSO) Management of object security attributes....64
8.2.35 FMT_MSA.3(PSO) Static attribute initialisation....64
8.2.36 FMT_MSA.3(TSO) Static attribute initialisation....64
8.2.37 FMT_MSA.3(NI) Static attribute initialisation....64
8.2.38 FMT_MSA.4(PSO) Security attribute value inheritance....65
8.2.39 FMT_MTD.1(AE) Management of TSF data....65
8.2.40 FMT_MTD.1(AS) Management of TSF data....65
8.2.41 FMT_MTD.1(AT) Management of TSF data....65
8.2.42 FMT_MTD.1(AF) Management of TSF data....65
8.2.43 FMT_MTD.1(NI) Management of TSF data....66
8.2.44 FMT_MTD.1(IAT) Management of TSF data....66
8.2.45 FMT_MTD.1(IAF) Management of TSF data....66
8.2.46 FMT_MTD.1(IAU) Management of TSF data....66
8.2.47 FMT_REV.1(OBJ) Revocation....67
8.2.48 FMT_REV.1(USR) Revocation....67
8.2.49 FMT_SMF.1 Specification of Management Functions....67
8.2.50 FMT_SMR.1 Security roles....68
8.2.51 FPT_STM.1 Reliable time stamps....68

8.2.52 FPT_TDC.1 Inter-TSF basic TSF data consistency....68
8.2.53 FTA_SSL.1 TSF-initiated session locking....68
8.2.54 FTA_SSL.2 User-initiated locking....69
8.2.55 FTP_ITC.1 Inter-TSF trusted channel....69
8.3 Rationale for Security Functional Requirements....70
8.3.1 Internal Consistency of Requirements....70
8.3.2 Security Requirements Coverage....71
8.3.3 Security Requirements Dependency Analysis....75
8.4 Security Assurance Requirements....78
8.4.1 ASE_CCL.1 refinement....79
8.5 Rationale for Security Assurance Requirements....79
9 Abbreviations....80

Index of Tables

Table 1: Coverage of security objectives for the TOE....36
Table 2: Coverage of security objectives for the TOE environment....37
Table 3: TOE threats sufficiency....38
Table 4: Security policies sufficiency....39
Table 5: Assumptions sufficiency....41
Table 6: Security Functional Requirements coverage....73
Table 7: Security Functional Requirements rationale....75
Table 8: Security Functional Requirements dependency analysis....78

Illustration Index

Illustration 1: Types of TOE instances and their boundaries....29

Revision History

Version	Date	Author	Changes
1.9	2010-04-06	Stephan Müller, atsec	Initial public release
2.0	2010-06-01	Andreas Siegert, atsec	Changed to support accessibility requirements

1 Protection Profile Introduction

This document 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. Candidates for an “extended package” must have the capability to act as a server for a centralized security service.

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 smartcard. In this scenario, the user authenticates to the smart card using his PIN, and the smartcard 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 (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.

1.1 Protection Profile reference

PP Title: Operating System Protection Profile

PP Version: 2.0

Publication Date: 2010-06-01

Author: Stephan Müller, Gerald Krummeck, Helmut Kurth, atsec information security GmbH

Certification ID: BSI-CC-PP-0067

CC-Version: 3.1 Revision 3

Keywords: Operating System, general-purpose Operating Systems

1.2 TOE overview

The OSPP covers general-purpose operating systems that provide a multi-user and multi-tasking environment.

The main purpose of a general-purpose operating system (from a security point of view) is to provide defined objects, resources and services to entities using the functions provided by the operating system at its external interfaces, and to enforce a defined policy on access to objects, use of resources, and use of services. At a minimum, the operating systems addressed by this Protection Profile export interfaces to programs executing "on top of" the operating systems and interfaces to external entities, including network interfaces, as well as interfaces to devices that are used to "transport" data or actions of external entities to the operating system (for example, a keyboard and a mouse). In addition, the operating system uses functions of the underlying hardware and software to provide its functions, including using devices that are not connected to an external entity such that this entity could affect the behavior of the device directly (for example, hard disks or displays).

An operating system conformant to this Protection Profile can be operated as a server system within a data center, but also as a client system used directly by one or more human users. While it is mandatory that an operating system conformant to this Protection Profile must be capable of providing and using some basic network services, such a system may also be started in an environment where it is not connected to any network and with the network services inactive. It is mandatory that an operating system conformant to this Protection Profile must provide basic security functionality for user identification and authentication, access control, management and audit.

The TOE will provide user services directly or serve as a platform for networked applications, and will support protected communication using one or more cryptographically-protected network protocols or the support of dedicated, physically-separated network links. To support protected communication, the TOE must implement at least the TCP/IP network protocol family; this Protection Profile makes no statements about the version of IP.

The OSPP addresses general-purpose operating systems operating in a well-managed enterprise environment. This addresses mostly servers, but also desktop clients if their operating environment fulfills the security problems defined in chapter 4, as well as the security problems defined by any OSPP extended packages claimed in the ST. These security problems include requirements for professional management of the system and basic protection against physical attacks that can be found in enterprise or government environments, but typically not in home environments administered by private users. The enterprise or government environments may include setups for mobile systems or home-offices provided that the TOE implements mechanisms that allow these environments to comply with the security problem definition in this PP. The OSPP makes no claims or statements that it specifically applies to either a server operating system or a client operating system. If an operating system meets the requirements defined in the security problem definition of the OSPP base, with or without any extended packages, the operating system can claim conformance to this Protection Profile.

1.2.1 TOE type

The requirements defined in this PP shall be applicable to general-purpose operating systems.

The OSPP shall provide a framework for specifying requirements to be provided by a general-purpose operating system.

1.2.2 Hardware / software / firmware supporting the TOE

The operating systems covered by the OSPP have dependencies on their underlying platform, which usually consists of hardware (processors, memory, devices) and firmware. In some cases, the operating system may execute on a separate software layer that provides logical partitioning or a

virtualization layer. Such virtualization emulates all or part of the hardware in a manner that is either transparent to the TOE or by having the TOE using dedicated interfaces to the virtualization layer. In any case, the interfaces to the underlying platform must be defined and described to allow analysis of how the operating system uses the functionality of the underlying platform.

At a minimum, the underlying platform must provide functions the operating system can use to protect itself from untrusted subjects interfering with the functionality of the operating system or bypassing its protection functions. This requires functions that allow the operating system to:

- Protect areas of main memory from being accessed by untrusted subjects.
- Protect devices from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.
- Protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.

This Protection Profile does not define how the underlying platform implements those mandatory protection functions.

At a minimum, the TOE boundary encompasses all parts of the operating system software that are capable of bypassing all or parts of the claimed protection functions. Many operating systems are structured into a “kernel” operating with privileges of the underlying hardware to configure memory, processor states and devices; and a set of "trusted subjects" that operate with privileges assigned by the kernel that allow those trusted subjects to violate all or parts of the security policy the whole operating system needs to enforce. Such trusted subjects also must be considered as part of the TSF.

The TSF subject to assessment may be augmented with OSPP extended packages adding useful security functionality.

In the view of this Protection Profile, the underlying platform is located in the IT environment. This does not preclude a conformant ST from drawing the TOE boundary differently by including all or parts of the underlying platform. For example, an ST author may decide to include the virtualization layer into the TOE, but still exclude the underlying hardware.

1.3 Structure of the Protection Profile

This document is structured as follows:

- Chapter 1 provides the introduction to the OSPP and gives the TOE overview. Please note that this section is expanded with the TOE use and major security functions in the introductory part of the OSPP base and in each OSPP extended package. The statements found in this chapter apply to the base, as well as to the extended packages of the OSPP.
- Chapter 2 defines and specifies the OSPP framework, including the split between the base and extended packages. It also defines mandatory information to be added to the ST derived from the OSPP and extended package documents to allow them to be related to the OSPP base or other OSPP extended packages.
- Chapter 3 contains an introduction of the OSPP base. This section starts the Protection Profile structure for the OSPP base derived from the CC part 1.
- Chapter 4 specifies the conformance claims for the OSPP.
- Chapter 5 contains the security problem definition.

- Chapter 6 defines the objectives.
- Chapter 7 contains the definition of extended components.
- Chapter 8 holds the security requirements definition.

This structure implies that this document specifies the general OSPP constraints, as well as the OSPP base. The additional OSPP extended packages are defined in separate documents with a structure very similar to the structure found in chapters 3ff.

1.4 Terminology

The following sections define terminology for the Operating System Protection Profile (OSPP).

1.4.1 Users

As defined in the Common Criteria, users are external entities that interact with the TOE. Such external entities include human users, as well as other IT systems.

Users can be either anonymous (that is, the operating system does not know the identity of the user) or they may be associated with an identity. In all cases where the security policy enforced by the operating system distinguishes between different users, the operating system must be sure that the identity of the user is correct.

It is quite common that an operating system supports different types of users. Those different types of users are allowed to use different sets of interfaces, have different security attributes, are identified and authenticated in different ways, and are subject to different rules of the security policy. For example, an IT system as a "user" may only be allowed to connect via defined network services, is authenticated using a challenge-response protocol that makes use of digital certificates, and is not allowed to directly access file system objects. On the other hand, "human users" are allowed to use the system call interfaces (via subjects bound to them), are authenticated using a userid/password combination (and eventually some other authentication mechanisms), and are allowed to directly access (via a subject started on behalf of the user) file system objects in accordance with the rules of a discretionary access control policy for those objects.

Users may be locally defined and managed. In this case, the operating system must maintain a list of valid users with their security attributes and must have a policy that defines how those users are managed.

In many cases, an operating system also allows users that are not locally-defined and managed to connect to the operating system and request services. In those cases, the operating system relies on another trusted IT system to ensure the following:

- The user is still a valid member of the user community and has not been revoked.
- User security attributes passed to the operating system by a remote trusted entity are still valid. Note that user security attributes may be passed to the TOE within a digital certificate. In this case, the certification authority that issued the digital certificate is the remote trusted entity, even though the TOE may never have a direct connection to this entity.

1.4.2 Groups

Groups define a set of users that can be referred to by a group identifier. Like users, groups may be managed either by the TOE itself or by a remote trusted entity. Management of groups includes:

- Definition of the group itself.
- Management of group membership.
- Management of the security attributes of the group (for example, privileges and access rights given to the members of the group).
- Definition of how the user and group security attributes or access rights are evaluated when they potentially may be in conflict (for example, when the same security attribute exists as both a user and a group security attribute or when access rights can be assigned to users as well as groups).
- Rules that define how group security attributes or group access rights are evaluated when a user can be a member of several groups.
- Rules that define the "active" group memberships a user may have (if a user can be a member of more than one group, the TOE security policy may restrict the number of groups that are considered when evaluating the rules of the TOE security policy).

Groups are often used to define roles by assigning the security attributes and access rights required for a role to a group, and then assigning users that are supposed to have a specific role to the group. Alternatively, operating systems may implement roles as a single security attribute that can be assigned to a user, where this security attribute defines a fixed or configurable set of privileges assigned to the user via the role.

1.4.3 Subjects

Subjects are the active entities in the system. With regard to the execution of programs, an OSPP-conformant operating system must allow for identifying and separating different active entities executing "on top of" the operating system into different "subjects" that are uniquely identifiable by the operating system, allowing the operating system to control the subject's access to objects, allocation of resources, and use of operating system services by enforcing the rules of a defined policy. The architecture of an OSPP-conformant operating system must prevent such subjects from violating any of the policy rules or bypassing the controls within the operating system that enforce the policy rules.

The operating system may recognize "trusted subjects" for which some or all of the policy rules are not enforced. Such "trusted subjects", when part of the evaluated configuration, must be part of the TSF. Such "trusted subjects" must not provide a way for untrusted users to violate the rules of the security policy.

This Protection Profile does not prescribe how an operating system implements, separates and controls the subjects it creates. This aspect must be explained in the Security Target and then further elaborated in the evidence presented for the security architecture assurance component.

An operating system conformant to this Protection Profile must be able to "bind" specific external entities ("users") to the subject. Subjects bound to a user are operating on his behalf. Since the policy rules enforced by the operating system are often defined by "user security attributes", the operating system must have rules that define how the security attributes of a subject operating on behalf of a user are derived when the operating system "binds" the subject to the user. In the simplest case, the user security attributes are copied one-to-one to the subject security attributes. Significantly more complex rules are implemented in many operating systems. For example, an operating system may have rules that define how the subject security attributes are derived from the user security attributes, the security attributes of the active groups the user is a member of, as well

as the environment in which the subject is started (which may include the time and date or the port the user has used to connect to the TOE), and the current state of the TOE. This Protection Profile does not prescribe the rules for user-subject binding. Therefore, those rules must be defined in a Security Target that claims conformance to this Protection Profile.

Note that operating systems themselves may create and use subjects that are actively involved in the enforcement of the security policy or that are able to bypass all or part of the policy. These subjects need to be "trusted" to enforce the defined policy and are, therefore, part of the TSF of the operating system. In addition, some operating systems create subjects that are part of the TSF upon creation, but change to "untrusted" subjects afterwards (for example, as part of the process of binding a user to the subject).

Subjects may be created by the operating system that are not bound to any user, for example, daemons that are started by the operating system either during start-up or as a result of specific events. For these subjects, the operating system must have a policy that defines the active set of privileges and access rights for these subjects in order to be able to consistently enforce the rules of the security policy. Some operating systems use a mechanism of "pseudo-users", whereby subjects are started with the identity of a "user" without this identity being assigned to any real user. This allows the operating system to use the functions of user management to assign privileges and access rights and to use the rules for user-subject binding to establish the active set of privileges and access rights for these subjects. Since pseudo-users do not represent external entities, usually no user authentication is required.

1.4.4 Resources

Resources are a finite set of logical and/or physical entities that the operating system may allocate to users, subjects or objects. Resource allocation must be managed by the TOE. Blocks of persistent storage, CPU cycles, main memory, and network bandwidth are examples of resources. Resources are usually allocated and if they are re-usable, later de-allocated and prepared for re-use. The OSPP base does not require a specific policy covering resources to be implemented and how they are allocated to subjects, users or objects. However, the OSPP base requires that all re-usable resources, when allocated to a different subject, user or object than the one it was last allocated to, must be prepared for re-use such that upon re-allocation, no information can be obtained from the resource about its previous use or content. OSPP extended packages may define more restricted resource clearing mechanisms, such as the clearing of the contents of a resource upon de-allocation. OSPP extended packages may also require the implementation of specific policies for allocating resources, for example, management of quotas or specific priorities when allocating resources.

1.4.5 Objects

Objects are passive entities created and controlled by the operating system, which provide services to users and/or subjects to use those objects. Named objects are covered by the operating system implementing an access control policy enforcing rules that define the conditions that must be met for users and/or subjects to use a specific type of named objects in a defined way. Named objects must have an identifier that allows the operating system to identify the object when a subject attempts to access the object or when the security attributes of or access rights to the object are managed. Please note that objects may exist or be instantiated by the TOE without being accessible to subjects. For such TOE-internal objects, the security policy of the TOE may not apply as long as they remain internal objects.

The OSPP base requires that at least one type of named object must be created and maintained in persistent storage and must allow users and/or subjects to:

- Create a new object of this type
- Write data to an object
- Read data from an object
- Delete an object

Other operations on this type of named object may be defined, but are not mandatory in the OSPP base.

For this type of named object, the OSPP base requires that an access control policy must be implemented that clearly defines the conditions that must be met to allow a user and/or subject to perform one of the four defined operations on an object of this type. Further conditions the access control policy must meet are defined later in this document.

An operating system usually implements a number of different types of named objects and may implement a different access control policy for each named object type.

1.4.6 Security attributes

An operating system defines security attributes it associates with non-anonymous users, subjects, and named objects. Some of these security attributes are then used by the operating system within the rules of the access control policy; some attributes may be used for different purposes, for example, to determine if a user or subject is allowed to perform certain management actions.

Privileges usually are authorizations that are required to perform administrative tasks. As administrative actions that have implications for security mechanisms must be restricted, the TOE must base these restrictions on verifiable properties, for example, the privileges of the subject performing these actions.

Such privileges may be specifically-assigned properties, such as the UID 0 in UNIX-like environments, or specific access control settings on resources that contain user and/or TSF data, in order to operate on otherwise inaccessible data.

In addition, privileges may be granted to subjects based on any other mechanism, for example, the state of the TOE, the interface through which the user on behalf of whom the subject is acting entered the TOE, the time in which the subject performs its actions, etc.

For each privilege referenced by the security functionality specification, the ST author must specify how this privilege is assigned to a subject.

1.4.7 Trusted users / subjects

Some users have security attributes or access rights that give them the capability to bypass some or all of the rules defined in the security policy or the capability to manage the TSF data on which the security policy relies. These users are trusted to not misuse their capabilities. Note that in some cases, those capabilities may be very limited, for example, the case in which a user is allowed to manage the access control lists of objects he owns. Also, such a user is trusted to use this capability in a sensible way and not, for example, to give all users access to a storage object he has used to store information that only a limited set of users of the system should have access to.

In addition to trusted users, an operating system may also have trusted subjects. Similar to trusted users, these are subjects that have the capability to bypass some or all of the rules defined in the security policy or the capability to manage TSF data on which the security policy relies. These subjects may either not be bound to a user, or they may be bound to a user and allow this user to access objects and/or resources he is not allowed to access when bound to an untrusted subject. Trusted subjects, therefore, have additional capabilities that untrusted subjects do not have, and they enforce a subject-specific policy on the use of such capabilities. An example is a trusted subject that allows a user to modify specific TSF data (for example, his own password). Because of their additional capabilities, trusted subjects are part of the TSF.

1.4.8 Security policy

The "Security Policy" of an operating system is the set of security-related rules it enforces when untrusted, as well as trusted subjects and users request services from the operating system. This set of security-related rules is defined in the Security Target of an operating system; this Protection Profile defines a minimum set of such rules that each operating system conformant to this Protection Profile must enforce.

1.4.9 Storage object types

This Protection Profile employs the terms “persistent storage objects” and “transient storage objects”. The following definitions apply:

Persistent storage objects are objects that can hold user data and/or TSF data and/or TSF functions that retain the stored data in the following ways:

- During initialization of the TOE
- During re-initialization of the TOE
- During powering off or power-cycling the TOE

Transient storage objects, on the other hand, can also hold user data and/or TSF data and/or TSF functions, but this data does not remain intact during the events specified for persistent storage objects. Note that this does not imply that transient storage objects are always cleared or zeroized after the above-mentioned events. Note that the OSPP base requires that transient storage objects or resources that could store data must be prepared for re-use when their re-allocation is performed without going through an event that causes them to automatically lose their data. No preparation for re-use is required when transient storage objects or resources are re-allocated to the same subject to which they previously were allocated or are allocated to another subject with identical security attributes to the subject to which they previously were allocated.

1.5 References

The following references are applicable to this document, as well as all OSPP extended package documents unless a reference is re-defined.

CC	Common Criteria for Information Technology Security Evaluation Parts 1 through 3, July 2009, Version 3.1 Revision 3
CEM	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3

2 OSPP Framework

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, 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, 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 an 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.

2.1 Mandatory information given by the ST

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

2.1.1 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.

2.1.2 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.

2.2 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.

2.2.1 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

2.2.2 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 minimum versions.
- A list of disallowed OSPP extended packages with their respective minimum versions.

Note that the extended package must not exclude the OSPP base or any portion of it; however, the extended package may specify a minimum version of the OSPP base that is required for the respective extended package.

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.

2.2.3 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
- 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, and the OSPP base shall ensure this.

2.3 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. 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 should be avoided when possible.

3 OSPP Base Introduction

The OSPP base defines the basic functionality found in today's general-purpose operating systems. It specifies functions and mechanisms that must be provided and that are already implemented in every general-purpose operating system.

The general audit requirement is added to the OSPP base, as this functionality is mandated by government users and required to fulfill basic accountability requirements mandated by many IT security standards.

The TOE may provide the security functionality in cooperation with other trusted IT entities. The security problem definition considers such scenarios as a possible way to utilize the TOE.

3.1 TOE overview

This section outlines the security functionality provided by a TOE claiming conformance with the OSPP base.

A general-purpose operating system as seen in this document has the following capabilities:

- Provides services to different "users", which may be human users, as well as other IT systems.
- Simultaneously supports multiple subjects (usually processes or address spaces), potentially operating on behalf of different users; and separates subjects operating for different users from each other.
- Mediates and enforces access to operating system-defined "named objects" and allows or disallows such access based on well-defined rules.
- Verifies 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.
- Records defined events with sufficient data that allows 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.
- Defines aspects of the security policy that can be managed, together with rules to restrict the users that can perform management activities.
- Protects itself and the data/objects it relies on from tampering and from bypass of the security policy.

3.1.1 Auditing

All operating systems conformant with this Protection Profile must implement audit functionality that allows the operating system to record events viewed as security-relevant. The records created by the operating system for such events must contain at least the type of the event, the time the event occurred, the identity of the user or subject that caused the event (where appropriate), and further event-specific data. If the event is a request to use a function, the record also needs to contain sufficient information about how the function was intended to be used (usually defined by the parameter passed to the function) and the outcome of the function. If the event is related to an operation performed on an object, the identity of the object must be contained in the record.

Audit records must be stored in an audit trail in persistent storage unless they are transmitted to a trusted centralized audit server, as indicated below. Local storage used for the audit trail must be protected from unauthorized access by users or subjects. A policy must exist that defines:

- The actual events to be audited (from the overall list of auditable events)
- Rules that define when a user or subject can define the events to be audited
- Rules that define when a user or subject can read audit records from the audit trail
- Rules that define when a user or subject can delete or re-initialize the audit trail

The operating system must monitor the amount of space allocated to the audit trail and take appropriate actions when it detects that it has insufficient space to store further audit records.

The audit generation functionality is completely provided locally (by the TSF exclusively). The TOE shall be able to:

- Gather audit information from security-relevant events
- Provide functionality to store audit information locally, and potentially provide a remote storage mechanism (analysis of audit data applies to locally-stored audit data only)
- Provide local analysis of the audit trail if the trail is stored locally
- Allow selection of which audit records are to be generated
- Provide protection of the audit trail when stored locally
- Provide protection that no audit records are lost

Note that remote audit handling is moved to an OSPP extended package. In addition, a TOE can use remote functions to store and/or evaluate audit data and allow appropriately authorized users to define which of the different audit capabilities are used.

3.1.2 Cryptographic services

The following section describes cryptographic services considerations of the Operating System Protection Profile.

3.1.2.1 Cryptographically-protected network protocols

In addition to any generic cryptographic services it makes available, the TOE shall provide applied cryptographic services in the form of network protocols to allow the integrity, confidentiality, and authenticity-protected transmission of user and TSF data.

At a minimum, the TOE must implement one of the following protocols:

- SSH (version 1 of this protocol is prohibited)
- TLS
- IPSEC – the OSPP mandates that the implementation must provide IKE and ESP; AH is not required by the OSPP when specifying IPSEC, but may be added by the ST author.

The OSPP neither mandates nor prohibits use of the cryptographic mechanisms underlying the above-mentioned protocols by other components or security functions outlined in different OSPP extended packages. However, if other network mechanisms implement their own instances of cryptographic mechanisms apart from other security functions, the evaluator must also assess these instances.

3.1.3 User data protection

The following sections describe user data protection considerations of the Operating System Protection Profile.

3.1.3.1 Discretionary access control

Discretionary access control implies that the access control settings on a specific named object can be defined individually for each user/subject – object relationship covered by the discretionary access control policy.

To support discretionary access control and allow the ruleset to apply to the intended users, the TSF may perform a user-subject binding. During this process, a subject is associated with a specific user and the operating system derives security attributes for the subject from the security attributes of the user it binds the subject to. After such a binding, the subject is a representative of the user. This binding is further detailed and specified in section 3.1.4.

The OSPP specifies the minimum types of named objects that are covered by the discretionary access control. These types of objects are:

- Named persistent storage objects backed by non-volatile storage (such as files, directories)
- Named transient storage objects backed by volatile storage (such as shared memory, message queues, pipes)

The operating system may implement different access control policies for different types of users/subjects and different types of objects. A Security Target conformant with this Protection Profile may well define different set of rules for such different access control policies.

For persistent storage objects, the OSPP requires fine-grained granularity of the discretionary access control mechanism. The following properties shall be implemented by the discretionary access control functionality:

- Access rights may be granted on a per-user basis (for example, by access control lists).
- Access rights may be granted on a per-group basis.
- Access rights must include at least the permissions of read, and write; more permissions may be specified by the ST.

For transient storage objects, the OSPP requires that the following properties shall be implemented by the discretionary access control functionality:

- Access rights may be granted to a user (simple permissions such as UNIX permission bits are sufficient).
- Access rights may be granted to a group.

Note that the requirement does not exclude the operating system from providing access to specific persistent storage object types using much simpler access control mechanisms. For example, database servers may use such persistent storage object types under their full control, therefore not requiring sophisticated control over the objects in that file system. However, this PP requires that any TOE claiming conformance with the OSPP must provide at least one type of persistent storage object that provides fine-grained access control as described above.

Note that in certain circumstances objects may be contained in other objects (for example, file systems implemented in a single file). In such a case, two different and possibly conflicting access

control policies may be applicable to the same portion of persistent storage. If the operating system does not resolve such conflicts automatically, the guidance must explain how to set appropriate access rights such that the two access control policies do not conflict.

The OSPP requires the ST author to specify the default access rights for new subjects, as well as new access-controlled objects.

Finally, the OSPP requires the ST author to specify the rules the TOE enforces before allowing a user or subject to manage TSF data used within the access control rules. Usually those rules are based on specific TSF data (like user privileges). If this TSF data can be managed, the management rules that apply also must be specified. It is up to the ST author to describe the conditions that must be satisfied in order to manage TSF data (including the TSF data used in the access control rules).

The OSPP allows locally- and remotely-stored TSF data to be used within the access control rules.

In addition, the OSPP allows the ST author to specify whether the TOE provides access control decisions for other remote trusted IT products. With this option, the ST author can specify the server side of permission storage.

3.1.3.2 Network information flow control

The TOE shall allow filtering of network data using an information flow control policy that defines how network data received are treated by the filter mechanism. The filtering functionality required by the OSPP base is limited to static filter rules for the protocols stated in section 8.2.20. For TCP/IP based filtering, the OSPP allows the ST author to define whether stateless and/or stateful packet filtering is supported.

The information flow control policy defines the rules to identify the network data and the operation to be performed on the network data.

The TOE performs the network information flow control based on initially identifying network data and subsequently performing actions on the network data. The identification of network data can be based upon properties of the network data and additional information maintained by the TOE when mediating the network traffic, for example, the state of TCP connections, time-based rules, or rules based on statistical methods like matching every n^{th} IP packet. Actions imposed on the identified network data can range from discarding the data, modifying the data, sending a notification to the sender, or allowing the network data to pass unaltered.

The OSPP allows the ST author to specify whether the TOE provides access control decisions for other remote trusted IT products. With this option, the ST author can specify the server side of the information flow control rules.

3.1.4 Identification and authentication

Identification and authentication is required to allow the TOE to establish the necessary trust in the identity of a user that interacts with the TOE. 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, and an operating system may also allow different methods for identification and authentication for the same type of users. For example, an operating system may support user ID/password, as well as token-based authentication for human users. After successful identification

and authentication, an operating system will perform a user-to-subject binding whenever it starts an untrusted subject that shall operate on behalf of the authenticated user.

The OSPP requires that a user or another IT system must be authenticated before utilizing any services of the operating system that are restricted by the security policy to specific users. An OSPP-conformant system may allow unauthenticated users to access objects controlled by the access control policy. This requires the access control policy to be able to assign access rights to unauthenticated users.

An operating system may accept users as identified and authenticated when another trusted IT system reports the identity of the user in a way that allows the operating system to verify the integrity and authenticity of the message that containing the information about the remotely authenticated user.

An operating system may also authenticate users with the help of another trusted IT system, for example, when it either retrieves information used for the authentication from the other system (for example, the hash value of a password), or redirects information it retrieves from the user to the other system such that the remote trusted IT system can perform the user authentication and report the result back to the TOE.

For the OSPP base, the TOE shall provide identification and authentication services by allowing locally- and remotely-performed identification and authentication with the following definitions:

- Local identification and authentication implies that the TOE performs the operations to establish the identity of the user. This definition allows storing the TSF data holding the user's credentials either on the TOE or on a remote trusted IT system. However, the TOE must be able to completely fetch the TSF data with the credential information and perform the necessary operations and checks that implement the identification and authentication logic locally. Another local identification and authentication is performed when a user provides a token (a certificate, Kerberos token, etc.) which defines the user's identity; the TOE must verify that token.
- Remote identification and authentication implies that the TOE is a client to an authentication server. The TOE sends the user-supplied identification and authentication data to the server and queries the server as to whether the transmitted credentials are positively or negatively verified. The TOE then enforces the decision made by the authentication server.
- For accessing public objects, the TOE shall allow operations by unauthenticated users (which shall be exempt from identification and authentication). The allowed operations and public objects must be defined by the ST author.

For example, a Directory Server may store the user credentials or the internal representations of the user credentials. When the TOE is able to obtain all credentials, including the user password, and performs the operations to validate the user-given credentials with the stored ones, then a local identification and authentication is performed. However, if the TOE only performs, for example, an LDAP-bind operation with the user-supplied credentials and observes whether the LDAP server rejects the operation, then remote identification and authentication is performed.

The OSPP allows for local, remote and combined local and remote identification and authentication, which can usually be found in large installations. For example, a local user database is defined with administrative user IDs that are only usable when the connection to the authentication server is severed. Another example would be that the TOE caches the user database of the authentication server and applies this database in case the link to the authentication server is severed. Note that if

the TOE allows multiple authentication methods concurrently (such as local and remote authentication), the ST author shall specify the order in which the authentication methods are applied.

In addition, the OSPP shall allow the ST author to specify whether the TOE provides identification and authentication for other remote trusted IT products. With this option, the ST author can specify the server side of the credential storage.

When credentials or the internal representations of the user credentials are stored within the TOE, the TOE shall ensure the quality of the credentials when they are being changed by administrative users or authorized users.

At a minimum, the identification and authentication functionality shall provide all of the following mechanisms:

- User ID / password
- Software token-based authentication

After successful identification and authentication, the TSF may perform a user-subject binding. Such a binding is required when the operating system creates and starts a subject to operate on behalf of the user. This process ensures that the external entity (or user) "binds" to the subject. The ST author must define the rules applicable to the user-subject binding process. Those rules define how the security attributes of the subject are initialized, usually derived from security attributes of the user. See section 1.4.3 for more details. During the user-subject binding, all security attributes of a subject used by the rules of the security policy must be established.

3.1.5 Management of security mechanisms

The TOE must provide management mechanisms for all security functions that are provided by the TOE.

If the TOE is supported by remote trusted IT systems, the management requirement only covers the functional aspects provided by the TOE.

The authority to perform management of aspects of security functions is based on dedicated management rules, which are often based on privileges. These privileges can be explicitly implemented by the TOE by requiring a specific privilege to use an administrative interface or to access resources that govern the behavior of the TSF. Privileges may also be given implicitly by granting write access to TSF data, such as configuration files or configuration databases holding the configuration of all or parts of the TSF. On the other hand, the rules that regulate how management operations can be performed can also be based on other aspects, like access to storage objects that contain TSF data, access to specific interfaces or devices, the state of the system, or any combination of these aspects.

In the OSPP base, the ST author must define the TSF data that can be managed, as well as the rules that determine if a management operation is allowed. At a minimum, TSF data that can be managed must include:

- Management of users and their manageable security attributes.
- Management of security attributes that are used for the discretionary access control policies. The manageable security attributes must be able to define access down to the granularity of a single user (for the type of users that are allowed to access the objects controlled by the access control policy).

- Management of security attributes that are used for the information flow control policy.
- Management of the audit policy, which includes at least the selection of the events to be audited and the management of the storage objects that contain the audit trail.

The OSPP does not mandate any specific implementation. However, the TOE must:

- Allow administrative functions to be assigned to zero, one, or more users.

The ST author shall specify the rules used to determine if a management activity is allowed and the TSF data used in those rules. The OSPP does not specify any policy or any specific set of rules. As such, the ST author has the ability to specify one user that is granted all privileges (like the UNIX root user). In addition, the ST author can also specify a sophisticated administration policy including hierarchical privileges or role-based management.

The TOE shall allow localized and/or centralized management of these security functions:

- Localized management implies that tools are provided with the TOE to configure aspects of security functions. The SFRs will not make any statement about whether the TOE data is stored remotely (see discussion about local identification and authentication above).
- Remote management implies that the management of the security functionality is not provided by the TOE, but the TOE enforces the management actions.

Irrespective of the management type (localized or remote), the configuration data can be stored locally or remotely. If stored remotely, there is no restriction about whether the configuration data is stored with the remote management system or on another system.

The OSPP allows locally- and remotely-stored TSF data used within the management rules.

In addition, the OSPP allows the ST author to specify whether the TOE provides management decisions for other remote trusted IT products. With this option, the ST author can specify the server side of the management operations.

3.1.6 Trusted channel

If the TOE relies on input from remote trusted IT systems to support security policy enforcement, the TOE shall establish a trusted channel to this remote trusted IT system. Involvement of the remote trusted IT system can mean active support by providing functions like user authentication, or simple remote storage and management of TSF data imported by the TOE from the remote trusted IT system (for example, user security attributes stored in a directory). The TOE can also use remote trusted IT systems to store user and TSF data such that the data can be used by the TOE, by the remote trusted IT system, or by other trusted IT systems. In addition, the TOE may provide security-related services to a remote trusted IT system. In all those cases, 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.

In many cases, an operating system will therefore use a trusted channel, which provides confidentiality and integrity protection as well as the mutual authentication of the end points of the channel. The capability to establish and maintain a trusted channel to remote IT systems is also a service an operating system can offer to subjects and users. An operating system conformant to this Protection Profile must provide such a capability to subjects.

This trusted channel can be provided by the following mechanisms (the list is not exhaustive):

- Use of cryptographic mechanisms when information is transmitted via a physical or logical network that can be accessed from untrusted subjects. The TOE may rely on one or more cryptographic network protocols specified in 3.1.2.1 for ensuring integrity, confidentiality, and/or authenticity.
- Use of a dedicated physical network that is restricted to administrative and/or trusted users and entities. Note that every IT system connected to this network must ensure that no information is routed to/from untrusted entities from/into this network.

The OSPP base requires that an operating system must provide at least one mechanism for a trusted channel based on cryptographic functions.

3.2 Co-operating trusted systems

It is common in current IT architectures that IT applications, as well as operating systems use services offered by centralized servers for use within a whole IT environment. This applies also for operating system functionality implementing security functions as defined in this Protection Profile. Examples are the use of Directory Servers used for the centralized management of user security attributes, centralized authentication servers, centralized access managers, centralized audit collection and evaluation, as well as centralized functions for security management. While the OSPP base does not mandate that such centralized services are used, it also does not prohibit an operating system conformant to the OSPP base to implement security functionality using remote trusted IT systems that provide part of the security functionality.

It is still required that an operating system conformant to the OSPP base must provide the interfaces for the security functionality claimed to users and subjects, and to ensure that any service provided by a remote trusted system is invoked correctly, with the results of such a service being used appropriately in accordance with the security policy of the TOE. For example, if an operating system uses a centralized access manager to support access control decisions, its TSF must ensure that the services of the remote access manager are invoked when required and are correctly invoked with respect to the access decision to be made, and that the TSF correctly uses the results passed back to it by the invocation of the remote access manager.

A TOE that uses such 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. Although not required, it may be helpful to specify those assumptions using the notion of security functional requirements. This allows for easier mapping of those assumptions to the security functional requirements defined in the Security Target of such a remote trusted IT system (provided this system is also implemented using an evaluated product). Section 8.1 provides the details of how the ST author must address such co-operating systems.

Many operating systems that use remote trusted IT systems to support security services also offer the possibility to configure the operating system such that it also is capable of providing such services. This allows system integrators to set up an IT environment with multiple systems all based on the same operating system product, where one of those systems is configured to act as the server for a centralized service and all other are configured to act as clients for this service, and use the centralized service in the enforcement of their security policy. A typical example is a Directory Server as a central service to store and manage user security attributes that are used by all systems within a specific IT environment to support user authentication and supply the user security attributes required for user-subject binding.

Such co-operation between trusted IT systems is not necessarily restricted to a client-server type of relationship. It may also be a peer-to-peer relationship, for example, where a smartcard is used as part of the user authentication process. In addition, an operating system may make use of multiple remote trusted IT systems to provide a single security functionality: to authenticate a user, the TOE may require the user to present a smartcard. The smart card (as the representative of the user) may present a digital certificate, in response to which the TOE may use a challenge-response protocol to verify that the smart card actually contains the private key associated with the digital certificate it presents. Furthermore, the TOE may use the services of a Directory Server to validate that the certificate has not been revoked. In addition, the TOE may also use its peer-to-peer connection to a cryptographic module outside of the TOE boundary in order to perform the cryptographic operations required for the smart card authentication process (including the validation of the digital signature of the CA that issued the certificate presented by the smart card) and the process to validate the digital signature of the certificate revocation list provided by the Directory Server.

3.3 TOE boundary

This Protection Profile considers the TOE boundary as follows: the TOE is a system that acts as a single unit to all external entities. By this definition, the following examples illustrate a single TOE instance and its boundary:

- A single machine hosting one operating system instance, such as one physical machine or a virtual machine.
- Multiple hardware components that all execute one single system image; that is, one software instance controlling all hardware components, such as a NUMA system with several hardware machines interconnected executing one operating system kernel.
- Multiple hardware components, each executing its own instance of the TOE operating system or operating system kernel, but any external entity has only one defined path to access this system and “sees” these multiple system acting as one, such as a high-performance computing cluster where different nodes have different tasks (such as one node performing the calculation work, one node hosting the disk space, one node establishing the network connectivity for the cluster, one node providing the interface to other entities), but which must work together to provide the entire cluster functionality.

Multiple operating system instances where external entities “see” these instances are considered to form multiple TOE instances. This especially applies to client-server or peer-to-peer setups where each operating system instance forms one TOE instance. For example, a central LDAP server provides the central identification and authentication instance to other operating system instances, where the operating system with the LDAP server and the other operating system instances form individual TOE instances. Similarly, instances of operating systems which share one or more resources like Storage Area Networks (SAN) or distributed file systems constitute independent TOE instances. The decision whether the shared resource belongs to one TOE or is considered to form a resource independent of any TOE is left to the ST author.

The following illustration depicts different forms of TOE instances. Every box shaded in blue is one example of a TOE instance. The lines connecting the boxes illustrate a possible interaction.

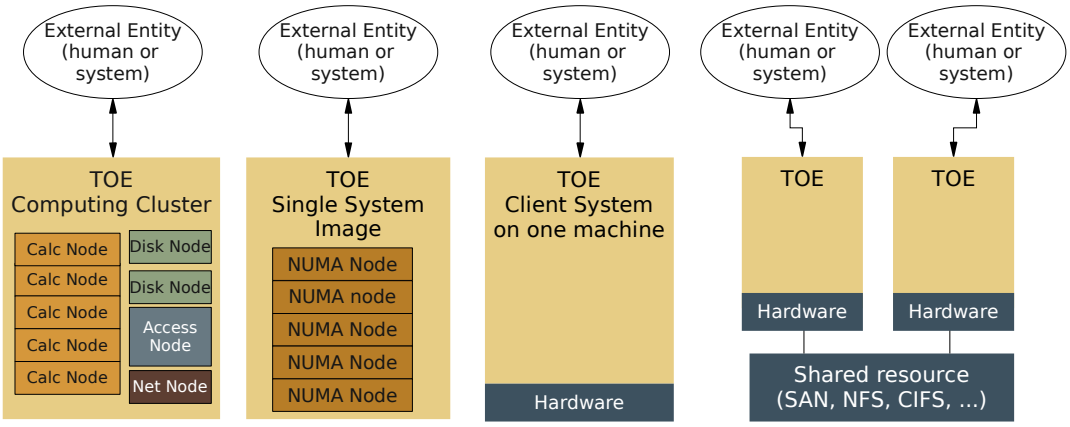

Illustration 1: Types of TOE instances and their boundaries

4 Conformance Claims

The following sections describe the conformance claims of the Operating System Protection Profile (OSPP).

4.1 Conformance with CC parts 2 and 3

OSPP is CC version 3.1 revision 3 Part 2 extended and Part 3 conformant.

4.2 Conformance with Packages

The PP claims an Evaluation Assurance Level of EAL4 augmented by ALC_FLR.3.

4.3 Conformance with other Protection Profiles

OSPP does not claim conformance to any other Protection Profile.

4.4 Conformance Statement

OSPP requires demonstrable conformance by an ST.

Note that the ST author must verify when claiming conformance with multiple OSPP extended packages that the integration of the OSPP base and all claimed OSPP extended packages into the ST complies with the rules specified by the [CC] for demonstrable conformance. It may be possible that an OSPP extended package is mutually exclusive with another OSPP extended package. Although the OSPP extended package author shall have performed an assessment of compatibility, the result of that assessment may be superseded by newer versions of OSPP extended packages or even newly-specified OSPP extended packages.

4.5 Conformance required by OSPP Extended Packages

OSPP extended packages are allowed to extend the functionality of the OSPP base. To extend the functionality, not only are SFRs added, but new objectives and additions to the security problem definition may be specified by extended packages. However, these extended packages must comply with the rules of the Common Criteria, specifically the rules outlined for demonstrable conformance in [CC] Part 1, Appendix D.

This requirement implies among others that:

- Assumptions stated in the OSPP base or a dependent OSPP extended package may be replaced with threats and/or organizational security policies that translate into SFRs to be covered by the TOE.
- No assumptions may be added for functionality that is already included in the OSPP base or dependent OSPP extended packages, as such assumptions would move functionality expected to be implemented by the TOE into the environment.

5 Security Problem Definition

The security problem definition of the OSPP base functionality shall define a general-purpose operating system implemented as a multiple-user, multiple-process system.

The following sections provide a definition of various important terms, threats, assumptions and policies that are the basis for the security functionality of the OSPP base.

5.1 Threats

Threats to be countered by the TOE are characterized by the combination of an asset being subject to a threat, a threat agent and an adverse action.

The definition of threat agents and protected assets that follows is applicable to the OSPP base, as well as to the OSPP extended packages, unless noted otherwise.

5.1.1 Assets

Assets to be protected are:

- Persistent storage objects used to store user data and/or TSF data, where this data needs to be protected from any of the following operations:
  - Unauthorized read access
  - Unauthorized modification
  - Unauthorized deletion of the object
  - Unauthorized creation of new objects
  - Unauthorized management of object attributes
- Transient storage objects, including network data
- TSF functions and associated TSF data
- The resources managed by the TSF that are used to store the above-mentioned objects, including the metadata needed to manage these objects.

5.1.2 Threat Agents

Threat agents are external entities that potentially may attack the TOE. They satisfy one or more of the following criteria:

- External entities not authorized to access assets may attempt to access them either by masquerading as an authorized entity or by attempting to use TSF services without proper authorization.
- External entities authorized to access certain assets may attempt to access other assets they are not authorized to either by misusing services they are allowed to use or by masquerading as a different external entity.
- Untrusted subjects may attempt to access assets they are not authorized to either by misusing services they are allowed to use or by masquerading as a different subject.

Threat agents are typically characterized by a number of factors, such as expertise, available resources, and motivation, with motivation being linked directly to the value of the assets at stake.

The TOE protects against intentional and unintentional breach of TOE security by attackers possessing an enhanced-basic attack potential.

The following threats are addressed by the OSPP base-conformant TOEs. The PP covers these threats and organizational security policies necessary to derive the necessary security functionality. There are no threats and policies to justify the assurance level. This is deemed unnecessary, since the chosen evaluation assurance level is already defined in the CC with a rationale explaining the threats countered by the assurance measures.

5.1.3 Threats countered by the TOE

T.ACCESS.TSFDATA	A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.
T.ACCESS.USERDATA	A threat agent might gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy.
T.ACCESS.TSFFUNC	A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.
T.ACCESS.COMM	A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.
T.RESTRICT.NETTRAFFIC	A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.
T.IA.MASQUERADE	A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA.USER	A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.

5.2 Organizational Security Policies

The following organizational security policies are addressed by PP-conformant TOEs:

P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

5.3 Assumptions

The specific conditions below are assumed to exist in a PP-conformant TOE environment.

5.3.1 Physical aspects

A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

5.3.2 Personnel aspects

A.MANAGE	The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

5.3.3 Procedural aspects

A.DETECT	Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
A.PEER.MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
A.PEER.FUNC	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.

5.3.4 Connectivity aspects

A.CONNECT	All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points. Application Note: If the TOE consists of separate parts and the TOE implements mechanisms ensuring the protection TSF data in transit between these parts, the ST author may consider claiming FPT_ITT.1 to supplement or replace A.CONNECT.

6 Security Objectives

The following sections describe the security objectives of the Operating System Protection Profile.

6.1 Security Objectives for the TOE

The following objectives are defined for the TOE.

O.AUDITING	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.CRYPTO.NET	The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.
O.DISCRETIONARY.ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.NETWORK.FLOW	The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.
O.SUBJECT.COM	The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.
O.I&A	The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.

O.TRUSTED_CHANNEL	The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.

6.2 Security Objectives for the Operational Environment

The following objectives are to be met by the operational environment of the TOE.

OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
OE.INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
OE.MAINTENANCE	Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
OE.RECOVER	Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.

OE.TRUSTED.IT.SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

6.3 Rationale for Security Objectives

The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat, assumption or policy and that each threat, assumption or policy is covered by at least one security objective.

6.3.1 Security Objectives coverage

Objectives	SPD coverage
O.AUDITING	P.ACCOUNTABILITY
O.CRYPTO.NET	T.ACCESS.USERDATA, T.ACCESS.TSFDATA, T.ACCESS.TSFFUNC
O.DISCRETIONARY.ACCESS	T.ACCESS.USERDATA, T.ACCESS.TSFDATA
O.NETWORK.FLOW	T.RESTRICT.NETTRAFFIC
O.SUBJECT.COM	T.ACCESS.USERDATA, T.ACCESS.TSFDATA
O.I&A	T.IA.MASQUERADE, T.IA.USER
O.MANAGE	P.ACCOUNTABILITY, P.USER, T.ACCESS.TSFFUNC
O.TRUSTED_CHANNEL	T.ACCESS.COMM

Table 1: Coverage of security objectives for the TOE

Objectives	SPD coverage
OE.ADMIN	A.AUTHUSER, A.MANAGE, A.TRAINEDUSER
OE.REMOTE	T.ACCESS.COMM, A.CONNECT
OE.INFO_PROTECT	P.USER, A.AUTHUSER, A.TRAINEDUSER, A.PHYSICAL, A.MANAGE
OE.INSTALL	A.MANAGE, A.DETECT
OE.MAINTENANCE	A.DETECT
OE.PHYSICAL	A.PHYSICAL
OE.RECOVER	A.MANAGE, A.DETECT
OE.TRUSTED.IT.SYSTEM	A.CONNECT, A.PEER.MGT, A.PEER.FUNC

Table 2: Coverage of security objectives for the TOE environment

6.3.2 Security Objectives sufficiency

Threats	Security Objectives
T.ACCESS.TSFDATA	The threat of accessing TSF data without proper authorization is removed by: • O.CRYPTO.NET requiring cryptographically-protected communication channels for data including TSF data controlled by the TOE in transit between trusted IT systems, • O.DISCRETIONARY.ACCESS requiring that data, including TSF data stored with the TOE, have discretionary access control protection, • O.SUBJECT.COM requiring the TSF to mediate communication between subjects.
T.ACCESS.USERDATA	The threat of accessing user data without proper authorization is removed by: • O.CRYPTO.NET requiring cryptographically-protected communication channels for data including user data controlled by the TOE in transit between trusted IT systems, • O.DISCRETIONARY.ACCESS requiring that data including user data stored with the TOE, have discretionary access control protection, • O.SUBJECT.COM requiring the TSF to mediate communication between subjects.
T.ACCESS.TSFFUNC	The threat of accessing TSF functions without proper authorization is removed by: • O.CRYPTO.NET requiring cryptographically-protected

Threats	Security Objectives
	communication channels to limit which TSF functions are accessible to external entities, • O.MANAGE requiring that only authorized users utilize management TSF functions.
T.ACCESS.COMM	The threat of accessing a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system is removed by: • O.TRUSTED_CHANNEL requiring that the TOE implements a trusted channel between itself and a remote trusted IT system protecting the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system, • OE.REMOTE requiring that those systems providing the functions required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
T.RESTRICT.NETTRAFFIC	The threat of accessing information or transmitting information to other recipients via network communication channels without authorization for this communication attempt is removed by: • O.NETWORK.FLOW requiring the TOE to mediate the communication between itself and remote entities in accordance with its security policy.
T.IA.MASQUERADE	The threat of masquerading as an authorized entity in order to gain unauthorized access to user data, TSF data or TOE resources is removed by: • O.I&A requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
T.IA.USER	The threat of accessing user data, TSF data or TOE resources without being identified and authenticated is removed by: • O.I&A requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only.

Table 3: TOE threats sufficiency

Security Policies	Security Objectives
P.ACCOUNTABILITY	The policy to hold users accountable for their security-relevant actions within the TOE is implemented by: • O.AUDITING providing the TOE with audit functionality, • O.MANAGE allowing the management of this function.
P.USER	The policy to match the trust given to a user and the actions the user is given authority to perform is implemented by: • O.MANAGE allowing appropriately-authorized users to manage the TSF, • OE.INFO_PROTECT, which requires that users are trusted to use the protection mechanisms of the TOE to protect their data.

Table 4: Security policies sufficiency

Assumptions	Security Objectives
A.PHYSICAL	The assumption on the IT environment to provide the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE is covered by: • OE.INFO_PROTECT requiring the approval of network and peripheral cabling, • OE.PHYSICAL requiring physical protection.
A.MANAGE	The assumptions on the TOE security functionality being managed by one or more trustworthy individuals is covered by: • OE.ADMIN requiring trustworthy personnel managing the TOE, • OE.INFO_PROTECT requiring personnel to ensure that information is protected in an appropriate manner, • OE.INSTALL requiring personnel to ensure that components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE, • OE.RECOVER requiring personnel to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
A.AUTHUSER	The assumption on authorized users to possess the necessary authorization to access at least some of the information managed by the TOE and to act in a cooperating manner in a benign environment is covered by: • OE.ADMIN ensuring that those responsible for the TOE are

Assumptions	Security Objectives
	competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains, • OE.INFO_PROTECT requiring that DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly and that users are authorized to access parts of the data maintained by the TOE.
A.TRAINEDUSER	The assumptions on users to be sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data is covered by: • OE.ADMIN requiring competent personnel managing the TOE, • OE.INFO_PROTECT requiring that those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner and that users are trained to exercise control over their own data.
A.DETECT	The assumption that modification or corruption of security-enforcing or security-relevant files will be detected by an administrative user is covered by: • OE.INSTALL requiring an administrative user to ensure that the TOE is distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE, • OE.MAINTENANCE requiring an administrative user to ensure that the diagnostics facilities are invoked at every scheduled preventative maintenance period, verifying the correct operation of the TOE, • OE.RECOVER requiring an administrative user to ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
A.PEER.MGT	The assumption on all remote trusted IT systems to be under the same management control and operate under security policy constraints compatible with those of the TOE is covered by: • OE.TRUSTED.IT.SYSTEM requiring that these remote trusted IT systems are under the same management domain as the TOE, and are managed based on the same rules and policies applicable to the TOE.
A.PEER.FUNC	The assumption on all remote trusted IT systems to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality is covered by:

Assumptions	Security Objectives
	• OE.TRUSTED.IT.SYSTEM requiring that the remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
A.CONNECT	The assumption on all connections to and from remote trusted IT systems and between physically separate parts of the TSF not protected by the TSF itself are physically or logically protected is covered by: • OE.REMOTE requiring that remote trusted IT systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results, • OE.TRUSTED.IT.SYSTEM demanding the physical and logical protection equivalent to the TOE.

Table 5: Assumptions sufficiency

7 Extended Components Definition

7.1 FCS_RNG Generation of random numbers

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

7.1.1 Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

7.1.2 Component leveling:

FCS_RNG.1 is not hierarchical to any other component within the FCS_RNG family.

7.1.3 Management

There are no management activities foreseen.

7.1.4 Audit

There are no actions defined to be auditable.

7.1.5 FCS_RNG.1 Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: physical, non-physical true, deterministic, physical hybrid, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: a defined quality metric].

7.1.6 Rationale

The quality of the random number generator is defined using this SFR. The quality metric required in FCS_RNG.1.2 is detailed in the German Scheme AIS 20 and AIS 31.

7.2 FDP_RIP.3 Full residual information protection of resources

FDP_RIP.3 is analog to FDP_RIP.2 except that it applies to the content of resources that are allocated to subjects or users.

7.2.1 Component leveling

FDP_RIP.3 is not hierarchical to any other component within the FDP_RIP family.

7.2.2 Management

See management description specified for FDP_RIP.2 in [CC].

7.2.3 Audit

See audit requirement specified for FDP_RIP.2 in [CC].

7.2.4 FDP_RIP.3 Full residual information protection of resources

Hierarchical to: No other component

Dependencies: No dependencies

FDP_RIP.3.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, de-allocation of the resource from] all subjects or users.

7.2.5 Rationale

FDP_RIP.3 addresses the problem of resources implemented in main memory that may be allocated to and de-allocated from subjects or users. Unless those resources lose their content automatically as part of the de-allocation and re-allocation process, they must be subject to a process that prepares them for re-use by rendering the previous content unavailable to the subject or user to which it is next allocated. An example is main memory that has been allocated to a subject; this memory must be cleared before it can be re-allocated to a subject with different security attributes (for example a subject operating on behalf of a different user). This preparation prevents the passing of security-critical information via this resource, since such unregulated passing would potentially allow the subject or user to which the memory is next allocated to use this information to violate the security policy. Typical examples of such critical information that may be passed via resources not prepared for re-use are passwords or cryptographic keys.

7.3 FIA_USB.2 Enhanced user-subject binding

FIA_USB.2 is analog to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

7.3.1 Component leveling

FIA_USB.2 is hierarchical to FIA_USB.1.

7.3.2 Management

See management description specified for FIA_USB.1 in [CC].

7.3.3 Audit

See audit requirement specified for FIA_USB.1 in [CC].

7.3.4 FIA_USB.2 Enhanced user-subject binding

Hierarchical to: FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.2.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].

FIA_USB.2.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB.2.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB.2.4 The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

7.3.5 Rationale

An operating system may derive subject security attributes from other TSF data that are not directly user security attributes. An example is the point-of-entry the user has used to establish the connection. An access control policy may also use this subject security attribute within its access control policy, allowing access to critical objects only when the user has connected through specific ports-of-entry.

8 Security Requirements

This chapter specifies the requirements set forth for the TOE. If the OSPP mandates a specific option that cannot be specified as part of the SFR or SAR, the PP marks it as “ST Author Note”. The ST author must apply this note when writing an ST and claiming conformance with this PP.

Notes marked as “Application Note” are informative to support the understanding of the SFR or SAR.

The following styles of marking operations are applied with this Protection Profile:

- Assignments and selections are marked in bold face font.
- Iterations are marked by appending a suffix to the SFR identification.
- Refinements are marked in bold and italic face font.

8.1 Security functionality provided by remote trusted IT systems

All security functional requirements defined in the OSPP base as well as the OSPP extended packages require that the respective functionality is enforced by the TSF. Current technology, however, allows the TSF to consult remote trusted IT systems that support the TSF in the decision process leading to the local enforcement of the decision.

The OSPP requires from ST authors special handling of such separated security mechanisms.

To illustrate such an approach, consider the following example: The TSF implements the mechanism for identification and authentication of users. The TSF may consult a remote LDAP server that is considered to be trusted by the TSF. The following procedure may be followed to provide the identification and authentication mechanism:

1. The TSF transmits the user-provided credentials to the remote LDAP server.
2. The remote LDAP server performs the identification and authentication of the user based on its local I&A policy.
3. The LDAP server communicates the result of the application of the local I&A policy to the TSF (whether the credentials are accepted or not).
4. The TSF enforces the decision of the remote LDAP server by either performing the user-subject binding (if the remote LDAP server accepted the credentials) or by rejecting the user's login attempt (if the remote LDAP server rejected the credentials).

The example can be applied to every security functionality defined with the OSPP base, as well as every OSPP extended package. It is always possible that the TOE may rely on one or more remote trusted IT systems to enforce its security policies.

When dissecting the separation of security functions that are supported by remote trusted IT systems, the following aspects can be identified:

- Security policy decisions made or security functionality provided by the remote trusted IT system. This remote trusted IT system can be considered to act as the “server” counterpart as it waits for requests including requests from the TSF, processes the requests, and returns the results to the requester.
- Security policy enforced and security functionality implemented by the TSF. The TSF can be considered to act as a “client” system as it actively requests service from the remote trusted IT

system and waits for its response. Based on the response, actions are taken. These actions can be as simple as enforcing the decision (in the example above, the user is allowed to log in or not), or these actions can be more complex, for example, the TSF might perform additional processing based on the response.

The OSPP requires the following consideration of the such security mechanisms that rely on remote trusted IT systems:

- If the TSF implements the client aspect, the ST author must specify:
  - One or more assumptions outlining the behavior expected from the remote trusted IT system, specified such that a different ST author (the ST author who may characterize the server side) can derive SFRs from this specification. Note that the specification shall be as precise as necessary for the TSF. The ST author might want to specify a precise rule set to be implemented by the server counterpart, but it might also be possible that the ST author only specifies a very generic reply type the TSF expects from the server.
  - The SFR specification must only cover the locally visible (at the TSFI) policy without any hint to the policy enforced by the remote trusted IT system. Note that the specification of this security policy is in addition to any security policies mandated by the OSPP base (extended packages may be specified requiring a pre-defined client-side security policy). This implies that such a security policy covering the client side of a general security policy must extend the OSPP base. It is not permissible that such a client side security policy is used to cover SFRs mandated by the OSPP base, as the client side functionality must be provided in addition to the general-purpose computing environment mandated by the OSPP base.
- If the TSF implements the server aspect, the ST author must specify:
  - SFRs implementing the security policy that comply with the assumptions specified in the ST for the client side. Note that the specification of this security policy is in addition to any security policies mandated by the OSPP base as outlined for the client-side above.
  - The TSF data of the client side covering the respective security functionality usually transform into user data on the server side, because for the server side, the transmitted data are not used to implement or enforce its security policy. For such scenarios, it is beneficial to define extended components on the server side that resemble the respective client-side SFR.

8.1.1 Example: Access control policy

The following example gives the ST author more insight into the application of the requirements stated above.

This example covers an access control mechanism that is separated as follows:

- The server side stores the permission information for each subject-object combination. In addition, the server side knows and implements the access control rules. It provides a service to other remote trusted IT systems to supply a request that contains the subject requesting access, the object to which access is requested, and the operation to be performed by the subject on the object. The server side returns information to the caller as to whether the request is allowed (the requested operation is allowed to proceed) or denied.

- The client side implements the access control enforcement by controlling and knowing the subjects, objects, and operations between subjects and objects. When an operation is requested from a subject on an object that is covered by the access control policy, the client side submits a corresponding request to the remote trusted IT system providing the above-mentioned information and waits for a response. Once the response is received, the client side enforces the response by either allowing or denying the requested operation.

The example must be covered in the ST specifying the TOE operating as a client:

A.REMOTE_PSO	A remote trusted IT system implements and provides access control decisions to the TSF for the following security policy: Access control policy decisions are returned to the TSF with the TSF providing the parameters with each request consisting of [subject security attribute of user ID, object security attribute of file system object name, and operation requested by the subject on the object].

FDP_ACC.2.1	The TSF shall enforce the **Extended Persistent Storage Object Access Control Policy** on a) **Subjects: processes acting on behalf of users;** b) **Objects: Persistent Storage Objects of file system object;** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.
FDP_ACF.1.1	The TSF shall enforce the **Extended Persistent Storage Object Access Control Policy** to objects based on the following: a) **Subject security attributes: user ID;** b) **Persistent storage object attributes: file system object name.**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: a) **Access to the object by the subject is granted if the remote trusted IT system that is provided with the parameters of [subject security attribute, object security attribute, and operation requested by the subject on the object] replies that the operation is to be allowed.**
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **If the remote trusted IT system is not available or does not respond within 30 seconds after the access request is submitted, access is denied**.

The example must be covered in the ST specifying the TOE operating as a server using the following SFRs defined as extended components (the extension is due to the removal of the

dependency on FDP_ACC.1, as the attributes are not assigned to subjects and objects covered by the TSF):

FDP_ACF_EXT.1.1 The TSF shall support the **Extended Persistent Storage Object Access Control Policy** for requesting clients based on the following:

a) **Subject security attributes:**

i. **user ID transmitted by a remote trusted IT system;**

ii. **group ID assigned to the user ID;**

b) **Persistent storage object attributes:**

i. **file system object name transmitted by a remote trusted IT system;**

ii. **file system object owning user ID;**

iii. **file system object owning group ID;**

iv. **file system object permissions.**

FDP_ACF_EXT.1.2 The TSF shall apply the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) **Per-user access granting: The TSF returns to the requester the indication that access to the object by the subject is granted if the subject security attribute of user ID is equal to the object security attribute of the file system object owning user ID and the permissions assigned to the subject attribute – object attribute combination allows the operation requested by the subject for the owning user; or**

b) **Per-group access granting: The TSF returns to the requester the indication that access to the object by the subject is granted if the subject security attribute group ID is equal to the object security attribute of the file system object owning group ID and the permissions assigned to the subject attribute – object attribute combination allows the operation requested by the subject for the owning group.**

FDP_ACF_EXT.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**.

FDP_ACF_EXT.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

8.2 Security Functional Requirements

8.2.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **basic**[1] level of audit; and

c) **all modifications to the set of events being audited;**

d) **all user authentication attempts;**

e) **all denied accesses to objects for which the access control policy defined in the OSPP base applies;**

f) **explicit modifications of access rights to objects covered by the access control policies; and**

g) **[assignment: other specifically defined auditable events][2].**

Application Note: FAU_GEN.1.1 has the operations being partially performed to reflect the minimum set of events each operating system conformant to this PP must be able to audit. Since the OSPP base requires that an authorized administrator has the capability to select the events to be audited, all activities that change this set are required to be auditable. In addition, all user authentication attempts must be auditable, but it is allowed that an authorized administrator restricts the events that are actually audited to failed authentication attempts, authentication attempts for specific types of users, authentication attempts when specific authentication methods are used, etc. The rules that allow an authorized administrator to define the events that are actually audited from the set of events the TOE is capable of auditing must be defined in the FAU_SEL.1 (or a hierarchically higher component).

It is also required that the operating system is capable of auditing denied access attempts to objects listed in the access control policies. This requirement allows for analysis of denied access attempts in order to detect a potential misconfiguration of access rights, for example, an attack that performs a large number of access attempts.

Explicit modifications of access rights are those that are performed by an explicit request for access right modification. These are critical if, for example, they are performed by a Trojan Horse.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and outcome of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST;

i. **User identity (if applicable); and**

ii. **[assignment: other audit relevant information][3].**

ST Author Note: The specified level of audit applies to all SFRs defined in the OSPP base, as well as every OSPP extended package with which the ST claims conformance.

[1] [selection, choose one of: minimum, basic, detailed, not specified]
[2] [assignment: other specifically defined auditable events].
[3] [assignment: other audit relevant information]

Application Note: The subject identity may be identical to the user identity in the case where the subject identity is established by the user-subject binding process. In this case, only one identity needs to be included in the audit record. The purpose here is the ability to trace an event to the user that caused the event. This may not be possible if the subject identity does not allow to identify the user the subject was bound to when the event happened. In order to support FAU_GEN.2, the user identity has, therefore, been added as the information to be recorded.

Application Note: The outcome to be recorded with the audited event can either be binary (success or failure) or the value resulting from the event, depending on the implementation of the TOE. For example, access control decision shall store the information about the result of the access control decision with the audit trail. A TOE may implement more decision results than just access allowed or denied, where all of these results shall be recorded as outcome of the access control check event.

8.2.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

8.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[4] with the capability to read [assignment: list of audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

ST Author Note: Authorized users can either be human users or other trusted IT systems. The ST author must define the conditions that must be satisfied to allow a user to read audit trail information. An operating system conformant to this Protection Profile may well define different types of users with the conditions they need to meet to read different information from the audit records. An operating system that allows defined human users to read specific types of audit records or specific fields from audit records while also allowing a specific external system to download all audit records is compliant with this requirement.

ST Author Note: The ST author needs to define the exact authorizations required to read the information from the audit record. This may be a specific role that has this capability assigned or one or more privileges that must be assigned to a user.

8.2.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

[4] [assignment: authorised users]

8.2.5 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) **Type of audit event;**[5]

b) **Subject or user identity**[6]**;**

c) **Outcome (success or failure) of the audit event;**

d) **Named object identity;**

e) **[assignment: list of additional attributes that audit selectivity is based upon].**[7]

8.2.6 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorised modifications to the audit records in the audit trail.

Application Note: The TOE may store its audit records locally, or it may pass its audit records on to a remote trusted IT system for storage and further processing. Even in this case, the TOE will usually need some kind of local audit trail as a (probably volatile) cache to buffer some audit records or to bridge the time when the remote audit server might not be available. Such a local audit trail must be protected as described in this SFR.

8.2.7 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit] ***or if any of the following [assignment: list of conditions] is detected that may result in a loss of audit records.***

ST Author Note: There may be a number of conditions that potentially could lead to a loss of audit data; reaching a defined threshold is just one of them. In cases where the audit data is automatically transferred to another trusted IT system, any problem in the communication link with this system could potentially lead to a loss of audit data. FAU_STG.3.1 requires the author of an ST to list the conditions of potential loss of audit data the TSF is able to detect and describe the reaction of the TSF when such a condition is detected. When the reaction is different for different conditions detected, the ST author shall use multiple iterations of FAU_STG.3.1 to describe the different reactions and associate them with the conditions for potential audit data loss detected by the TSF.

ST Author Note: This SFR explicitly is not restricted to the audit trail stored by the TSF only. If the TOE stores the audit trail with a remote trusted IT system, it must be ensured that if the audit trail storage reaches the specified threshold, the TOE

[5] [assignment: list of additional attributes that audit selectivity is based upon]
[6] [selection: object identity, user identity, subject identity, host identity, event type]
[7] [assignment: list of additional attributes that audit selectivity is based upon]

sends a notification to the remote trusted IT systems sending audit data to the TOE to inform about this state.

8.2.8 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by ***~~the authorised user with special rights~~ [assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]***”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

ST Author Note: This SFR explicitly is not restricted to the audit trail stored by the TSF only. If the TOE stores the audit trail with a remote trusted IT system, it must be ensured that if the audit trail storage is full, the TOE sends a notification to the remote trusted IT systems sending audit data to the TOE to inform about this state.

8.2.9 FCS_CKM.1(SYM) Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate ***symmetric*** cryptographic keys in accordance with a specified cryptographic key generation algorithm **capable of generating a random bit sequence**[8] and specified cryptographic key sizes:

a) **128 bits,**

b) **168 bits,**

c) **256 bits,**

d) **[assignment: other cryptographic key sizes]**[9]

that meet the following: **[assignment: cryptographic key generation algorithm that has the following properties: Compromising the security of the key generation method shall require as least as many operations as determining the value of the generated key by exhaustive search of the key space]**[10]**.**

Application Note: The SFR statement assumes the random bit generator to apply a "pessimistic" estimate of the entropy in its entropy pool. The requirement of the SFR concerning the entropy specifies that even with the pessimistic entropy estimate, the number of bits extracted from the entropy pool is less than the estimated entropy in the pool.

Forward secrecy means that even with the knowledge of all extracted random bits, it is not possible to predict the next random bits that will be extracted.

Backward secrecy means that even when extracting an arbitrary sequence of random bits, it is not possible to deduce any previously extracted random bits.

ST Author Note: Multiple implementations of the key generation mechanism may be present in the TOE. The ST author shall specify:

8 [assignment: cryptographic key generation algorithm]
9 [assignment: cryptographic key sizes]
10 [assignment: list of standards]

a) Which implementations are covered by the SFR claim, and

b) Which usage scenarios are covered by the SFR claim (for example, implementation covers support for SSH only).

ST Author Note: If the key generation is based on a random number generator or random bit generator, national schemes may require additional extended SFRs to be claimed. For example, in the German scheme, the ST author shall claim FCS_RNG.1 from the version of AIS20/AIS31 current at the time of ST release published by the German scheme.

ST Author Note: If the national scheme does not define any specific evaluation requirements for random number generators, the extended component FCS_RNG.1 defined with this PP has to be added to the ST by the ST author.

8.2.10 FCS_CKM.1(RSA) Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate ***RSA*** cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in U.S. NIST FIPS PUB 186-3 appendix B.3**[11] and specified cryptographic key sizes:

a) **2048 bits,**

b) **[assignment: other cryptographic key sizes]**[12]

that meet the following:

a) **U.S. NIST FIPS PUB 186-3,**

b) **[assignment: list of standards]**[13].

ST Author Note: Multiple implementations of the key generation mechanism may be present in the TOE. The ST author shall specify:

a) Which implementations are covered by the SFR claim, and

b) Which usage scenarios are covered by the SFR claim (for example, implementation covers support for SSH only).

8.2.11 FCS_CKM.1(DSA) Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate ***DSA*** cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in U.S. NIST FIPS PUB 186-3 appendix B.1**[14] and specified cryptographic key sizes:

[selection:

a) **L=1024, N=160 bits;**

b) **L=2048, N=224 bits;**

c) **L=2048, N=256 bits;**

d) **L=3072, N=256 bits;**

e) **[assignment: other cryptographic key sizes];**

11 [assignment: cryptographic key generation algorithm]
12 [assignment: cryptographic key sizes]
13 [assignment: list of standards]
14 [assignment: cryptographic key generation algorithm]

f) **DSA domain parameter generation for specified values for L and N];**[15]

that meet the following:

a) **U.S. NIST FIPS PUB 186-3,**

b) **[assignment: list of standards]**[16].

ST Author Note: Multiple implementations of the key generation mechanism may be present in the TOE. The ST author shall specify:

a) Which implementations are covered by the SFR claim, and

b) Which usage scenarios are covered by the SFR claim (for example implementation covers support for SSH only).

8.2.12 FCS_CKM.2(NET) Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with ***~~a~~ the following*** specified cryptographic key distribution method ***~~[assignment: cryptographic key distribution method]~~*** that meets the following: **[selection:**

a) **Diffie-Hellman key agreement method defined for the SSH protocol by RFC4253;**

b) **Public [selection: DSS, RSA] host key exchange defined for the SSH protocol by RFC4253;**

c) **RSA encrypted exchange of pre-master secrets defined for the TLS protocol by RFC5246;**

d) **Diffie-Hellman key agreement method defined for the IKE protocol by RFC2409;**

e) **Diffie-Hellman key agreement method defined for the IKE protocol by RFC4306;**

f) **[assignment: other key distribution methods with their standards]]**[17].

Application Note: The TOE must implement at least one network protocol which protects the transported data.

8.2.13 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **of [selection: zeroization, [assignment: other cryptographic key destruction method]]**[18] that meets the following: **[selection: vendor-specific zeroization, [assignment: list of applicable standards]]**[19].

15 [assignment: cryptographic key sizes]
16 [assignment: list of standards]
17 [assignment: list of standards]
18 [assignment: cryptographic key destruction method]
19 [assignment: list of standards]

Application Note: The ST author shall consult the national scheme for acceptable key destruction standards.

8.2.14 FCS_COP.1(NET) Cryptographic operation

FCS_COP.1.1 The TSF shall perform **encryption, decryption, integrity verification, peer authentication**[20] in accordance with ***~~a specified~~ the following*** cryptographic algorithm***s,*** cryptographic key sizes ***~~[assignment: cryptographic key sizes] that meet the following~~ and applicable standards***: **[selection:**

a) **SSH allowing the use of TDES in CBC mode with 168 bits key size, and HMAC-SHA1 defined by RFC 4253;**

b) **SSH allowing the use of AES in CBC mode with 128 bits and 256 bits key size, and HMAC-SHA1 defined by RFC 4253;**

c) **TLS allowing the use of TDES in CBC mode with 168 bits key size, and SHA-1 defined by RFC5246;**

d) **TLS allowing the use of AES in CBC mode with 128 bits and 256 bits key size, and SHA-1 defined by RFC5246;**

e) **IPSEC with IKE allowing the use of TDES in CTR mode with 168 bits key size, and SHA-1 defined by RFC 4301 and RFC 4303;**

f) **IPSEC with IKE allowing the use of AES in CTR mode with 128 bits and 256 bits key size, and SHA-1 defined by RFC 4301 and RFC 4303;**

g) **[assignment: other cryptographic network algorithms, keys sizes with their standards]**

][21].

ST Author Note: The TOE must implement at least one network protocol that protects the transported data. When using the assignment, the ST author must specify protocols that comply with all requirements specified for O.CRYPTO.NET. It is permissible to specify multiple protocols that meet the requirements of O.CRYPTO.NET when combining them. In this case, the ST must clearly specify that multiple protocols are required and must specify how these protocols are combined to achieve the objective.

Application Note: Please note that when selecting IPSEC, the given selections only refer to ESP. If the ST author also wants to claim AH, a reference to RFC4302 should be added.

8.2.15 FDP_ACC.1(PSO) Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Persistent Storage Object Access Control Policy**[22] on

a) **[assignment: list types of users and/or types of subjects covered by the SFP];**

[20] [assignment: list of cryptographic operations]
[21] [assignment: list of standards]
[22] [assignment: access control SFP]

b) **Objects**:

i. **Persistent Storage Objects of the following type [assignment: enumerate all persistent storage objects covered by this SFP]**;

ii. **[assignment: other storage objects covered by this SFP];**

c) **Operations: [assignment: list of operations covered by the SFP]**[23].

ST Author Note: The list of operations on the object needs to cover the creation of a new object, the destruction of an object, all types of access to the object, as well as operations on TSF data associated and stored with the object (for example, object name, access control list associated with the object, other object security attributes). If some of those operations are covered by SFRs related to the management of TSF data, the ST author shall include a reference to those SFRs in order to allow the ST reader to identify where those operations are described.

ST Author Note: When the TOE includes several different types of named objects implemented using persistent storage and when the TOE implements fundamentally different access control rules for those different types of named objects, the ST author shall use iterations of FDP_ACC to describe the access control rules for the different object types.

Application Note: A persistent storage object establishes a data storage or data exchange link between two or more subjects. Examples of persistent storage objects are: files, directories.

8.2.16 FDP_ACC.1(TSO) Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Transient Storage Object Access Control Policy**[24] on

a) **[assignment: list types of users and/or types of subjects covered by the SFP];**

b) **Objects:**

i. **Transient Storage Objects of the following type [assignment: enumerate all transient storage objects covered by this SFP];**

ii. **[assignment: other storage objects covered by this SFP];**

c) **Operations: [assignment: list of operations covered by the SFP]**[25].

Application Note: A transient storage object establishes a data exchange link between two or more subjects or users. Examples of transient storage objects are: shared memory, semaphores, message queues, named/unnamed pipes.

8.2.17 FDP_ACF.1(PSO) Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Persistent Storage Object Access Control Policy**[26] to objects based on the following: [assignment: list of subjects ***or users*** and

[23] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[24] [assignment: access control SFP]
[25] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[26] [assignment: access control SFP]

objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[assignment: rules governing access among controlled subjects ***and/or users*** and controlled objects using controlled operations on controlled objects ***that allow to grant access down to the granularity of single subjects or users***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly authorise access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly deny access of subjects to objects].

8.2.18 FDP_ACF.1(TSO) Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Transient Storage Object Access Control Policy**[27] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly authorise access of subjects to objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly deny access of subjects to objects].

8.2.19 FDP_IFC.2(NI) Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the **Network Information Flow Control Policy**[28] on

a) **Subjects:**

   i. **unauthenticated external IT entities that send and receive information mediated by the TOE;**

   ii. **[assignment: list of subjects or users] that send and receive information mediated by the TOE;**

b) **Information:**

   i. **Network data routed through the TOE;**

   ii. **[assignment: other information covered by the SFP];**[29]

[27] [assignment: access control SFP]
[28] [assignment: information flow control SFP]
[29] [assignment: list of subjects and information]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application Note: The OSPP explicitly does not specify the version of the Internet Protocol. This implies that the Internet Protocol versions usable in the evaluated configuration must be covered by this SFR.

8.2.20 FDP_IFF.1(NI) Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Network Information Flow Control Policy**[30] based on the following types of subject and information security attributes:

a) **Object security attribute: the logical or physical network interface through which the network data entered the TOE;**

[selection:

b) **TCP/IP information security attributes:**

i. **Source and destination IP address,**

ii. **Source and destination TCP port number,**

iii. **Source and destination UDP port number,**

iv. **Network protocol of [selection: IP, TCP, UDP, ICMP, [assignment: other protocols]],**

v. **TCP header flags of [selection: SYN, ACK, [assignment: other flags]],**

vi. **[assignment: other attributes of an IP packet];**

c) **IEEE 802.1Q VLAN tag information security attributes:**

i. **VLAN tag;**

d) **[assignment: other network data information security attributes]**

][31].

Application Note: Logical network interfaces include the interface provided by the TOE to local subjects acting on behalf of local users. Such interfaces may include network sockets introduced by the Berkeley Software Distribution (BSD) or any other mechanism that allows subject to initiate an IP-based connection.

Application Note: The minimum requirement of the network flow control specified in FDP_IFF.1.3(NI) defines the purpose of the Network Information Flow Control Policy, namely to identify network data using the security attributes specified here and to at least discard the identified network data or allow it to pass the TOE unaltered. An ST author may specify network data security attributes which differ from the TCP/IP attributes or the VLAN tag attributes. However,

30 [assignment: information flow control SFP]

31 [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

these security attributes must allow the minimum requirements of FDP_IFF.1.3(NI) to be achieved.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

FDP_IFF.1.3 The TSF shall enforce the **following rules:**

Identification of network data using one or more of the following concepts:

a) **Information security attribute matching;**

b) **[selection: Matching based on the state of a TCP connection, Time-based matching, Statistical analysis matching, [assignment: other matching concepts]];**

Performing one or more of the following actions with identified network data:

a) **Discard the network data [selection: without any further processing, with sending a notification to the sender];**

b) **Allow the network data to be processed unaltered by the TOE according to the routing information maintained by the TOE;**

c) **[assignment: other actions]**[32].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly authorise information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes ***or other TSF data***, that explicitly deny information flows].

Application Note: The OSPP explicitly does not specify the version of the Internet Protocol for the TCP/IP network data security attributes. This implies that the Internet Protocol versions usable in the evaluated configuration must be covered by this SFR.

8.2.21 FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the **Persistent Storage Access Control Policy, Transient Storage Access Control Policy, Network Information Flow Control Policy, [assignment: access control SFP(s) and/or information flow control SFP(s)]**[33] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

[32] [assignment: additional information flow control SFP rules]
[33] [assignment: access control SFP(s) and/or information flow control SFP(s)]

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

Application Note: If, for example, file names or file name extensions are used for access control decisions, they are security attributes. In the case that an external file system is mounted, this is considered an import of user data with security attributes, and therefore, FDP_ITC rules must be defined and satisfied.

Application Note: Based on the wording of FDP_ITC.2.1, the TOE complies with this SFR even when it does not allow import of objects covered by the persistent or transient storage object control policy.

However, the network information flow control policy must always be covered by the TOE, as it applies to the networking capability of the TOE to control traffic originating from outside the TOE. In this case, the interpretation of security attributes is defined by the respective protocol family.

8.2.22 FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, de-allocation of the resource from] all objects.

8.2.23 FDP_RIP.3 Full residual information protection of resources

FDP_RIP.3.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, de-allocation of the resource from] all subjects or users.

8.2.24 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator-configurable number of**[34] unsuccessful authentication attempts ***for the authentication method [assignment: authentication method]*** occur related to [assignment: list of authentication events].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall: [assignment: list of actions].

Application Note: The TOE may use different authentication methods for different types of users and have different rules for how to handle authentication failures based on the authentication method and/or user type. Authentication failures for remote systems are usually treated differently from authentication attempts for human users. Even for human users, the reaction to authentication failures may be different for authentication via userid/password and authentication via smartcards or digital certificates.

[34] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

8.2.25 FIA_ATD.1(HU) User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ***human*** users:

a) **User identifier;**

b) **Group memberships;**

c) **User password;**

d) **Software token verification data;**

e) **Security roles;**

f) **[assignment: other user security attributes]**[35].

ST Author Note: If the TOE allows a remote trusted IT system to maintain the user attributes and the TOE maintains a local data store for either a backup reason (for example, if the connection to the remote trusted IT system is severed) or as a supplement to the remote trusted IT system, the ST author shall iterate this SFR with one iteration applicable to the security attribute maintained by the TSF and the other one applicable to the security attribute maintained by the remote trusted IT system.

Application Note: The software token verification data can be implemented as transient in nature. For example, a Kerberos ticket granting ticket or Kerberos ticket is created when the user requests these tickets. The ticket granting server has the data to verify the Kerberos ticket granting ticket, whereas the application server has the data to verify the Kerberos ticket.

8.2.26 FIA_ATD.1(TU) User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ***technical*** users:

a) **the logical or physical network interface through which the network data entered the TOE;**

b) **identity of the logical or physical external interface through which the user connected to the TOE;**

c) **[assignment: other user security attributes]**[36].

ST Author Note: The ST Author Note defined for FIA_ATD.1(HU) applies here, as well.

Application Note: Bullet a) of this SFR relates to FDP_IFC.2(NI) and FDP_IFF.1(NI). In the Common Criteria scheme, external entities are always considered to be users. Therefore, every network data entity must be specified as user in this PP.

8.2.27 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20**[37]**.**

[35] [assignment: list of security attributes]
[36] [assignment: list of security attributes]
[37] [assignment: a defined quality metric]

8.2.28 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

a) **the information flow covered by the Network Information Flow Control Policy;**

b) **[assignment: list of TSF other mediated actions]**[38]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.2.29 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **the following authentication mechanisms:**

a) **Authentication based on username and password;**

b) **Authentication based on software token verification data;**

c) **[assignment: list of other authentication mechanisms]**[39]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following rules:**

a) **Authentication based on username and password is performed for TOE-originated requests and credentials stored by the TSF;**

b) **Authentication based on software token verification data is performed for TOE-originated requests;**

c) **[assignment: other rules describing how the multiple authentication mechanisms provide authentication and to which authentication policy it applies]**[40].

ST Author Note: Bullet a) requires that the TOE provides a complete self-sufficient identification and authentication mechanism based on on username and password with locally stored credentials which supports the identification and authentication mechanism defined by the OSPP base. Nevertheless, the ST author is allowed to specify additional username/password based authentication mechanisms with potentially remote credential stores. In such a case, the ST author must specify the relationship between the two (or more) username/password based authentication mechanisms, such as the specification of the precedence.

In general, if multiple authentication methods are specified for the same credentials, the ST author must specify the relationship between them.

ST Author Note: If any aspect of the rules for authentication can be managed, the ST author shall specify an iteration of FMT_MTD.1 covering this management aspect.

[38] [assignment: list of TSF mediated actions]
[39] [assignment: list of multiple authentication mechanisms]
[40] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

Application Note: For the term “software token verification data”, see the application note for FIA_ATD.1(HU).

Application Note: To support the specification of the SFR of FIA_UAU.5, the ST author may want to specify the link mechanism between the frontends and the backends for providing the authentication mechanisms. For example, the ST author may wish to state that a login application uses GSSAPI to utilize Kerberos.

8.2.30 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only **obscured feedback**[41] to the user while the authentication is in progress.

8.2.31 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

8.2.32 FIA_USB.2 Enhanced user-subject binding

FIA_USB.2.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

a) **The user identity that is associated with auditable events;**

b) **The user security attributes that are used to enforce the Persistent Storage Object Access Control Policy;**

c) **The user security attributes that are used to enforce the Transient Storage Object Access Control Policy;**

d) **The software token that can be used for subsequent identification and authentication with the TSF or other remote IT systems;**

e) **Active roles;**

f) **Active groups;**

g) **[assignment: list of other security attributes]**[42].

ST Author Note: It is permissible to assign only a subset of the specified attributes to a subject acting on behalf of a user at one specific user-subject binding process. However, all of the specified assignments must be supported and enforced by the TOE depending on the type of the user-subject binding process in case multiple types are implemented. These types must be enumerated in the following assignments.

FIA_USB.2.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

41 [assignment: list of feedback]
42 [assignment: list of user security attributes]

FIA_USB.2.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB.2.4 The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

8.2.33 FMT_MSA.1(PSO) Management of object security attributes

FMT_MSA.1.1 The TSF shall enforce the **Persistent Storage Object Access Control Policy**[43] to restrict the ability to **modify [selection: change_default, query, delete, [assignment: other operations]]**[44] the security attributes **of the objects covered by the SFP**[45] to **the owner of the object and [assignment: rules that need to be satisfied for other users to perform the operations]**[46].

8.2.34 FMT_MSA.1(TSO) Management of object security attributes

FMT_MSA.1.1 The TSF shall enforce the **Transient Storage Object Access Control Policy**[47] to restrict the ability to **modify [selection: change_default, query, delete, [assignment: other operations]]**[48] the security attributes **of the objects covered by the SFP**[49] to **the owner of the object and [assignment: rules that need to be satisfied for other users to perform the operations]**[50].

8.2.35 FMT_MSA.3(PSO) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Persistent Storage Object Access Control Policy**[51] to provide **restrictive**[52] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[53] to specify alternative initial values to override the default values when an object or information is created.

8.2.36 FMT_MSA.3(TSO) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Transient Storage Object Access Control Policy**[54] to provide **restrictive**[55] default values for security attributes that are used to enforce the SFP.

43 [assignment: access control SFP(s), information flow control SFP(s)]
44 [selection: change_default, query, modify, delete, [assignment: other operations]]
45 [assignment: list of security attributes]
46 [assignment: the authorised identified roles]
47 [assignment: access control SFP(s), information flow control SFP(s)]
48 [selection: change_default, query, modify, delete, [assignment: other operations]]
49 [assignment: list of security attributes]
50 [assignment: the authorised identified roles]
51 [assignment: access control SFP, information flow control SFP]
52 [selection, choose one of: restrictive, permissive, [assignment: other property]]
53 [assignment: the authorised identified roles]
54 [assignment: access control SFP, information flow control SFP]
55 [selection, choose one of: restrictive, permissive, [assignment: other property]]

FMT_MSA.3.2 The TSF shall allow the **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[56] to specify alternative initial values to override the default values when an object or information is created.

8.2.37 FMT_MSA.3(NI) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Network Information Flow Control Policy**[57] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[58] to specify alternative initial values to override the default values when an object or information is created.

8.2.38 FMT_MSA.4(PSO) Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes ***for Persistent Storage Objects***: [assignment: rules for setting the values of security attributes] .

8.2.39 FMT_MTD.1(AE) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **query, modify**[59] the **set of audited events**[60] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[61].

Application Note: This SFR applies to FAU_SEL.1.

8.2.40 FMT_MTD.1(AS) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **clear, [selection: configure the storage location, create, delete, [assignment: other operations]]**[62] the **audit storage**[63] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[64].

Application Note: This SFR applies to FAU_STG.1.

8.2.41 FMT_MTD.1(AT) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify, [selection: add, delete]**[65] the

a) **threshold of the audit trail when an action is performed;**

56 [assignment: the authorised identified roles]
57 [assignment: access control SFP, information flow control SFP]
58 [assignment: the authorised identified roles]
59 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
60 [assignment: list of TSF data]
61 [assignment: the authorised identified roles]
62 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
63 [assignment: list of TSF data]
64 [assignment: the authorised identified roles]
65 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

b) **action when the threshold is reached**[66]

to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[67].

Application Note: This SFR applies to FAU_STG.3.

8.2.42 FMT_MTD.1(AF) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify, [selection: add, delete]**[68] the **actions to be taken in case of audit storage failure**[69] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[70].

Application Note: This SFR applies to FAU_STG.4.

8.2.43 FMT_MTD.1(NI) Management of TSF data

FMT_MSA.1.1 The TSF shall restrict the ability to **query, modify, delete, [selection: change_default, [assignment: other operations]]**[71] the **security attributes for the rules governing the**

a) **identification of network data;**

b) **actions performed on the identified network data**[72]

to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[73].

Application Note: This SFR applies to FDP_IFF.1(NI).

8.2.44 FMT_MTD.1(IAT) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify**[74] the **threshold for unsuccessful authentication attempts**[75] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[76].

Application Note: This SFR applies to FIA_AFL.1.

66 [assignment: list of TSF data]
67 [assignment: the authorised identified roles]
68 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
69 [assignment: list of TSF data]
70 [assignment: the authorised identified roles]
71 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
72 [assignment: list of TSF data]
73 [assignment: the authorised identified roles]
74 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
75 [assignment: list of TSF data]
76 [assignment: the authorised identified roles]

8.2.45 FMT_MTD.1(IAF) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **re-enable**[77] the **authentication to the account subject to authentication failure**[78] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[79].

Application Note: This SFR applies to FIA_AFL.1.

8.2.46 FMT_MTD.1(IAU) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **initialize, modify, delete**[80] the **user security attributes**[81] to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[82].

Application Note: This SFR applies to FIA_ATD.1, FIA_UAU.1, FIA_UID.1.

8.2.47 FMT_REV.1(OBJ) Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke **object security attributes defined by SFPs**[83] associated with the **corresponding object**[84] under the control of the TSF to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[85].

FMT_REV.1.2 The TSF shall enforce the ***following*** rules:

a) **The access rights associated with an object shall be enforced when an access check is made;**

b) **[assignment: specification of other revocation rules]**[86].

8.2.48 FMT_REV.1(USR) Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke **user security attributes defined by the SFP**[87] associated with the **corresponding user**[88] under the control of the TSF to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[89].

FMT_REV.1.2 The TSF shall enforce the ***following*** rules:

a) **The enforcement of the revocation of security-relevant authorizations with the next user-subject binding process during the**

77 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
78 [assignment: list of TSF data]
79 [assignment: the authorised identified roles]
80 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
81 [assignment: list of TSF data]
82 [assignment: the authorised identified roles]
83 [assignment: list of security attributes]
84 [selection: users, subjects, objects, [assignment: other additional resources]]
85 [assignment: the authorised identified roles]
86 [assignment: specification of revocation rules]
87 [assignment: list of security attributes]
88 [selection: users, subjects, objects, [assignment: other additional resources]]
89 [assignment: the authorised identified roles]

next authentication of the user;

b) **[assignment: specification of other revocation rules][90].**

8.2.49 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) **Management of auditing;**

b) **Management of cryptographic network protocols;**

c) **Management of Persistent Storage Object Access Control Policy;**

d) **Management of Transient Storage Object Access Control Policy;**

e) **Management of Network Information Flow Control Policy;**

f) **Management of identification and authentication policy;**

g) **Management of user security attributes;**

h) **[assignment: other management functions to be provided by the TSF][91].**

8.2.50 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

a) **User role with the following rights:**

i. **Users are authorized to modify their own user password;**

ii. **Users are authorized to modify the access control permissions for the named objects they own;**

iii. **[assignment: other rights];**

b) **[assignment: other management roles][92].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

8.2.51 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

8.2.52 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.

ST Author Note: This SFR applies to FDP_ITC.2 and operations must be performed consistent with FDP_ITC.2.

[90] [assignment: specification of revocation rules]
[91] [assignment: list of management functions to be provided by the TSF]
[92] [assignment: the authorised identified roles]

8.2.53 FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session ***to a human user maintained by the TSF*** after [assignment: time interval of user inactivity] by:

a) clearing or overwriting ***TSF controlled*** display devices, making the current contents unreadable;

b) disabling any activity of the user's ***TSF controlled*** data access/***TSF controlled*** display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session:

a) **Successful re-authentication with the credentials of the user owning the session using [assignment: list of authentication methods out of the list of allowed methods specified in FIA_UAU.5];**

b) **[assignment: other events to occur]**[93].

Application Note: It is possible that the TSF establishes a connection to a session on a remote trusted IT system, for example when using SSH. This remote trusted IT system maintains the session established with the communication channel. The locking requirement however applies to the session maintained by the TSF only as the TSF can only exercise control of the sessions it maintains.

8.2.54 FTA_SSL.2 User-initiated locking

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session ***maintained by the TSF***, by:

a) clearing or overwriting ***TSF controlled*** display devices, making the current contents unreadable;

b) disabling any activity of the user's ***TSF controlled*** data access/***TSF controlled*** display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session:

a) Successful re-authentication with the credentials of the user owning the session using [assignment: list of authentication methods out of the list of allowed methods specified in FIA_UAU.5];

b) [assignment: other events to occur].

Application Note: It is possible that the TSF establishes a connection to a session on a remote trusted IT system, for example when using SSH. This remote trusted IT system maintains the session established with the communication channel. The locking requirement however applies to the session maintained by the TSF only, as the TSF can only exercise control of the sessions it maintains.

8.2.55 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels

[93] [assignment: events to occur]

and provides assured identification of its end points and protection of the channel data from modification ***~~or~~ and*** disclosure ***using the following mechanisms:***

a) Cryptographically-protected communication channel using [assignment: defined cryptographic protocol];

b) [selection: physically protected communication channel;

c) [assignment: other mechanisms for trusted communication channels]].

ST Author Note: The ST author must ensure that the cryptographic protocol specified in this SFR is also listed in FCS_COP.1(NET).

FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **all security functions specified in the ST that interact with remote trusted IT systems and [assignment: list of functions or other conditions which require a trusted channel]**[94].

8.3 Rationale for Security Functional Requirements

This section provides the rationale for the internal consistency and completeness of the security functional requirements defined in this Protection Profile.

8.3.1 Internal Consistency of Requirements

The mutual support and internal consistency of the components selected for this Protection Profile is described in this section.

The following rationale demonstrates the internal consistency of the functional requirements.

8.3.1.1 Audit

The TOE shall implement a general audit mechanism. This audit mechanism shall generate audit records for all security-relevant events, where an authorized user shall have the capability to select the audited events. An authorized user shall be provided with the means to read and interpret the audit data. The TOE shall protect the audit trail and ensure that proper actions are taken when the audit trail fills up or is full.

8.3.1.2 Cryptographic Support

The TOE shall provide a cryptographically-protected network protocol based on symmetric ciphers, which supports authentication of the remote peer. For supporting the authentication, the TOE shall provide the means to generate DSA and RSA keys.

8.3.1.3 User Data Protection

Two general types of user data shall be protected by a TOE, namely persistent storage objects and transient storage objects, for which access control policies are defined. In addition, an information flow control policy ensures that only intended network traffic is allowed by the TOE. The user data protection is supported by proper residual information protection.

[94] [assignment: list of functions for which a trusted channel is required]

8.3.1.4 Identification and Authentication

Entities interacting with the TOE shall be properly identified and authenticated (with the exception of the information flow controlled by the TOE security policy, which only requires proper identification). The user-subject binding process ensures that external entities have a TSF-controlled representation to allow the enforcement of the security policies on them. Supporting to the identification and authentication is the password quality mechanism mandated by the TOE.

8.3.1.5 Security Management

The TOE shall provide management mechanisms for all security functions, including the management functionality itself.

8.3.1.6 TOE Access

The TOE shall provide the capability to lock sessions established for subjects either initiated by the user controlling the subject or by the TOE.

8.3.1.7 TOE Protection

Communication between the TOE and remote trusted IT systems shall be protected using TSF mechanisms.

8.3.2 Security Requirements Coverage

SFR	Objectives
FAU_GEN.1	O.AUDITING
FAU_GEN.2	O.AUDITING
FAU_SAR.1	O.AUDITING
FAU_SAR.2	O.AUDITING
FAU_SEL.1	O.AUDITING
FAU_STG.1	O.AUDITING
FAU_STG.3	O.AUDITING
FAU_STG.4	O.AUDITING
FCS_CKM.1(SYM)	O.CRYPTO.NET
FCS_CKM.1(RSA)	O.CRYPTO.NET
FCS_CKM.1(DSA)	O.CRYPTO.NET
FCS_CKM.2(NET)	O.CRYPTO.NET
FCS_CKM.4	O.CRYPTO.NET
FCS_COP.1(NET)	O.CRYPTO.NET
FDP_ACC.1(PSO)	O.DISCRETIONARY.ACCESS

SFR	Objectives
FDP_ACC.1(TSO)	O.SUBJECT.COM
FDP_ACF.1(PSO)	O.DISCRETIONARY.ACCESS
FDP_ACF.1(TSO)	O.SUBJECT.COM
FDP_IFC.2(NI)	O.NETWORK.FLOW
FDP_IFF.1(NI)	O.NETWORK.FLOW
FDP_ITC.2	O.DISCRETIONARY.ACCESS O.SUBJECT.COM O.NETWORK.FLOW
FDP_RIP.2	O.AUDITING O.CRYPTO.NET O.DISCRETIONARY.ACCESS O.SUBJECT.COM O.NETWORK.FLOW O.I&A
FDP_RIP.3	O.AUDITING O.CRYPTO.NET O.DISCRETIONARY.ACCESS O.SUBJECT.COM O.NETWORK.FLOW O.I&A
FIA_AFL.1	O.I&A
FIA_ATD.1(HU)	O.I&A
FIA_ATD.1(TU)	O.NETWORK.FLOW
FIA_SOS.1	O.I&A
FIA_UAU.1	O.I&A
FIA_UAU.5	O.I&A
FIA_UAU.7	O.I&A
FIA_UID.1	O.I&A O.NETWORK.FLOW
FIA_USB.2	O.I&A
FMT_MSA.1(PSO)	O.MANAGE
FMT_MSA.1(TSO)	O.MANAGE

SFR	Objectives
FMT_MSA.3(PSO)	O.MANAGE
FMT_MSA.3(TSO)	O.MANAGE
FMT_MSA.3(NI)	O.MANAGE
FMT_MSA.4(PSO)	O.MANAGE
FMT_MTD.1(AE)	O.MANAGE
FMT_MTD.1(AS)	O.MANAGE
FMT_MTD.1(AT)	O.MANAGE
FMT_MTD.1(AF)	O.MANAGE
FMT_MTD.1(NI)	O.MANAGE
FMT_MTD.1(IAT)	O.MANAGE
FMT_MTD.1(IAF)	O.MANAGE
FMT_MTD.1(IAU)	O.MANAGE
FMT_REV.1(OBJ)	O.MANAGE
FMT_REV.1(USR)	O.MANAGE
FMT_SMF.1	O.MANAGE
FMT_SMR.1	O.MANAGE
FPT_STM.1	O.AUDITING
FPT_TDC.1	O.DISCRETIONARY.ACCESS O.SUBJECT.COM O.NETWORK.FLOW
FTA_SSL.1	O.I&A
FTA_SSL.2	O.I&A
FTP_ITC.1	O.TRUSTED_CHANNEL

Table 6: Security Functional Requirements coverage

Objectives	Coverage Rationale
O.AUDITING	The events to be audited are defined in [FAU_GEN.1] and are associated with the identity of the user that caused the event [FAU_GEN.2]. Authorized users are provided the capability to read the audit records [FAU_SAR.1], while all other users are denied access to the audit records [FAU_SAR.2]. The authorized user must

Objectives	Coverage Rationale
	have the capability to specify which audit records are generated [FAU_SEL.1]. The TOE prevents the audit log from being modified or deleted [FAU_STG.1] and ensures that the audit log is not lost due to resource shortage [FAU_STG.3, FAU_STG.4]. To support auditing, the TOE is able to maintain proper time stamps [FPT_STM.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
O.CRYPTO.NET	The cryptographically-protected network protocol [FCS_COP.1(NET)] is supported by the generation of symmetric keys [FCS_CKM.1(SYM)], as well as asymmetric keys [FCS_CKM.1(RSA), FCS_CKM.1(DSA)]. As part of the cryptographic network protocol, the TOE securely exchanges the symmetric key with a remote trusted IT system [FCS_CKM.2(NET)]. The TOE ensures that all keys are zeroized upon de-allocation [FCS_CKM.4]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
O.DISCRETIONARY.ACCESS	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must have a defined scope of control [FDP_ACC.1(PSO)]. The rules for the access control policy are defined [FDP_ACF.1(PSO)]. When import of user data is allowed, the TOE must ensure that user data security attributes required by the access control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
O.NETWORK.FLOW	The network information flow control mechanism controls the information flowing between different entities [FDP_IFC.2(NI)]. The TOE implements a rule-set governing the information flow [FDP_IFF.1(NI)]. To facilitate the information flow control, the information must be identified [FIA_UID.1] based on security attributes the TOE can maintain [FIA_ATD.1(TU)]. The TOE must ensure that security attributes of the network data required by the information flow control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
O.SUBJECT.COM	The TSF must control the exchange of data using transient storage objects between subjects based on the identity of users.

Objectives	Coverage Rationale
	The access control policy must have a defined scope of control [FDP_ACC.1(TSO)]. The rules for the access control policy are defined [FDP_ACF.1(TSO)]. When import of user data is allowed, the TOE must ensure that user data security attributes required by the access control policy are correctly interpreted [FDP_ITC.2, FPT_TDC.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3].
O.I&A	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process [FIA_UID.1, FIA_UAU.1]. Multiple I&A mechanisms are allowed as specified in [FIA_UAU.5]. To ensure authorized access to the TOE, authentication data is protected [FIA_ATD.1(HU), FIA_UAU.7]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB.2]. The appropriate strength of the authentication mechanism is ensured [FIA_SOS.1]. To support the strength of authentication methods, the TOE is capable of identifying and reacting to unsuccessful authentication attempts [FIA_AFL.1]. In addition, user-initiated and TSF-initiated session locking [FTA_SSL.1, FTA_SSL.2] protect the authenticated user's session. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2, FDP_RIP.3] are present.
O.MANAGE	The TOE provides management interfaces globally defined in [FMT_SMF.1] for: • the access control policies [FMT_MSA.1(PSO), FMT_MSA.1(TSO), FMT_MSA.3(PSO), FMT_MSA.3(TSO)]; • the information flow control policy [FMT_MSA.3(NI), FMT_MTD.1(NI)]; • the auditing aspects [FMT_MTD.1(AE), FMT_MTD.1(AS), FMT_MTD.1(AT), FMT_MTD.1(AF)]; • the identification and authentication aspects [FMT_MTD.1(IAT), FMT_MTD.1(IAF), FMT_MTD.1(IAU)]. Persistently stored user data is stored either in hierarchical or relational fashion, which implies an inheritance of security attributes from parent object [FMT_MSA.4(PSO)]. The rights management for the different management aspects is defined with [FMT_SMR.1]. The management interfaces for the revocation of user and object attributes is provided with [FMT_REV.1(obj) and FMT_REV.1(USR)].

Objectives	Coverage Rationale
O.TRUSTED_CHANNEL	The TOE provides a trusted channel protecting communication between a remote trusted IT system and itself [FTP_ITC.1].

Table 7: Security Functional Requirements rationale

8.3.3 Security Requirements Dependency Analysis

SFR	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes: FAU_GEN.1 Yes: FIA_UID.1
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes: FAU_GEN.1 Yes: FMT_MTD.1(AE)
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3	FAU_STG.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_CKM.1(SYM)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Yes: FCS_COP.1(NET) Yes: FCS_CKM.4
FCS_CKM.1(RSA)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Yes: FCS_COP.1(NET) Yes: FCS_CKM.4
FCS_CKM.1(DSA)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Yes: FCS_COP.1(NET) Yes: FCS_CKM.4
FCS_CKM.2(NET)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Yes: FCS_CKM.1(SYM), FCS_CKM.1(RSA), FCS_CKM.1(DSA) Yes: FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes: FCS_CKM.1(SYM)
FCS_COP.1(NET)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Yes: FCS_CKM.1(SYM), FCS_CKM.1(RSA), FCS_CKM.1(DSA) Yes: FCS_CKM.4
FDP_ACC.1(PSO)	FDP_ACF.1	Yes: FDP_ACF.1(PSO)

SFR	Dependencies	Resolved
FDP_ACC.1(TSO)	FDP_ACF.1	Yes: FDP_ACF.1(TSO)
FDP_ACF.1(PSO)	FDP_ACC.1 FMT_MSA.3	Yes: FDP_ACC.1(PSO) Yes: FMT_MSA.3(PSO)
FDP_ACF.1(TSO)	FDP_ACC.1 FMT_MSA.3	Yes: FDP_ACC.1(TSO) Yes: FMT_MSA.3(TSO)
FDP_IFC.2(NI)	FDP_IFF.1	Yes: FDP_IFF.1(NI)
FDP_IFF.1(NI)	FDP_IFC.1 FMT_MSA.3	Yes: FDP_IFC.2(NI) Yes: FMT_MSA.3(NI)
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	Yes: FDP_ACC.1(PSO), FDP_ACC.1(TSO), FDP_IFC.2(NI) Yes: FTP_ITC.1 Yes: FPT_TDC.1
FDP_RIP.2	N/A	Yes
FDP_RIP.3	N/A	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1(HU)	N/A	Yes
FIA_ATD.1(TU)	N/A	Yes
FIA_SOS.1	N/A	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.5	N/A	Yes
FIA_UAU.7	FIA_UAU.1	Yes
FIA_UID.1	N/A	Yes
FIA_USB.2	FIA_ATD.1	Yes: FIA_ATD.1(HU)
FMT_MSA.1(PSO)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes: FDP_ACC.1(PSO) Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MSA.1(TSO)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes: FDP_ACC.1(TSO) Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MSA.3(PSO)	FMT_MSA.1 FMT_SMR.1	Yes: FMT_MSA.1(PSO) Yes: FMT_SMR.1
FMT_MSA.3(TSO)	FMT_MSA.1	Yes: FMT_MSA.1(TSO)

SFR	Dependencies	Resolved
	FMT_SMR.1	Yes: FMT_SMR.1
FMT_MSA.3(NI)	FMT_MSA.1 FMT_SMR.1	NO, but satisfied with FMT_MTD.1(NI) Yes: FMT_SMR.1
FMT_MSA.4(PSO)	[FDP_ACC.1 or FDP_IFC.1]	Yes: FDP_ACC.1(PSO)
FMT_MTD.1(AE)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(AS)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(AT)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(AF)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(NI)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(IAT)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(IAF)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MTD.1(IAU)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_REV.1(OBJ)	FMT_SMR.1	Yes
FMT_REV.1(USR)	FMT_SMR.1	Yes
FMT_SMF.1	N/A	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	N/A	Yes
FPT_TDC.1	N/A	Yes
FTA_SSL.1	FIA_UAU.1	Yes
FTA_SSL.2	FIA_UAU.1	Yes
FTP_ITC.1	N/A	Yes

Table 8: Security Functional Requirements dependency analysis

The dependencies for security assurance requirements are all fulfilled based on the following facts:

- EAL4 is completely self-sufficient with all dependencies being fulfilled with the package of EAL4.
- The security assurance requirement of ALC_FLR.3 which is in addition to EAL4 does not have any dependencies.
- The refinement of ASE_CCL.1 does not introduce any dependencies.

Rationale for unresolved dependencies:

- FMT_MSA.3(NI): FMT_MTD.1(NI) is specified to require the management of security attributes for the Network Information Flow Control Policy, just as a potential FMT_MSA.1(NI) would have been specified. However, the Network Information Flow Control Policy is not required to be enforced when managing the security attributes, as the management aspect of the network information flow control functionality is not protected by the network information flow control mechanism. Therefore, FMT_MSA.1 is not applicable and is replaced with FMT_MTD.1(NI).

8.4 Security Assurance Requirements

The Protection Profile includes all Security Assurance Requirements specified in CC Part 3 based on the EAL defined in section 4.2 considering the following refinements.

8.4.1 ASE_CCL.1 refinement

ASE_CCL.1 specified in CC Part 3 is refined as follows: All Developer Action Elements, Content and Presentation Elements, Evaluator Action Elements remain unaltered, except the following:

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs ***including the statements marked as "ST-Author Note" and the specification given in section 8.1 of the OSPP base*** for which conformance is being claimed.

8.5 Rationale for Security Assurance Requirements

The target evaluation assurance level for products complying with this Protection Profile is specified in section 4.2. This Protection Profile is intended for general-purpose, commercial-off-the-shelf operating systems, which are generally seen as appropriate for a controlled environment where attackers have an enhanced-basic attack potential. In addition, due to operating systems being complex systems which are the basis for almost all applications in todays IT environments, this protection profile requires the inclusion of ALC_FLR.3 mandating the developer to provide security-relevant patches in due time after the identification of a flaw.

The augmentation of ASE_CCL.1.10C is considered to include certain requirements of this Protection Profile with which the ST author must comply. These requirements specify conditional requirements that only apply when the TOE shows special properties or mechanisms. The [CC] does not define such conditional statements, which are therefore introduced by this Protection Profile.

9 Abbreviations

Abbreviation	Description
AH	Authentication Header
CC	Common Criteria
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPSEC	IP Security Protocol
MAC	Mandatory Access Control
OSPP	Operating System Protection Profile
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE security function
TSFI	TSF Interface
TSP	TOE security policy