General-Purpose Operating System Protection Profile

A joint effort by NIAP and BSI for the development of a Common Criteria Protection Profile

Version 3.9

Part1: General Model, Security Problem Definition, Security Functional Requirements and Security Assurance Requirements

Table of contents

Index of Tables

Illustration Index

Revision History

Version	Date	Author	Changes
3.0	2012-03-15	Helmut Kurth, atsec	Changes due to harmonization effort
3.1	2012-03-21	Helmut Kurth, atsec	Addressing comments from BSI
3.2	2012-04-11	Helmut Kurth, atsec	Addressing additional comments from Microsoft and from the last Telco
3.3	2012-04-16	Helmut Kurth, atsec	Addressing additional comments
3.3a	2012-05-05	Helmut Kurth, atsec	Completing to address contract with BSI
3.3b	2012-07-17	Helmut Kurth, atsec	Update of the SFR from comments received
3.4	2012-08-03	Helmut Kurth, atsec	Updates from comments received. First version for distribution to a larger community
3.5	2012-08-07	Helmut Kurth, atsec	Last updates before distribution
3.6	2012-08-17	OSPP TC	Final updates
3.7	2012-09-07	OSPP TC	Minor change on FTP_ITC.1
3.8	2012-12-03	Gerald Krummeck, atsec	Added assurance requirements as agreed by OSPP TC; added rationale for unresolved dependencies Updated wording on future extended packages
3.9	2012-03-06	OSPP TC	Final changes for publication: • mark PP as DRAFT • refer to CC V3.1 R4 • FIA_X509_EXT changed to FIA_PK_EXT to allow for public keys (SSH) in addition to X.509 certificates • FTP_ITC.1: Re-arranged list of mandatory and optional cipher suites • minor editorial changes

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. It also provides a set of assurance components that define the minimum set to be used in an evaluation of an operating system for compliance with this Protection Profile. Part 2 of this PP defines the general approach and assurance activities required to be performed during the evaluation, thereby refining the stated assurance components.

Unlike most other Protection Profiles, the General-Purpose 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. In this draft of the harmonized OSPP, extended packages are not yet available.

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.

The security functional requirements specified in this "base" document specify functions that the operating system needs to provide without online support from other IT systems in its environment. Functions that rely on support of the operational environment will be left to extended packages or ST specific extensions.

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: General-Purpose Operating System Protection Profile

PP Version: 3.9

Publication Date: 2012-12-06

Author: OSPP Technical Community

CC-Version: 3.1 Revision 4

Keywords: operating system, general-purpose operating system

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 and rationale.

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 General-Purpose 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.

Note that the requirements specified in this base Protection Profile apply for locally defined users. Therefore an operating system compliant with this Protection Profile **must** have the capability for defining and managing users locally without support of the TOE environment. The operating system **may** also have the capability to deal with remotely defined and managed users, which then have to be expressed in additional SFRs included in the Security Target or by claiming compliance to an extended package that defines such functionality.

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, September 2012, Version 3.1 Revision 4

CEM Common Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4

OSPP-2 General-Purpose Operating System Protection Profile. Part2: General Approach and Assurance Activities for OSPP Evaluations, Version 3.9.

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, security functional requirements, and security assurance requirements that are to be satisfied by every general-purpose operating system claiming conformance to the OSPP base. 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. OSPP extended packages need to be approved by the OSPP Technical Community or at least by the scheme where the extended package is used.

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 is 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 (strict)
- Conformance claim to the security assurance requirements 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 (called "remote IT entity" in this Protection Profile).
- 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. They may alternatively be transmitted to a trusted centralized audit server, but the operating system must support local audit storage in the case the user does not configure a centralized audit storage or such centralized audit storage becomes unavailable. 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 local 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 User data protection

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

3.1.2.1 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 3.1.3.

A single operating system may well implement different discretionary access control policies for different types of subjects or objects and this should not be a problem as long as all of those access control policies satisfy the basic requirement of being able to specify access rights down to the granularity of a single user and as long as the sum of all those access control policies covers all types of subjects and objects.

A full specification of a discretionary access control policy needs to include:

- The type(s) of objects covered by the policy
- The type(s) of subjects/users covered by the policy
- The operations covered by the policy
- The rules that are used to determine if a specific subject/user is allowed to perform an operation covered by the access control policy on a specific object, including the subjects/user security attributes, the object security attributes and any other TSF data used in those rules

In addition the following aspects need to be covered:

- The rules that determine if an object can be created
- The rules that determine the default security attributes of the object used in the discretionary access control policy
- The rules that determine when a user is allowed to add/modify/delete an access right
- The rules that determine when a user is allowed to modify/add/delete an object security attribute used in the policy
- The rules that determine when a user is allowed to delete an object

Access control policies have to exist for all types of objects that may be used by users to share data. This includes persistent objects (e. g. files) as well as temporary objects (e. g. shared memory). The intention is that an operating system compliant with this Protection Profile allows users to operate in isolation from other regular users (i. e. to not share data with any other non-administrative user of the operating system) as well as the capability to define sharing down to the granularity of a single user. To achieve this goal, there must be at least one discretionary access control policy for at least one type of persistent objects that allows for the definition of access rights down to the granularity of a single user. Note that not all discretionary access control policies are required to provide this level of granularity.

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 including - if applicable - the rules defining how those default access rights can be managed.

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.

3.1.2.2 Network information flow control

The TOE shall allow filtering of network data sent by an external entity to the TOE or network data generated by a subject within the TOE to be sent to an external entity 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 3.1.5.1. For TCP/IP based filtering, the OSPP allows the ST author to define whether stateless and/or stateful packet filtering is supported. Those filtering rules are defined as an information flow policy, since the filter rules specify the conditions that need to be satisfied to allow network data to flow from a network interface to its target "consumer" in the TOE.

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.

3.1.3 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. An operating system compliant with this Protection Profile must support user ID/password for human users, as well as authentication based on cryptographic tokens for remote IT entities that want to establish a trusted channel. The authentication method using cryptographic tokens are defined by the network protocol and a TOE compliant with this Protection Profile must support at least one the protocols SSH, TLS, or IPSec (with certificate based authentication).

A TOE compliant with this protection Profile may support additional authentication methods for human and remote IT entities, which then need to be defined in the Security Target together with the management functionality required to manage the authentication method.

After successful identification and authentication of a human user, 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. If the operating system allows for other IT systems to have subjects started on their behalf and if the user-subject binding process is different for this case, the Security Target needs to include a second instantiation of the user-subject-binding security functional requirement specifying the rules how the subject security attributes are derived for such subjects.

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. The access control policy must be capable of restricting the operations allowed for unauthenticated users to such "public" operations that do not modify the object.

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. This would be a functionality beyond what is specified in this base Protection Profile and would require additional SFRs that define such functionality.

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 (for human users)
- Software token-based authentication (for remote IT entities that want to set up a trusted channel)

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.

3.1.4 Management of security mechanisms

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

If in addition 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. Note that this would be an optional functionality that needs to be defined using additional SFRs not included in this base Protection Profile.

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.

3.1.5 Trusted channel

In order to support remote management, the OSPP requires that an operating system has the capability to establish a trusted channel to a trusted remote entity. Remote management activities shall require such a trusted channel, which also needs to use public key based authentication of the remote entity.

In addition, 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.

3.1.5.1 Cryptographically-protected network protocols

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 not allowed)
- 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.

For more details see the section on trusted channels above.

In addition a TOE may implement generic cryptographic services it may make directly available to users or subjects. Those services are not addressed by this base Protection Profile, but may be specified as additional SFRs in a Security Target. It is also intended to specify basic requirements for a cryptographic service provider in an extended package.

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.

3.2 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. Still, as mentioned above, an Operating System conformant to the OSPP base **must** implement functionality that satisfies the SFRs listed in the OSPP base locally, i. e. without support by the IT environment. As an example, an operating system that wants to claim compliance to the OSPP base may of course offer identification and authentication services or user management that rely on an external directory server as an option, but it must also support local user authentication and user management.

In cases where the operating system provides functionality that uses support from the IT environment, it is still required that the operating system must provide the interfaces for the security functionality claimed to users and subjects, and 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 allows the optional use of 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).

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.

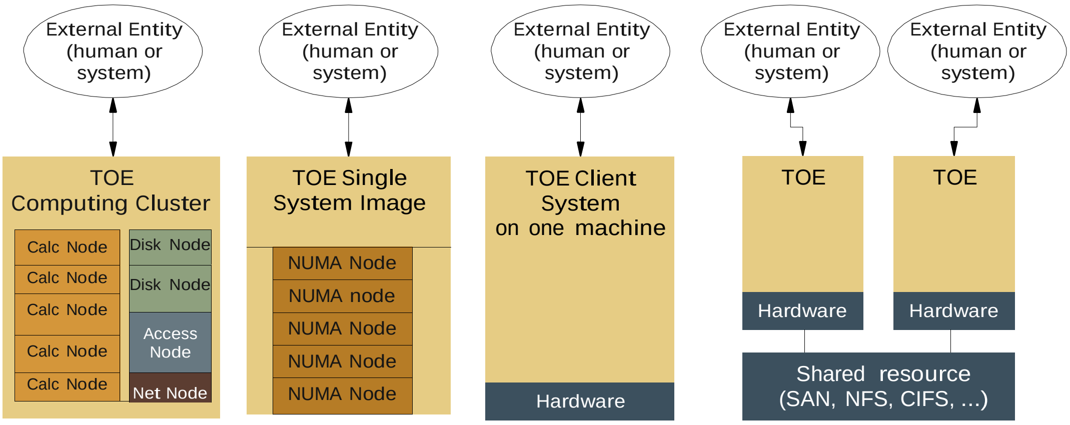
External Entity (human or system)
External Entity (human or system)
External Entity (human or system)
External Entity (human or system)
External Entity (human or system)
TOE Computing Cluster
Calc Node
Calc Node
Calc Node
Calc Node
Calc Node
Disk Node
Disk Node
Access Node
Net Node
TOE Single System Image
NUMA Node
NUMA node
NUMA Node
NUMA Node
NUMA Node
TOE Client System on one machine
Hardware
TOE
TOE
Hardware
Hardware
Shared resource (SAN, NFS, CIFS, ...)

Illustration 1: Types of TOE instances and their boundaries

4 Conformance Claims

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

4.1 Conformance with CC parts 2 and 3

OSPP is CC version 3.1 revision 4 Part 2 extended and Part 3 conformant.

4.2 Conformance with other Protection Profiles

OSPP does not claim conformance to any other Protection Profile.

4.3 Conformance Statement

OSPP requires strict 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 strict 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.

4.4 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 strict 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:

- 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
- 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 may read or modify TSF data using functions of the TOE without the necessary authorization.

T.ACCESS.USERDATA A threat agent may gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy by using functions provided by the TOE.

T.ACCESS.TSFFUNC A threat agent may use or manage functionality of the TSF bypassing protection mechanisms of the TSF.

T.ACCESS.COMM A threat agent may access cryptographically protected data transferred via a trusted channel between the TOE and another remote trusted IT system, modify such data during transfer in a way not detectable by the receiving party or masquerade as a remote trusted IT system.

T.RESTRICT.NETTRAFFIC A threat agent may send data packets to the recipient in the TOE via a network communication channel in violation of the information flow control policy.

T.IA.MASQUERADE A threat agent may 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 may gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated by the TSF.

T.UNATTENDED_SESSION A threat agent may gain unauthorized access to an unattended session.

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.

P.ROLES Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has.

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 General-Purpose 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.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 network communication between an entity outside of the TOE and a recipient within the TOE in accordance with its network information flow security policy.

O.SUBJECT.COM The TOE shall mediate any possible sharing of objects or resources between subjects acting with different subject security attributes in accordance with its discretionary access control policy.

O.I&A The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to be provided 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, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.

O.TRUSTED_CHANNEL 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. The protocol must also prevent masquerading of the remote trusted IT system.

O.UNATTENDED_SESSION The TOE must allow for the temporary suspension of a user's session allowing the continuation of such a suspended session and user related input and output only after the user has resumed the session by re-authenticating himself to the TSF.

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.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.USERDATA, T.ACCESS.TSFDATA, T.ACCESS.TSFFUNC, T.ACCESS.COMM
O.UNATTENDED_SESSION	T.UNATTENDED_SESSION

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 mitigated by: □ O.TRUSTED_CHANNEL 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 mitigated by: □ O.TRUSTED_CHANNEL 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 mitigated by: □ O.TRUSTED_CHANNEL requiring cryptographically-protected 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 mitigated 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

Threats	Security Objectives
	other recipients via network communication channels without authorization for this communication attempt is mitigated 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 mitigated 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 mitigated 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.
T.UNATTENDED_SESSION	The threat of an attack agent using an unattended session to gain access to protected functionality of the TSF, user data, or TSF data is mitigated: □ O.UNATTENDED_SESSION requiring the capability that unattended sessions can be protected from use by unauthorized persons.

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 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

Assumptions	Security Objectives
	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: □ 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 FIA_PK_EXT.1 Public key based authentication

FIA_PK_EXT.1 is a SFR related to public key cryptography used for authentication of remote IT systems.

7.1.1 Component leveling

FIA_PK_EXT.1 is not hierarchical to any other component of part2 of [CC].

7.1.2 Management

Management of keys or certificates needs to be addressed by an instantiation of FMT_MTD.1.

7.1.3 Audit

There are no audit requirement for FIA_PK_EXT.1.

7.1.4 FIA_PK_EXT.1 Public key based authentication

Hierarchical to: None
Dependencies: FMT_MTD.1 Management of TSF data

FIA_PK_EXT.1.1 The TSF shall use [selection: [assignment: certificate format standard], public key cryptography] as defined by [assignment: certificate management and certificate validation standards or other method for key management/key validation] to support authentication for [assignment: cryptographic protocol] connections.

FIA_PK_EXT.1.2 The TSF shall store and protect certificates and/or public keys from unauthorized deletion and modification.

7.1.5 Rationale

Remote IT entities are often authenticated based on public key cryptography. This SFR specifies the method used for public key based authentication and the cryptographic protocols that perform public key based authentication. If digital certificates are used it also defines the standard used for certificate path validation. Note: the use of public key based authentication must be compliant with the definition of the use of public key based authentication in the cryptographic protocol selected.

7.2 FMT_SMF_RMT.1 Remote Management Capabilities

FMT_SMF_RMT.1 is a SFR related to remote management.

7.2.1 Component leveling

FMT_SMF_RMT.1 is not hierarchical to any other component of part2 of [CC].

7.2.2 Management

No requirement

7.2.3 Audit

There are no specific audit requirement for FMT_SMF_RMT.1.

7.2.4 FMT_SMF_RMT.1 Remote Management Capabilities

Hierarchical to: None
Dependencies: FTP_ITC.1 Inter-TSF Trusted Channel
FMT_SMF_RMT.1.1 The TSF shall allow management functions also to be performed from a remote IT entity using a trusted channel established in accordance with the requirements stated in FTP_ITC.1.

7.2.5 Rationale

Remote management capabilities using a trusted channel are required for general-purpose operating systems. Administrators using this capability need to be authenticated, which can either be done by requesting them to provide valid authentication information in the same way as for local user authentication or by certificates that are unambiguously bound to the administrative user.

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 Functional Requirements

8.1.1 Class: Security Audit (FAU)

8.1.1.1 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 **not specified** 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) **other specifically defined auditable events as defined in the table in FAU_GEN.1.2.**

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 (success or failure) of the event; and

b) **for all management SFRs included in the Security Target: the identity of the user that performed/attempted to perform the management operation, an identification of what was managed and the indication what the administrative user has changed as part of the management operation, and**

c) For each audit event type, based on the auditable event definitions of the functional components included in the *following table:*

SFR	**Events and Event specific information**
FAU_SAR.1	Event: Any attempt to access the audit records - identity of the user attempting to access the audit records - success or failure
FAU_SEL.1	Event: Any attempt to modify the events to be audited - identity of the user attempting to modify the events to be audited - success or failure - in case of success: modification to the set of events to be audited
FDP_ACF.1	Event: Any attempt to access an object protected by the SFP - identity of the user attempting to access an object protected by the SFP. Note: if the operation is attempted by a subject not operating on behalf of a user: identity of the subject - identity of the object the user attempts to access - attempted operation - Success or failure
FDP_IFF.1	Event: Denied information flow - identification of the network interface - reason for denying information flow
FIA_AFL.1	Event: Exceeding the limit of unsuccessful consecutive authentication attempts

SFR	Events and Event specific information
	- user identity where the limit was exceeded
FIA_UAU.1(HU)	Event: Verification that a user has been successfully authenticated - user identity - indicator that the user has been successfully authenticated In the case the authentication is performed by the TOE, also the event of a failed authentication attempt needs to be auditable: - user identity provided - indicator that the authentication failed
FTA_SSL.1	Event: Re-authentication attempt to unlock a session - user identity - success or failure of re-authentication
FTA_SSL.2	Event: Re-authentication attempt to unlock a session - user identity - success or failure of re-authentication
FTP_ITC.1	Event: Initialization of a trusted channel - identity of the communication partner - protocol used to establish the channel - success or failure of setting up the channel

Table 6: Minimum set of auditable events with event specific information

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.

Application Note: The table defined in FAU_GEN.1.2 above defines a minimum set of events an operating system compliant to this Protection Profile must be able to audit, together with the minimum amount of information that needs to be contained in the audit record in addition to the general information of time and date, event type. The event specific information often refines the requirements for "subject identity" and "outcome of the event". For example if the event specific information in an entry in the table specifies the "identity of the user", there is no need to also record a subject identity in addition to this 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 the access control decision functionality 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.

Application Note: A Security Target that includes additional SFRs e. g. for additional management activities needs to specify the audit requirements for such an additional SFR in an extension to the table above in the Security Target. As a general rule for all management activities initiated by an administrative user, the event specific information needs to contain the identity of the user that performed/attempted to perform the management operation, an identification of what was managed and the indication what the administrative user has changed as part of the management operation. Operations where an administrative user just queries the status of manageable items do not need to be auditable.

8.1.1.2 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.

8.1.1.3 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 perform the activity]]** 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.

8.1.1.4 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.

8.1.1.5 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;**

b) **Subject or user identity;**
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].**

8.1.1.6 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.

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

8.1.1.8 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 **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to perform the activity]]**”, “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.

8.1.2 Class: User Data Protection (FDP)

8.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on

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

b) **[assignment: list of types of named Objects covered by the SFP**:

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

ST Author Note: An operating system may implement multiple access control SFPs and the intention here is to allow for multiple instantiations of FDP_ACC.1, FDP_ACF.1 and associated management SFRs to describe each access control SFP in terms of the types of users/subjects, types of objects, and operations covered by the SFP with the related instantiation of FDP_ACF.1 describing precisely the rules that are followed in order to determine if a specific user/subject is allowed to perform a specific operation on a specific object covered by the SFP.

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.

8.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects *or users* 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/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].

Application Note: There must be at least one access control SFP for persistent storage objects (e. g. files) that allows for the specification of access rights down to the granularity of a single user/subject. Access control lists that allow for specifying access right for individual users while by default denying access to user or groups that are not part of an entry in the access control list is an example of an implementation that would satisfy this condition. An additional capability to assign access to groups or bind access to privileges which themselves can be assigned individually to users/subjects and/or groups does not violate the condition of being able to assign access down to the level of a single user.

ST Author Note: Access control policies can be highly complex and an operating system may implement a large number of "exceptions" e. g. by binding some access rights to specific privileges. In order to avoid the overall rule set to become overly complex the ST author may decide to describe not all those exceptions. This is allowed provided that the guidance for the evaluated configuration clearly describes how to configure and manage the TOE such that those exceptions are not relevant for the evaluated configuration. For example an access right automatically given to a user with a specific privilege may be ignored in the description of the access control rules provided the guidance clearly states that this privilege shall not be assigned to a user when operating in the evaluated configuration.

ST Author Note: The ST has to repeat FDP_ACF.1 for each instance of FDP_ACC.1 with FDP_ACF.1 describing the relevant security attributes used in the rules that determine access as well as the rules that determine access themselves. The description provided must allow the reader/evaluator to identify the TSF data that is used in making the access decision as well as derive a model of the access decision process. The identification of the TSF data used in the access decision rules is required since the evaluator needs to determine how this TSF data is derived and managed in order to identify possible ways an attacker may influence the access control decision by influencing the TSF data used in the decision process.

8.1.2.3 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Network Information Flow Control Policy** on

a) **Originating entities:**
   i. **unauthenticated external IT entities that send network data to a network interface of the TOE;**
   ii. **subjects within the TOE that send network data to unauthenticated external IT entities via a network interface of the TOE;**

b) **Information:**
   i. **Network data received by the TOE from an external IT entity;**
   ii. **Network data provided to the TOE by a subject executing on the TOE intended to be sent to an external IT entity via a network interface controlled by the TOE;**
   iii. **[selection: [assignment: other information covered by the SFP], none];**

c) **Operations:**
   i. **Receiving network data from an unauthenticated external IT entity;**

   ii. **Sending network data to an unauthenticated IT entity by a subject within the TOE;**

Application Note: This SFR together with FDP_IFF.1 requires the TOE to implement the capability to define basic packet filtering rules for both incoming and outgoing network packets. The requirement is as a minimum to have filtering capabilities for TCP/IP, VLANs or both where an administrator can define rules for inspecting packets and then deciding if a packet is allowed to be sent to the intended recipient or discarded.

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.

8.1.2.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Network Information Flow Control Policy** based on the following types of subject and information security attributes:
Object security attribute: the logical or physical network interface through which the network data from an external IT entity entered the TOE or is intended to be sent out;
[selection (of either a or b or both):

a) **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 IP, TCP, UDP, [selection: ICMP, [assignment: other protocols]],**
   v. **[selection: TCP header flags of [selection: SYN, ACk, [assignment: other TCP header flags]], [assignment: other network data information security attributes], no other security attributes];**

b) **Layer 2 security attributes**
   i. **MAC address;**
   ii. **VLAN identifier,**
   iii. **[selection: [assignment: other network data information security attributes], no other security attributes]**

].

Application Note: A TOE compliant to this Protection Profile does not need to allow for different rule sets applicable to different network interfaces, but in case it provides this capability the network interface the data has been received or is intended to be sent out needs to be considered by the TOE as a security attribute used to select the correct set of rules that needs to be applied.

Application Note: The minimum requirement of the network flow control specified in FDP_IFF.1.3 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.

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:

for both receiving network data from an external IT entity and sending network data by a subject within the TOE to an external IT entity:

a) **if the set of rules defined in accordance with the security attributes defined in FDP_IFF.1.3 define that the network data is discarded the network data shall not be delivered by the TOE to the intended recipient;**

b) if the set of rules defined in accordance with the security attributes defined in FDP_IFF.1.3 define that the network data is to be delivered unaltered the network data shall be delivered unaltered by the TOE to the intended recipient;

c) **if the set of rules defined in accordance with the security attributes defined in FDP_IFF.1.3 define another action to be taken than discarding the network data or delivering the data unaltered to the intended recipient, the TOE shall perform this action**.

Application Note: For network data received from an external IT entity the "intended recipient" is the process within the TOE the network data is supposed to be delivered to for further processing. This may be a subject operating on behalf of a user, another subject (e. g. a network daemon) or a dedicated part of the TSF.
For network data generated within the TOE that is intended to be sent to a remote IT entity the "intended recipient" is the remote IT entity identified by either the IP address or the MAC address as specified in the network data before it is processed by the filtering rules.

FDP_IFF.1.3 The TSF shall enforce the **following rules consisting of an identification when the rule fires and an action to be taken when the rule fires: Identification of network data using one or more of the following concepts:** a)
Information security attribute matching based on the following security attributes [assignment: list of security attributes used in the matching rules];

b) **[selection: [assignment: matching rules based on the state of a TCP connection], [assignment: time-based matching rules], [assignment: statistical analysis matching rules]], [selection: no other matching concepts, [assignment: other matching concepts]];**

Performing one or more of the following actions:

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

b) **Allow the network data to be delivered unaltered by the TOE to the intended recipient;**

c) **[selection: and perform no other action, [assignment: other actions that are performed when the rule fires]].**

ST author note: FDP_IFF.1.3 a) requires the ST author to define those security attributes in the network protocol that are used in the rules for simple matching (i. e. where a simple comparison with the value of the security attribute decides if the network package is allowed to pass or is not allowed to pass. FDP_IFF.1.3 b) requires the TOE to have at least one more complex set of rules are either based on the state of TCP connections, based on time or based on some statistical properties (e. g. too many network packages of the same kind coming from specific sources). The ST author may specify in FDP_IFF.1.3 the rules for at least one of those concepts, explaining which matching concept he uses and shall also specify other matching concepts implemented by the TOE that are used to decide if a network package is allowed to pass or not. Specifying the complete set of rules is important to determine the expected results for tests at the network interfaces and compare those with the real results obtained. The ST author then needs to specify the possible actions that can be taken when the rules "fire", which must at least allow for discarding the network data or passing the network data unaltered.

ST author note: An example of another action that may be specified is the logging of actions performed potentially including network data discarded. If this is defined as an action, the list of events to be audited in FAU_GEN.1 needs to be extended. In cases where this network filtering related logging is not performed using the audit mechanisms for other auditable events, the ST author needs to describe how the full set of audit related SFRs is addressed by the TOE for the network filtering related auditing functionality.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, 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, 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.

8.1.2.5 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, *subjects or subject/object related TSF data before the resource is assigned or made available to another subject or user.*

Application Note: The purpose of this SFR is to ensure that an untrusted subject or user is not able to obtain TSF or user data from a resource that has been previously assigned to another subject. This includes of course disk space previously allocated to a file belonging to another user, main memory previously allocated to a subject operating on behalf of another user, but also registers after a context switch from a process belonging to a subject operating on behalf of another user, or TSF internal memory previously used for storing information that requires protection against disclosure.

Note that resources re-assigned to the same subject/user or the same object do not require preparation for re-use, since the information they contain had anyhow been accessible to the subject or user before it was released.

8.1.3 Class: Identification and Authentication (FIA)

The TOE must support different types of identification and authentication schemes for human users (administrators and untrusted users) and IT entities in the course of its operation. Some of the requirements that might normally be considered part of the I&A process are specified in other sections of this PP, particularly those related to cryptographic protocols called out in FTP_ITC.1 Inter-TSF trusted channel. So, for IT entity authentication, where the authentication is solely at a machine level, the authentication is performed using a cryptographic protocol using X.509v3 certificates. This was done to keep I&A requirements on IT entities grouped with the identified protocols and their respective RFCs grouped together for understandability (FPT_ITC.1).

The requirements in this section cover the following distinct aspects of the I&A capabilities of conformant TOEs:

- I&A for the human user. The TOE must provide a password mechanism that may be used by users connecting the TOE locally (e.g., console), or when the user is connecting to the TOE remotely (e.g., trusted channel via an IT entity). It is required that every user is authenticated using at least one of the user authentication mechanisms the ST author defines in FIA_UAU.5.
- Credentials. The protocols (FTP_ITC.1) and mechanisms (FIA_UAU.5) specified in this and other sections of the PP rely on different credentials that are used in the I&A process: passwords or optional other user authentication mechanisms listed in FIA_UAU.5 for users, and certificates for IT entities connecting to the TOE using a trusted channel and one of the protocols listed in FTP_ITC.1 (IPsec, TLS, SSH)).

8.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator-configurable positive integer within a range of acceptable values of** unsuccessful authentication attempts *for the authentication method password based authentication [assignment: other authentication method or none]* occur related to [assignment: list of authentication events].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, 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.

Application Note: The unsuccessful authentication attempts need not be consecutive, but rather related to an authentication event. Such an authentication event could be the count from the last successful session establishment at a given terminal.

Application Note: Although the list of actions can be TOE specific, the set of actions needs to ensure that any subsequent authentication attempts will prevent an attack based on semi-exhaustive searches through the space of possible authentication data. For example an action that limits the number of unsuccessful additional authentication attempts to one per day would be acceptable while an action that just modifies an optional audit of unsuccessful authentication attempts into a mandatory audit would not be acceptable.

Application Note: The first assignment in FIA_AFL.1.1 is straightforward and simply requires the ST Author to list any authentication methods that may be employed that are subject to some form of failure handling. The second assignment relates to how the authentication failure attempts are measured, and may be different depending on the authentication method. This is true for the selection and assignment in FIA_AFL.1.2 as well – there may be different actions taken based upon the authentication method. For example, for a user locally entering a password at the console and failing three times, may result in the account being locked, whereas a user remotely entering a password and failing three times, may simply result in the remote session being terminated. The action taken may be different for untrusted users versus administrative users. All these examples are acceptable, what is important is that the requirement is clear as to what authentication methods are covered, under what circumstances an action will result, and what the resulting action will be.

8.1.3.2 FIA_ATD.1 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) **Security roles;**
e) **[assignment: other user security attributes].**

ST Author Note: Note that the user security attributes listed above need to be maintained by the TOE itself to allow the TOE to enforce its SFRs even in the case when supporting trusted systems in the TOE environment are not available. This does not prohibit a TOE that operates in an environment where support of other trusted IT systems is available to use such support.

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 expressing clearly which security attribute is held where.

8.1.3.3 FIA_UAU.1(RITE) Timing of authentication

FIA_UAU.1.1 The TSF shall allow

a) **the information flow covered by the Network Information Flow Control Policy (for remote IT entities);**
b) **[assignment: list of TSF other mediated actions]**

on behalf of the remote IT entity to be performed before the remote IT entity is authenticated.

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

Application Note: This element applies to network traffic sent by remote IT entities and processed by the TOE. Some network traffic sent by remote IT entities is used to set up a communications channel that is subsequently used for authenticating the remote IT entity. The FTP_ITC.1.3 element is where the ST author specifies which conditions (actions performed using the trusted channel) require the remote IT entity to be authenticated. Additionally, remote IT entities may send traffic that does not require authentication as allowed by the Network Information Flow Control Policy described in the FDP_IF* components. Both of these cases are covered under the “a” portion of the FIA_UAU.1.1 element. There may be other actions that the TOE takes with respect to remote IT entities that are not covered by the FDP_IF* requirements as they are specified in the ST; in these cases, the ST author uses the assignment to specify these capabilities.

8.1.3.4 FIA_UAU.1 (HU) Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] 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.

8.1.3.5 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 (for human users);**

b) **[selection: [assignment: list of other authentication mechanisms], none]**

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 with credentials stored by the TSF by default unless another authentication method defined for human users in FIA_UAU.5.1 b is selected;**

b) **Users with expired passwords are [selection: required to create a new password after correctly entering the expired password, locked out until their password is reset by an administrator];**

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

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.

8.1.3.6 FIA_UAU.7 Protected authentication feedback

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

Application Note: Note that "no feedback" is viewed as a specific (stronger) method of providing "obscured feedback".

8.1.3.7 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.

8.1.3.8 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following security attributes with subjects acting on the behalf of that *human* user:

a) **The user identity;**

b) **[assignment: list of security attributes used to enforce the access control policies, enforce the management policies, or used to satisfy auditing requirements];**

Application Note: Throughout the SFR FIA_USB.1 the term "user security attribute" has been refined to "security attribute" since operating systems may assign security attributes to a subject that are not derived from security attributes of the user the subject is bound to.

Application Note: Roles, groups and privileges also need to be assigned to the subject as long as they are used to enforce any SFR mentioned in the Security Target. A TOE may allow for the definition of roles as a set of privileges that can be assigned to a user but during user-subject binding the TOE may resolve those roles into the privileges that define the role and assign the individual privileges. In this case the "roles" themselves are no longer visible when the subject is executing. For simplification purpose it is still valid to state in a Security Target the set of security attributes as a "role" assigned to the subject rather than listing the individual privileges that define the role. This is required for cases where the set of privileges that define a role can be managed.

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

Application Note: The rules shall define how the TSF identifies and selects the subject's security attributes upon user-subject binding. In many cases the subject will just inherit user security attributes from a user's profile. For some security attributes, the TSF may decide based on specific rules if the user security attribute is included in the subject's security attributes (e. g. a TOE may allow a user to select his active role(s) from the list of overall roles he has). Other subject security attributes derived from user security attributes may be determined by the TSF based on other TSF data. For example the TSF may assign a specific critical management privilege to a subject only if the user has this privilege assigned and the user connects to the TOE via a specific connection like a local console. While a TOE compliant to this Protection Profile is not required to implement such complicated rules, they need to be specified precisely if he does.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

Application Note: Changes to a subject's security attributes may be allowed by explicit user or administrator action or may happen automatically as the result of specific activities. For example in Unix-type systems the effective user- and group-ID may change as the result of invoking programs with specific attributes. This part of the SFR is intended to define such rules.

ST author note: The SFR above applies to "human" users, not necessarily remote IT entities. Many operating systems implement subjects that are not directly bound to a 'human" user but in order to avoid having to implement two different ways of user-subject binding, they have a mechanisms that allows the definition of "pseudo-users", which are protected from being used by a human user (they do not have authentication information associated with them) but can only be used by the TSF. The TSF may start specific subjects and "bind" those to the security attributes defined for "pseudo-users". Daemons in Unix are a typical example for such subjects. A TOE that implements such a concept has to include an instantiation of FIA_USB.1 that describes the rules of such a user-subject binding process (in case they differ from the ones defined for "human" users).

8.1.3.9 FIA_PK_EXT.1 Public key based authentication

FIA_PK_EXT.1.1 The TSF shall use **[selection: X.509v3 certificates, public key cryptography]** as defined by **[assignment: RFC5280 or other method for key management/key validation if no X.509v3 certificates are used]** to support authentication for **[selection: IPSec, TLS, SSH]** connections.

FIA_PK_EXT.1.2 The TSF shall store and protect certificates and/or public keys from unauthorized deletion and modification.

Application Note: For FIA_PK_EXT.1.1, the ST author should select the protocols that are used to implement administrative connectivity that also use public key based authentication. It should be noted that if X.509v3 certificates are used, RFC 5280 defines certificate validation and certification path validation requirements that must be implemented by the TOE as per this requirement. Depending on the protocols selected, there may be additional protocol-specific certificate-related requirements (and associated assurance activities) specified (for instance, RFC 4945 for IPsec). These additional requirements are specified in the requirements associated with that protocol.

Application Note: FIA_PK_EXT.1.2 applies to certificates and/or public keys that are used and processed by the TSF. Certificates or public keys that are used and process by other components in the Operational Environment (e.g., the RADIUS server) are not intended to be covered by this element.

Application Note: If a TOE contains preloaded certificates or public keys, this is acceptable as long as the administrator can “disable” (e.g., revoke, delete) and enable their use.

8.1.4 Class: Security Management (FMT)

8.1.4.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour of** the functions **password based user authentication** to **[assignment: *rules that need to be satisfied for other users to perform the operations*] *by allowing those users to specify rules for acceptable passwords that:***

a) allow for uppercase characters, lowercase characters, digits, and special characters to be used in passwords

b) define a minimum password length of 8 characters or more (at least up to 15 characters)

c) define that passwords must have at least one digit and one special character

d) reject passwords used by the same user before up to a history of at least 6 passwords

8.1.4.2 FMT_MSA.1 Management of object security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP] to restrict the ability to **modify** ***and*** **[selection: change_default, query, delete, [assignment: other operations]]** the security attributes **of the objects covered by the SFP** to **the owner of the object and [assignment: rules that need to be satisfied for other users to perform the operations].**

8.1.4.3 FMT_MSA.3(DAC) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP] to provide **restrictive** 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 perform the activity]]** to specify alternative initial values to override the default values when an object or information is created.

8.1.4.4 FMT_MSA.3(NI) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Network Information Flow Control Policy** 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 perform the activity]]** to specify alternative initial values to override the default values when an object or information is created.

8.1.4.5 FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes *for objects covered by an access control policy*: [assignment: rules for setting the values of security attributes] .

Application Note: The rules need to specify how a new object covered by one of the access control policies gets its security attributes initialized. If those rules differ per object type, the ST author shall use multiple instantiations of FMT_MSA.4 to cover all object types that have security attributes. Inheriting security attributes from another object or from the user/subject that creates the object is one possible way a specific TOE may determine how to initialize an object's security attributes.

8.1.4.6 FMT_MTD.1(AE) Management of TSF data

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

Application Note: This SFR applies to FAU_SEL.1.

8.1.4.7 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]]** the **audit storage** to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to perform the activity]]**.

Application Note: This SFR applies to FAU_STG.1.

8.1.4.8 FMT_MTD.1(AT) Management of TSF data

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

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

b) **action when the threshold is reached**

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

Application Note: This SFR applies to FAU_STG.3.

8.1.4.9 FMT_MTD.1(AF) Management of TSF data

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

Application Note: This SFR applies to FAU_STG.4.

8.1.4.10 FMT_MTD.1(CM) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **import, enable, disable** the **digital certificates or public keys used for remote entity authentication [selection: [assignment: other security functions], no other security function]** to **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to perform the activity]]**.

Application Note: This SFR applies to FTP_ITC.1. The ability to disable could include deletion or revocation of a certificate or key. The enable aspect would make a certificate or key valid for use. These management functions apply to preloaded certificates or public keys as well as those loaded by an administrator.

8.1.4.11 FMT_MTD.1(NI) Management of TSF data

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

a) **identification and matching of network data;**

b) **actions performed on the identified network data**

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

Application Note: This SFR applies to FDP_IFF.1.

8.1.4.12 FMT_MTD.1(IAT) Management of TSF data

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

Application Note: This SFR applies to FIA_AFL.1.

8.1.4.13 FMT_MTD.1(IAF) Management of TSF data

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

Application Note: This SFR applies to FIA_AFL.1.

8.1.4.14 FMT_MTD.1(IAU) Management of TSF data

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

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

8.1.4.15 FMT_REV.1(OBJ) Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke **object security attributes defined by SFPs** associated with the **corresponding object** 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 perform the activity]]**.

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]**.

8.1.4.16 FMT_REV.1(USR) Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke **user security attributes defined by the SFP** associated with the **corresponding user** 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 perform the activity]]**.

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 next authentication of the user;**

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

8.1.4.17 FMT_SMF_RMT.1 Remote Management Capabilities

FMT_SMF_RMT.1.1 The TSF shall allow management functions also to be performed from a remote IT entity using a trusted channel established in accordance with the requirements stated in FTP_ITC.1.

8.1.4.18 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

a) **authorized administrator;**

b) **regular user;**

c) **[assignment: other management roles].**

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

Application Note: When the TOE is started for the first time there needs to be one role that is able to perform the management functions required to configure the TOE. This is viewed as the "authorized administrator". A TOE may have pre-defined additional roles (e. g. for specific management operations) and may also allow for the dynamic definition of additional roles. This SFR is intended to specify the pre-defined roles (as far as they are relevant for the security policy defined by the SFRs), but of course can not be used to specify all roles that may be created dynamically.

Therefore this Protection Profile requires the specification of general rules used by the policy to decide if a user is allowed to perform specific management operations. Those rules may be based on the roles a user has, but also on specific privileges assigned to a user or the group the user belongs to, as well as on additional TSF data (e. g. the user is bound to a specific subject, time and date, approval of the activity by another user, etc.). As long as those rules allow for the restriction of management activities to a defined set of users and as long as the overall rules do not allow user to escalate their own privileges, such rules such rules are acceptable. The ST author is required to specify those rules in the Security Target.

A specific TOE may support more privileges than the developer may want to be specified in the security policy defined by the SFRs. For those privileges that are not used in the Security Target, the developer shall provide some user guidance explaining that any privileges not mentioned in the Security Target may only be assigned to users at the risk of the organization operating the TOE, since their correct implementation with respect to the overall guidance documentation has not been tested or otherwise analyzed as part of the evaluation.

8.1.5 Class: Protection of the TSF (FPT)

8.1.5.1 FPT_STM.1 Reliable time stamps

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

Application Note: A TSF may obtain reliable time stamps from a local hardware clock or may use a secured network connection to obtain the time stamp from a trusted remote entity (if such an entity is available). In the case of a local hardware clock, either the TSF needs to export a management interface that allows a trusted administrator to set or modify the local time, which causes the TSF to use its interfaces to the local hardware clock to perform those actions, or have a protected interface to the hardware in the IT environment that allows for setting or modifying the time clock. For example the possibility to manage the local hardware clock using a dedicated management console used to configure the hardware is acceptable.

8.1.6 Class: TOE Access (FTA)

8.1.6.1 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 data access/*TSF controlled* display devices other than unlocking the session.

Application Note: FTA_SSL.1.1 b) does not prohibit an operating system to continue operation for processes operating on behalf of the user when a session is locked. The operating system should just not display any output from such processes on the display device and not accept any input from input devices associated with the display device (e. g. keyboard and mouse) except those required for unlocking the session as long as the session is locked.

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]**.

Application Note: The intent of the first assignment is that a specific time period or range of time periods are available for the administrator to set. For example, a TOE may allow an administrator to choose a timeout to be 5 minutes, 15 minutes, an hour, or anywhere between using 1 minute increments. It is important that the TOE can be configured such that only an administrator, or a user with some form of privilege , can set the timeout period.

It is possible that a user connects to the TOE from a remote system, for example when using SSH, however this requirement does not apply to such sessions.

8.1.6.2 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 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: The application notes defined above for FTA_SSL.1 also apply here.

8.1.7 Class: Trusted Path/Channels (FTP)

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

Cryptographically-protected communication channel using [selection:

i. **SSH as defined in RFCs 4251, 4252, 4253, and 4254 with a combination of the following cipher suites defined there:**
   - **3DES-CBC, AES256-CBC, AES128-CBC, [selection: AES192-CBC, AEAD_AES_128_GCM (as defined in RFC 5647), AEAD_AES_256_GCM (as defined in RFC 5647), no other algorithms] for encryption;**
   - **[selection: HMAC_SHA1, HMAC-SHA1-96, HMAC-MD5, HMAC-MD5-96] for integrity**
   - **DIFFIE-HELLMAN-GROUP14-SHA1, [selection: DIFFIE-HELLMAN-GROUP1-SHA1, no other algorithm] for key exchange**
   - **SSH-DSS, SSH-RSA, [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms] for public key encryption;**

ii. **TLS as defined in RFC 5246 using X.509 certificates and supporting the following cipher suites defined there:**
   - **TLS_RSA_WITH_AES_128_CBC_SHA**
   - **TLS_RSA_WITH_AES_256_CBC_SHA**

   [selection:
   - **none**
   - **TLS_RSA_WITH_AES_128_CBC_SHA256**
   - **TLS_RSA_WITH_AES_256_CBC_SHA256**
   - **TLS_DH_DSS_WITH_AES_128_CBC_SHA**

- **TLS_DH_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DHE_DSS_WITH_AES_128_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA**
- **TLS_DH_DSS_WITH_AES_256_CBC_SHA**
- **TLS_DH_RSA_WITH_AES_256_CBC_SHA**
- **TLS_DHE_DSS_WITH_AES_256_CBC_SHA**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA**
- **TLS_DH_DSS_WITH_AES_128_CBC_SHA256**
- **TLS_DH_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_DHE_DSS_WITH_AES_128_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA256**
- **TLS_DH_DSS_WITH_AES_256_CBC_SHA256**
- **TLS_DH_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_DHE_DSS_WITH_AES_256_CBC_SHA256**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
- **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256**
- **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384;**

iii. **IPSEC protocol ESP as defined in RFC 4303 using the cryptographic algorithms:**

- **AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, Triple-DES, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106] for ESP encryption;**
- **[selection: HMAC-SHA1-96, AES-XCBC-MAC-96] for ESP authentication and authentication header protection;**
- **[selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996, 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]] for key negotiation and SA establishment;**
- **DH Groups 14 (2048-bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), [assignment: other DH groups that are implemented by the TOE], no other DH groups] for use in IKE key establishment;**
- **[selection: DSA, rDSA, ECDSA] algorithm for Peer Authentication;**

Application Note: For a specification of those cipher suites, see the RFCs mentioned.

Application Note: It is mandatory that the TOE can be configured to reject the setup of a trusted channel if not one of the above mentioned cipher suites is used. A TOE compliant with this base OSPP may still implement a subset of the cipher suites listed above and may also implement cipher suites not contained in the list above but listed in the RFCs referenced. It just needs to provide the capability to ensure that a combination of cryptographic algorithms mentioned above is used if a trusted channel is requested. Other cipher suites may only be used for untrusted channels.

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]**.

8.2 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.

8.2.1 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.

8.2.1.1 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 events to be audited. 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. This applies to local audit storage, which the TOE must provide. Optionally the TOE may allow a configuration where audit data is transferred to a remote trusted IT system where it is stored.

8.2.1.2 User Data Protection

User data needs to be protected from unauthorized access. This requires the TOE to implement an access control policy for all types of objects that may be used to share user data between different users or subjects. For at least one type of persistent objects the access control policy must allow for specifying access control down to the level of a single user. 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.

8.2.1.3 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.

8.2.1.4 Security Management

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

8.2.1.5 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.

8.2.1.6 TOE Protection

The TOE shall provide a cryptographically-protected network protocol based on symmetric ciphers, which supports certificate based authentication of the remote peer. For supporting the authentication, the TOE shall use digital certificates as defined in the protocol specifications.

8.2.2 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
FDP_ACC.1	O.DISCRETIONARY.ACCESS, O.SUBJECT.COM
FDP_ACF.1	O.DISCRETIONARY.ACCESS, O.SUBJECT.COM
FDP_IFC.1	O.NETWORK.FLOW
FDP_IFF.1	O.NETWORK.FLOW
FDP_RIP.2	O.AUDITING O.DISCRETIONARY.ACCESS O.SUBJECT.COM O.NETWORK.FLOW O.I&A
FIA_AFL.1	O.I&A
FIA_ATD.1	O.I&A
FIA_UAU.1(RITE)	O.NETWORK.FLOW
FIA_UAU.1(HU)	O.I&A
FIA_UAU.5	O.I&A

SFR	Objectives
FIA_UAU.7	O.I&A
FIA_UID.1	O.I&A
FIA_USB.1	O.I&A
FIA_PK_EXT.1	O.TRUSTED_CHANNEL
FMT_MOF.1	O.I&A, O.MANAGE
FMT_MSA.1	O.MANAGE
FMT_MSA.3(DAC)	O.MANAGE
FMT_MSA.3(NI)	O.MANAGE
FMT_MSA.4	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(CM)	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_RMT.1	O.MANAGE
FMT_SMR.1	O.MANAGE
FPT_STM.1	O.AUDITING
FTA_SSL.1	O.I&A
FTA_SSL.2	O.I&A
FTP_ITC.1	O.TRUSTED_CHANNEL

Table 7: 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 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].
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]. The rules for the access control policy are defined [FDP_ACF.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2].
O.NETWORK.FLOW	The network information flow control mechanism controls the information flowing between different entities [FDP_IFC.1]. The TOE implements a rule-set governing the information flow [FDP_IFF.1]. Information flow control is enforced for unauthenticated remote IT entity, allowing authenticated remote IT entity to be excluded from the rules of the network information flow control policy (FIA_UAU.1(RITE)). The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2].
O.SUBJECT.COM	The TSF must control the exchange of data using transient storage objects between subjects based on the identity of users. The access control policy must have a defined scope of control [FDP_ACC.1]. The rules for the access control policy are defined [FDP_ACF.1]. The protection of reused resources ensures that no data leaks from other protected sources [FDP_RIP.2].
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(HU)]. Multiple I&A mechanisms are allowed as specified in [FIA_UAU.5]. To ensure authorized access to the TOE,

Objectives	Coverage Rationale
	authentication data is protected [FIA_ATD.1, FIA_UAU.7]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB.1]. To support the strength of authentication methods, the TOE is capable of identifying and reacting to unsuccessful authentication attempts [FIA_AFL.1] and define password rules [FMT_MOF.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] are present.
O.MANAGE	The TOE provides management interfaces for: □ the access control policies [FMT_MSA.1, FMT_MSA.3(DAC)]; □ 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)]; □ digital certificates [FMT_MTD.1(CM)]; □ 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]. 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)]. Management of password rules is defined in [FMT_MOF.1]. Remote management capabilities need to be provided as defined in [FMT_SMF_RMT.1].
O.TRUSTED_CHANNEL	The TOE provides a trusted channel protecting communication between a remote trusted IT system and itself [FTP_ITC.1]. Digital certificates must be used for remote entity authentication [FIA_PK_EXT.1].

Table 8: Security Functional Requirements rationale

8.2.3 Security Requirements Dependency Analysis

SFR	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1	Yes: FAU_GEN.1

SFR	Dependencies	Resolved
	FIA_UID.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
FDP_ACC.1	FDP_ACF.1	Yes: FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes: FDP_ACC.1 Yes: FMT_MSA.3(DAC)
FDP_IFC.1	FDP_IFF.1	Yes: FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes: FDP_IFC.1 Yes: FMT_MSA.3(NI)
FDP_RIP.2	N/A	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	N/A	Yes
FIA_UAU.1(RITE)	FIA_UID.1	Yes
FIA_UAU.1(HU)	FIA_UID.1	Yes
FIA_UAU.5	N/A	Yes
FIA_UAU.7	FIA_UAU.1	Yes: FIA_UAU.1(HU)
FIA_UID.1	N/A	Yes
FIA_USB.1	FIA_ATD.1	Yes: FIA_ATD.1
FIA_PK_EXT.1	FMT_MTD.1	Yes: FMT_MTD.1(CM)
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes: FDP_ACC.1 Yes: FMT_SMR.1 Yes: FMT_SMF.1
FMT_MSA.3(DAC)	FMT_MSA.1	Yes: FMT_MSA.1

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	[FDP_ACC.1 or FDP_IFC.1]	Yes: FDP_ACC.1
FMT_MTD.1(AE)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(AS)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(AT)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(AF)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(CM)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(NI)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(IAT)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(IAF)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_MTD.1(IAU)	FMT_SMR.1 FMT_SMF.1	Yes: FMT_SMR.1 No: FMT_SMF.1
FMT_REV.1(OBJ)	FMT_SMR.1	Yes
FMT_REV.1(USR)	FMT_SMR.1	Yes
FMT_SMF_RMT.1	FTP_ITC.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_STM.1	N/A	Yes
FTA_SSL.1	FIA_UAU.1	Yes: FIA_AUA.1(HU)
FTA_SSL.2	FIA_UAU.1	Yes: FIA_AUA.1(HU)
FTP_ITC.1	N/A	Yes

Table 9: Security Functional Requirements dependency analysis

Rationale for unresolved dependencies:

- The dependencies in several SFRs on FMT_SMF.1 have not been resolved, since the SFR FMT_SMF.1 has not been included in the Protection Profile. Instead the Protection Profiles contains specific instances of FMT_MTD.1 for each individual management aspect with the ability (and requirement) for the ST author to specify exactly the rules a TOE uses to determine if a user has the required authority to perform a management activity.
- 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).

8.3 Security Assurance Requirements

This protection profiles includes the following assurance components, which are refined by the assurance activities in OSPP Part2: “General Approach and Assurance Activities for OSPP Evaluations” ([OSPP-2]).

SAR	Title
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE.TSS.1	TOE summary specification
ADV_ARC.1	Security architecture description
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.3	Authorisation controls
ALC_CMS.3	Implementation representation CM coverage
ALC_DEL.1	Delivery procedures
ALC_FLR.3	Systematic flaw remediation
ALC_LCD.1	Developer defined life-cycle model
ATE_COV.2	Analysis of coverage

SAR	Title
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.2	Vulnerability analysis

Table 10: Security Assurance Requirements

8.4 Security Assurance Requirements Rationale

SAR	Dependency	Resolved
ASE_INT.1	–	–
ASE_CCL.1	ASE_INT.1	Yes
	ASE_ECD.1	Yes
	ASE_REQ.1	Yes
ASE_SPD.1	–	–
ASE_OBJ.2	ASE_SPD.1	Yes
ASE_ECD.1	–	–
ASE_REQ.2	ASE_OBJ.2	Yes
	ASE_ECD.1	Yes
ASE.TSS.1	ASE_INT.1	Yes
	ASE_REQ.1	Yes
	ADV_FSP.1	Yes
ADV_ARC.1	ADV_FSP.1	Yes
	ADV_TDS.1	No
ADV_FSP.1	–	–
AGD_OPE.1	ADV_FSP.1	Yes
AGD_PRE.1	–	–
ALC_CMC.3	ALC_CMS.1	Yes
	ALC_DVS.1	No
	ALC_LCD.1	Yes
ALC_CMS.3	–	–

SAR	Dependency	Resolved
ALC_DEL.1	–	–
ALC_FLR.3	–	–
ALC_LCD.1	–	–
ATE_COV.2	ADV_FSP.2	No
	ATE_FUN.1	Yes
ATE_DPT.1	ADV_ARC.1	Yes
	ADV_TDS.2	No
	ATE_FUN.1	Yes
ATE_FUN.1	ATE_COV.1	Yes
ATE_IND.2	ADV_FSP.2	No
	AGD_OPE.1	Yes
	AGD_PRE.1	Yes
	ATE_COV.1	Yes
	ATE_FUN.1	Yes
AVA_VAN.2	ADV_ARC.1	Yes
	ADV_FSP.2	No
	ADV_TDS.1	No
	AGD_OPE.1	Yes
	AGD_PRE.1	Yes

Table 11: Security Assurance Requirements dependency analysis

Rationale for unresolved dependencies:

- Several dependencies on components of the ADV_TDS family have not been satisfied (ADV_ARC.1, ATE_DPT.1, AVA_VAN.2). Although no component from the ADV_TDS family is included in this mapping, design-related aspects from the description of the SFR-related assurance activities described in this document have to be considered during an evaluation. No component of the ADV_TDS family has been included since none of them fits the view on the required design evaluation aspects for products compliant with this Protection Profile. Still, the authors believe that sufficient design information is provided to perform the evaluation activities for the components with unsatisifed dependencies.
- Several dependencies on ADV_FSP.2 have not been satisfied (ATE_COV.2, ATE_IND.2, AVA_VAN.2). This protection profile only includes ADV_FSP.1. However, the intention is that all TSFI provided by the developer are described to the extent that they can be used to develop test cases, correctly identify the expected test result and to perform the vulnerability analysis.

Therefore, the authors believe that sufficient information on the TSFI is provided to allow for the evaluation activities for the components with unsatisfied dependencies to be performed.

- The dependency of ALC_CMC.3 to ALC_DVS.1 is not satisfied. However, it is expected that the evaluator will examine that the CM processes described by the developer for ALC_CMC.3 are established as described. This can be achieved for example by verifying that the described process steps are being applied during an evaluator's on-site visit (e.g., to perform independent testing). Therefore, the authors believe that the evaluator will gain sufficient confidence in the existence and proper application of the CM processes described in ALC_CMC.3.

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	General-Purpose 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