

HASK-PP

Protection Profile for a High Assurance Security Kernel

Type + No: [CCV3.1 Protection Profile]
Identifier: HASK-PP
Version: 1.14
Date: 30th of June 2008
Status: [FINAL]
Classification: [PUBLIC]

SIRRIX AG SECURITY TECHNOLOGIES.

Address: Im Stadtwald, Geb. D3 2, 66123 Saarbrücken, Germany

Phone: +49 681 936251-0

Fax: +49 681 936251-500

E-Mail: info@sirrix.com

Web: <http://www.sirrix.com>

COPYRIGHT © 2008 BY SIRRIX AG SECURITY TECHNOLOGIES AND BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI)

ALL RIGHTS RESERVED.

DISCLAIMERS:

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED OR INTENDED HEREBY.

SIRRIX and BSI, DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, RELATING TO THE USE OF THE INFORMATION IN THIS SPECIFICATION AND TO THE IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. SIRRIX AND BSI, DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE SUCH RIGHTS.

WITHOUT LIMITATION, SIRRIX AND BSI DISCLAIM ALL LIABILITY FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE, ARISING IN ANY WAY OUT OF USE OR RELIANCE UPON THIS SPECIFICATION OR ANY INFORMATION HEREIN.

All product names are trademarks, registered trademarks, or service marks of their respective owners.

Revision History

Version	Change Date	Author(s)	Changes to Previous Version
0.9	2007-04-30	Krummeck	Initial version
1.0		Kurth, Krummeck	First version for commenting
1.1	2007-06-22	Kurth, Krummeck	Included comments from workshop, more detail
1.2	2007-07-03	Kurth, Krummeck	First Complete Version
1.3	2007-07-06	Kurth, Krummeck	Additional changes addressing comments
1.4	2007-07-16	Kurth, Krummeck	Additional changes addressing comments from BSI
1.5	2007-08-31	Kurth	Some clarifications to avoid misinterpretations
1.6	2007-10-22	Kurth	Addressing comments from the evaluation
1.7	2007-11-19	Kurth, Stüble	Addressing additional comments from the evaluation and BSI, reformatting
1.8	2007-12-28	Stüble	Addressing comments from the evaluation
1.9	2008-02-28	Kurth, Stüble	Addressing comments from version 1.8
1.10	2008-03-18	Stüble	Addressing comments from version 1.9
1.11	2008-03-25	Stüble	Addressing comments from version 1.10
1.12	2008-03-26	Stüble	Addressing comments from version 1.11
1.13	2008-03-27	Stüble	Added FMT_MSA.2 to the security requirements rationale of O.MANAGE Fixed typo in O.CONFIDENTIALTY_USERDATA
1.14	2008-06-30	Stüble	Addressing comments form version 1.13

Table of Contents

1	PP introduction	5
1.1	PP reference.....	5
1.2	TOE overview.....	5
1.2.1	TOE type	5
1.2.2	Summary of TOE architecture and functions.....	5
1.2.3	TOE subjects, objects and security attributes	10
1.2.4	TOE policies	13
1.2.5	TOE operational environment	15
2	Conformance claim	17
2.1	CC conformance claim	17
2.2	PP claim, Package claim	17
2.3	Conformance rationale	17
2.4	Conformance statement	18
3	Security problem definition	18
3.1	Threats	18
3.1.1	Threats to be addressed by the TOE	19
3.1.2	Threats to be addressed by the TOE environment	20
3.2	Organizational security policies	20
3.3	Assumptions.....	20
4	Security objectives.....	22
4.1	Security objectives for the TOE	22
4.2	Security objectives for the operational environment	23
4.3	Security objectives rationale	24
5	Extended components definition	27
6	Security requirements.....	27
6.1	Security functional requirements.....	27
6.1.1	SFR summary	27
6.1.2	Audit (FAU).....	29
6.1.3	Communication (FCO)	30
6.1.4	Cryptographic support (FCS).....	30
6.1.5	User data protection (FDP).....	30
6.1.6	Identification and Authentication (FIA).....	35
6.1.7	Security management (FMT)	37
6.1.8	Protection of the TSF (FPT).....	40
6.1.9	Resource utilisation (FRU)	41
6.1.10	Trusted path/channel (FTP)	41
6.2	Security assurance requirements	42
6.3	Security requirements rationale.....	42
6.3.1	Tracing security objectives to security functional requirements	42
6.3.2	Security requirements dependency analysis	47
7	References	49

1 PP introduction

This section contains overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The PP identification provides the labelling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a stand-alone abstract for PP catalogues and registers.

1.1 PP reference

This protection profile is referenced as follows:

Title:	Protection Profile for a High Assurance Security Kernel
Version:	1.14
Authors:	Helmut KURTH, Gerald KRUMMECK (atsec information security) Christian STÜBLE (Sirrix AG security technologies) Marion WEBER (German Federal Office for Information Security) Marcel WINANDY (Ruhr-University Bochum)
Publication Date:	30 th of June 2008

1.2 TOE overview

1.2.1 TOE type

This Protection Profile is defined for security kernels that provide functions for the management and separation of compartments operating on top of the security kernel. Examples of product types that may implement the functions described in this Protection Profile are:

- Microkernel
- Virtual machine monitors
- Logical partitioning products

An important function that must exist in a product claiming compliance with this Protection Profile is the ability to "proof" a "trust status" to a remote trusted IT product and to verify the correctness of a status submitted by a remote trusted IT product. This status shall show that the external entity is authentic, has not been modified, and is "fresh" (i. e. the status information received has not been replayed from a previous status information potentially intercepted by an attacker). The Protection Profile deliberately does not prescribe which method is used to generate and verify such status information.

A TOE compliant to this Protection Profile requires hardware, software or firmware in its environment that is able to ensure the integrity of the TOE and its data during start-up.

1.2.2 Summary of TOE architecture and functions

This Protection Profile (PP) specifies the security functional and assurance requirements for a class of security kernels that allow executing multiple separated compartments on a single trusted system. Each compartment can behave like a single platform separated from each other with the TOE enforcing this separation and controlling the communication between

compartments as well as with external entities in accordance with a defined policy. Any product claiming compliance with this PP shall provide the necessary security functionality with a high degree of assurance to its users.

Compartments are active entities within the TOE that request services from the TSF. The TSF itself can be either a monolithic kernel or a kernel plus a set of trusted compartments. This Protection Profile does not prescribe the way the TSF is designed and implemented.

In addition to compartments, external entities can communicate with the TSF and/or compartments controlled by the TSF. To control the communication of external entities with compartments as well as the communication between compartments, the TSF manages a set of "communication objects" that can be assigned to compartments. Those communication objects allow the TSF to control which external entities and other compartments a compartment can communicate with and how this communication is protected. Protection of communication is defined by security attributes assigned to communication objects. Those attributes can define characteristics of the communication link like

- the set of external entities one can communicate with using this communication object,
- the kind of protection for the communicated data requested from the TSF when using the communication object (integrity protection, confidentiality protection, authentication of the communication peer).

In addition to the communication objects the TOE also manages "containers" of persistent or volatile storage called "storage container" in the rest of this document. Those may be whole disks, disk partitions, disk sectors, etc. where the technology to implement those containers (magnetic disks, flash disks, memory disks etc.) is not relevant for this Protection Profile.

The TSF has the following (abstract) set of functions:

- Management of compartments (creation, deletion, starting, changing attributes)
- Management of objects, which are at least containers and communication objects (creation, deletion, changing attributes, defining and managing access control policies)
- Management of resources, which are at least processor time and memory (assignment to compartments, setting resource limits, controlling resource limits)
- Generation and verification of information that reliably shows the integrity of the TSF, a compartment managed by the TSF or specific data.

A TOE compliant with this Protection Profile needs to control the way compartments can access objects, use resources and communicate with each other and with external entities. This requires the TOE to implement access control policies between compartments and the objects controlled by the TOE. This Protection Profile requires a TOE to implement both a discretionary access control policy as well as a mandatory access control policy. The rules of both policies are left to be defined by a specific TOE that claims compliance with this PP, but the following needs to be implemented:

- The discretionary access control policy must at least allow differentiating between "no access" and "access" and must allow to specify those access modes down to individual compartments and objects. It is left to a TOE compliant to this Protection Profile to allow other access modes (e. g. read only). If a TOE defines such additional access modes, the access control rules associated with those modes must also be defined in the ST of such a TOE.
- The mandatory access control policy must allow separating two compartments to a level that no information flow between those two compartments is possible.

All other, more refined rules of the discretionary and mandatory access control policy are left to the author of a ST that claims compliance with this PP.

A TOE compliant to this Protection Profile also has to provide a set of functions that assure the integrity of the TSF, the compartments as well as data in storage container. Integrity is here

defined as the ability to detect any unauthorized modification to those data including the attempt to replay older versions of such data. The integrity verification of the TSF itself has to be verified within the TOE environment or with the assistance of the TOE environment before or when the TOE is started. How this is done is not specified in this Protection Profile. This allows for the use of different methods that are able to achieve this security objective.

Once the TSF is started using such a secure start-up process, the TSF shall implement a functionality that is able to verify the integrity of a compartment before or while it loads and starts a compartment. Compartments itself may request the TSF to apply similar integrity protection for storage container. The TSF must be able to generate evidence of this integrity to remote trusted IT product upon an authorized request to do so. This evidence must allow the remote trusted IT product to unambiguously verify the integrity of the entity it has requested the integrity verification data for. In addition the TSF must have a functionality to verify such integrity verification data submitted upon request from another trusted IT product.

Those functions together allow for a chain of integrity verification starting from the assured integrity of the TSF by the TOE environment, the assured integrity of a compartment and the assured integrity of storage container used by a compartment. This creates a chain of trust for integrity. The specification of the specific mechanisms used to implement this chain of trust is left to the individual TOEs and not prescribed in this Protection Profile.

In a similar way also the confidentiality of the TSF and TSF data, the compartment and compartment data and the storage container need to be protectable. The TOE environment is requested to protect (if necessary) the confidentiality of the TSF and TSF data loaded as part of the start-up process while the TSF itself needs to be able to protect the confidentiality of compartments, storage container and TSF data not protected by the TOE environment. In addition the TSF needs to provide an interface that allows compartments to request confidentiality protection for storage container. The specific mechanisms used to implement this chain of trust are left to the individual TOEs and not prescribed in this Protection Profile.

The TOE will allow communication between compartments and with external entities. A mandatory requirement is that the TOE allows compartments to communicate with compartments and external entities under the control of the TSF. This is done using the communication objects. A communication object itself is subject to both the discretionary and mandatory access control policy, allowing the TOE to decide based on this policy if a compartment is allowed to use the communication object at all. Other access modes (e. g. read only) may be implemented but are not mandated by this Protection Profile.

Once a compartment is allowed to use a communication object, the security attributes of the communication object control what a compartment can do using this communication object. Mandatory security attributes of a communication object are security attributes that are required to evaluate the rules of the discretionary and mandatory access control policies used to decide which external entities and compartments can be communicated with using this communication object.

The evaluation of the rules of the discretionary and mandatory access control policies designate the external entities and compartments that can be communicated with using this communication object. The TSF will enforce that the communication object can not be used to communicate directly with other than those external entities and compartments.

Another security attribute that is mandatory to implement in a TOE compliant with this Protection Profile is the trusted channel attribute which can be assigned either to the communication object as a whole or to individual external entities or compartments that can be used to communicate with using the communication object. The trusted channel attribute, when assigned, requires the TSF to ensure that the communication link to the external entities and compartments for which this attribute applies is set up using a trusted channel, i. e. provides integrity and confidentiality protection of the user data transferred over the channel

and ensures identification and authentication of the communication partner. Again this Protection Profile does not prescribe any specific protocol. This is left to the individual TOEs.

The implementation of additional security attributes of communication objects is also left to the individual TOEs. Potential examples of such additional security attributes of communication objects are:

- Address translation rules assigned to a communication object as a whole or to individual communication partners in the list
- Filter rules assigned to a communication object as a whole or to individual communication partners in the list
- Specification of protocols allowed for the communication object

An example for the use of communication objects and their security attributes is when a compartment is allowed to use a communication object to communicate with a defined subset of IP addresses only where the communication is routed through a Virtual Private Network (VPN) router that is implemented as a trusted compartment as part of the TSF. The kernel would route communication between a compartment that is allowed to access the communication object and an external entity to the trusted compartment providing this with the security attributes assigned to the communication object. The trusted compartment would then implement the VPN functionality as defined by the security attributes of the communication object.

A TOE compliant to this Protection Profile does not need to have human users defined. The designer of a TOE compliant to this Protection Profile may decide to have human users as an extension to the minimum security policy defined in the Protection Profile. In this case the Security Target for such a TOE needs to include functions for user management, user identification and authentication as well as potentially a user-subject binding function that defines how the security attribute of a subject are defined as the result of such a binding. The author of such a Security Target needs to ensure that those additions do not conflict with the security functional requirements defined in this Protection Profile.

This Protection Profile requires identification of the subjects (compartments and external entities) as well as authentication of external entities requesting services from the TSF. This is necessary to base the decision of the access control policies as well as the management functions on assured identities of the entities requesting access to controlled objects or performing management activities. There is no method prescribed in this Protection Profile how the TSF verifies the identity of a subject. This is left to the author of a Security Target claiming compliance to this Protection Profile.

Another mandatory function is the definition of a role model that allows to restrict management activities to defined authorized roles. This Protection Profile does not prescribe the type of roles, their number or the privileges that are assigned to specific roles. In the simplest form there could be a single management role that is allowed to perform all management activities and that is bound to a specific compartment identity. The Protection Profile also allows a Security Target to define a complex dynamic role model that allows to have a fine granularity of privileges that can be assigned to roles thus allowing to split the management activities to a number of different roles. This Protection Profile does not mandate that roles have to be dynamic but if a specific TOE claiming compliance with this Protection Profile does so, it has to define the rules for management of those roles (including the management of privileges assigned to roles and the assignment of roles to subjects) in its Security Target.

Usage and major security features of the TOE

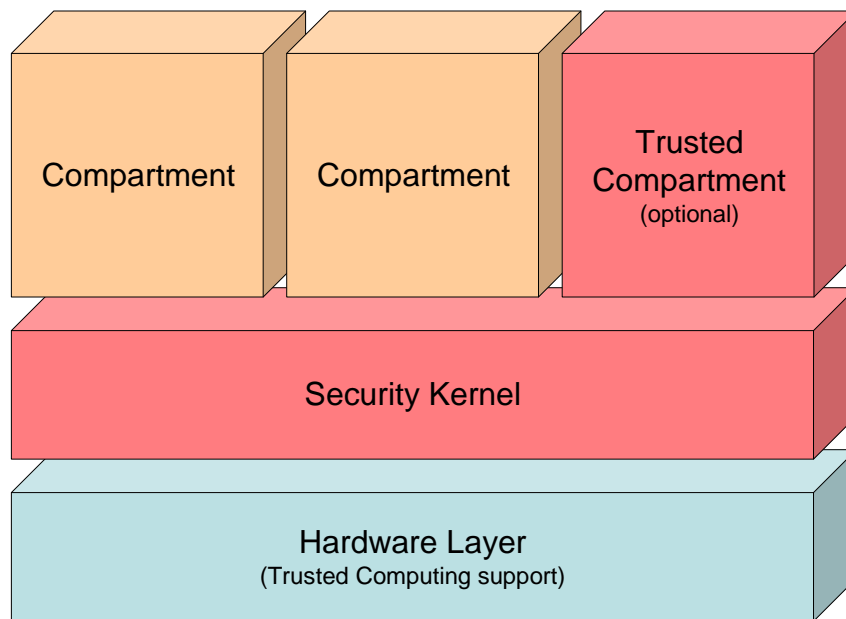


Figure 1: TOE architecture (red parts implement the TSF)

The TOE envisaged by this Protection Profile consists of a security kernel running on top of a trusted hardware layer (which is part of the TOE's IT environment), and controlling several compartments within the TOE. Compartments may be trusted, i.e. have privileges which allow them to extend the security policy and provide additional security functionality (e.g. management of security functionality or sophisticated access control functionality). An example is the definition of a "proxy compartment" where the proxy compartment provides some kind of additional service not included in the base functions. An example is a proxy compartment that performs communication or disk encryption transparent to the user.

Major security functionality implemented by the TSF of any product compliant to this PP are:

- Management of compartments (creation, deletion, starting, changing attributes)
- Management of storage containers and communication objects (creation, deletion, changing attributes)
- Protection of storage containers
- Protection of communication through communication objects
- Management of resources, which are at least processor time and memory regions (assignment to compartments, setting resource limits, controlling resource limits)
- Support for user roles (including administrative roles). Note that the security kernel will most likely deal with privileges assigned to compartments or to requests from external entities without the need to associate them with users, but the Common Criteria use the notion of authorized roles, thus requiring the introduction of users and roles to express certain security requirements.
- Protection of the TSF itself, which includes verification of the integrity of TSF data, verification of the correct function of the TSF protection features
- Establishment of trusted channels to remote trusted IT products

The implementation of products compliant to this PP will most likely require additional security functionality which are not stated in this PP to avoid the specification of a certain implementation or mechanism to achieve the objectives set forth in this PP. However, the PP authors envisage that STs claiming compliance to this PP would probably include:

- Provision of cryptographic functions to ensure the integrity, confidentiality and authenticity of user and TSF data transferred over unsecured communication links and to ensure the authenticity of integrity evidence data.
- Identification and authentication of users before they are assigned to compartments. Note that compartments may implement their own user management, which is not subject of this PP.
- Establishment of a trusted path for user authentication.

Compartments will have containers assigned that they can use to store their data. Those can be viewed as partitions of a disk that the software in each compartment can use to store persistent data. Functions will allow a compartment to request additional containers from the TOE or release unused containers to the TOE.

Available non-TOE hardware/software/firmware

In order to perform those functions a TOE compliant with the PP needs to rely on the following functions of the IT environment:

- A secure function for the support of the generation of evidence that the TSF has not been tampered with.
- Hardware support for memory protection that allows separating the physical memory used by compartments from the one used by other compartments or the TSF.
- Hardware support to prohibit direct access of compartments to devices not solely allocated to the compartment.
- Support for a secure start-up of the TSF

1.2.3 TOE subjects, objects and security attributes

1.2.3.1 Subjects

In the envisaged architecture, subjects are the active entities requesting services to be performed by the TSF. Two kinds of subjects are recognized:

- **Compartments** are the active entities within the TOE. A compartment can be for example
 - a partition running a complete legacy operating system, which itself manages a number of processes, or
 - a single application providing some dedicated service;

A compartment may be assigned one or more specific roles. Roles are used to define the subjects that are allowed to perform specific management activities.

Compartments may interact with human users or other type of users not known to the TOE. The security kernel itself is not required to have a notion of human users, although implementations may choose to associate compartments with users and build parts of their security policy based on this association.

Compartments have the following security attributes:

- Identity – compartments are identified by a unique identifier which will be used by the TSF to distinguish between the compartments managed by the TSF. It is left to the individual TOE's claiming compliance to this Protection Profile how this unique identifier is established and how uniqueness is achieved.

- List of privileges assigned to the compartment. Assignment of such privileges (e.g. to start and stop other compartments, change vital TSF data, administer audit functions, etc.) depends on the trust in the compartment is managed by the TSF. The TOE may implement specific policies on how to set and manage the maximum set of privileges that a compartment has (e.g. by a combination of privileges pre-defined in the TSF data and privileges inherited from the subject requesting the compartment's start). The TOE may also define specific policies how to deal with privileges. For example, compartments could be allowed to give up certain privileges before performing sensitive operations and re-acquire those privileges later on. Another implementation could be to only give up privileges permanently, i.e. without the chance to reacquire them.
- Integrity status (the TSF needs to include a functionality that can verify the integrity of a compartment and provide evidence of this to an external entity upon request)
- Information flow control security attributes; examples for such additional attributes could be
 - ◆ Label – a security label used for information flow decisions
- Potentially other security attributes assigned and managed by a TOE compliant to this PP and necessary to implement parts of the security policy not fully specified in this PP. Examples for such additional attributes could be
 - ◆ Owner
- Inheritable privileges (as a subset of the maximum set of privileges allowed for the compartment)
- **External entities** are active entities, too, but are located outside the TOE boundary. External entities may request a service from the TOE, e.g. to start or stop a compartment. The TOE needs to verify the authorization of such requests, which may or may not require the identification of the entity. If identification of an external entity is required, it is also required to properly authenticate it.

External entities have the following security attributes:

- List of privileges assigned to the external entity. The privileges are taken from the same set as for compartments.
- Information flow control security attributes; examples for such additional attributes could be
 - ◆ Label – a security label used for information flow decisions
- other security attributes assigned and managed by a TOE compliant to this PP and necessary to implement parts of the security policy not fully specified in this PP; Examples are:
 - ◆ User attributes. If users are distinguished by the TOE, it would need to handle
 - User ID
 - authentication data to verify the user's identity
 - role

Note that external entities may also connect to a compartment (via a communication object) and ask the compartment to make a request on its behalf. In such a case, the compartment needs to be allowed to use the communication object and needs to be allowed to make such a request itself; the decision whether or not to grant the external entities's request and forward it to the TOE's TSF is with the compartment; the TSF will only check the privileges of the compartment in this case.

A TOE compliant with this Protection Profile may also request an external entity to authenticate to the TSF and the TSF then "binds" this external entity to a compartment. In those cases the Security Target needs also to define how the security attributes of the compartment are set or modified as a result of this TSF-controlled binding. For example, in the case of an external entity that has certain administrative privileges assigned to it, the binding process may give those privileges to the compartment the external entity is bound to. Such a function is not mandatory for a TOE compliant to this Protection Profile but may be included provided it is implemented in a way that does not violate any of the mandatory requirements defined in this Protection Profile.

1.2.3.2 Objects

Objects are the passive entities in the system. At a minimum, PP-compliant systems must recognize at least two types of objects: storage containers and communication objects.

- **Storage Containers** are objects that hold user data accessed and used by compartments. They can be persistent (like a file or a hard disk partition) or volatile (like a memory region). It is allowed that the TSF uses the same type of storage container to store some TSF data (e. g. an audit trail) as long as all the requirements for the protection of the specific type of TSF data are satisfied.

Storage containers have the following security attributes:

- Identity – storage containers are identified by a unique identifier which will be used by the TSF to distinguish between the compartments managed by the TSF. It is left to the individual TOEs claiming compliance to this Protection Profile how this unique identity is established.
 - Integrity and confidentiality attributes
 - List of Resources assigned to the object
 - Access control security attributes necessary to enforce the compartment access control policy; examples of such attributes could be
 - ◆ Owner
 - ◆ Access control lists
 - Information flow control security attributes; examples for such additional attributes could be
 - ◆ Label – a security label used for information flow decisions
- **Communication objects (COs)** can be assigned to compartments and allow them to communicate with other compartments or external entities.

COs have the following security attributes:

- Identity – communication objects are identified by a unique identifier which will be used by the TSF to distinguish between the COs managed by the TSF. It is left to the individual TOEs claiming compliance to this Protection Profile how this unique identity is established.
- Integrity and confidentiality protection information; for trusted channels between TOE or a compartment and external entities, information on the protection mechanisms may be required (if the protection and the mechanisms used can be negotiated); This may include information on cryptographic algorithms as well as keys associated, e.g. with sessions established over the CO. It may also include sophisticated rules (for example based on network address, certificate trust, incoming or outgoing requests, etc.) governing the establishment of connections through COs
- Information flow control security attributes; examples for such additional attributes could be

- ◆ Label – a security label used for information flow decisions
- Potentially other security attributes assigned and managed by a TOE compliant to this PP and used to enforce the compartment access control policy. Such an attribute could be, for example,
 - ◆ Owner – the ID of the entity defined as owner with associated management rights
 - ◆ Rules ...

1.2.3.3 Resources

Resources are managed by the security kernel and assigned to compartments based on policy rules. Resources required to be controlled in this Protection Profile are:

- CPU cycles (or whole CPUs)
- Memory regions

A TOE compliant with this Protection Profile may define additional resources like I/O devices, disk space, etc. The TSF must be able to enforce a policy on such resources which include a maximum value of a resource type a compartment may use at a time. Access to serial reusable resources (e. g. specific I/O devices) may also be regulated using the resource management policy.

1.2.4 TOE policies

1.2.4.1 Audit policy

A TOE compliant with this Protection Profile must support the generation of audit records for at least

- Start and stop of the audit function
- Attempted and successful modification of the security policy (which includes all management activities)
- Detected integrity violations

The TOE must provide the ability for an authorized role to select which of those events are actually audited. It is left to the individual implementation if the audit trail is stored within the TOE or if the audit events are sent to another trusted IT entity for storage and evaluation.

1.2.4.2 Discretionary access control policy

A TOE compliant with this Protection Profile must support a discretionary access control policy between subjects and objects that covers at least the subjects and objects defined in this Protection Profile. This access control policy must be able to define access down to the level of individual subjects. No specific rules for the access control policy are predefined in this Protection Profile. Especially the aspect how this access control policy is managed is left to the individual TOEs. This allows them to implement a policy where the modification of access rights is left to dedicated administrators as well as a policy where the modification of access rights is allowed for the "owner" of an object. In the later case "owner" needs to be defined as an authorized role with respect to the objects owned by a subject.

It is also left to a TOE compliant with this Protection Profile to define the rules that have to be satisfied to allow or deny access as well as the security attributes or other TSF data evaluated as part of those rules.

1.2.4.3 Information flow control policy

A TOE compliant with this Protection Profile must support an information flow control policy that at least allows to isolate compartments within the TOE (i. e. not allow any information flow

between those compartments) and also allows to regulate the information flow between compartments and external entities. In contrast to the discretionary access control policy, the rules of the information flow policy also need to apply for subjects and objects a TOE may implement in addition to the ones defines in this Protection Profile. As with the definition of the discretionary access control policy, the specific rules that define when an information flow between subjects is allowed is left to the individual TOEs claiming compliance to this Protection Profile. In the simplest case the requirements of the information flow control policy can be implemented by a very simple attribute that either allows or forbids information flow with other subjects. Another example is a Bell-LaPadula [BLP] like information flow policy based on a set of labels that form a lattice. Also more complex information flow policies based on complex attributes of subjects are possible.

1.2.4.4 Import and export of user data

A TOE compliant with this Protection Profile must support import and export of user data controlled by the TSF. This includes especially data with attributes showing the integrity status.

1.2.4.5 Trust policy and integrity verification

One of the most important aspects of a TOE compliant with this Protection Profile is the trust that can be placed into the integrity of the TSF and individual compartments executing under the control of the TSF. The operational environment is required to ensure the integrity of the TSF code and data during the start-up process. When this integrity check for the TSF is successful, the TSF itself has to provide functionality that ensure the integrity of compartments when starting them. The TSF also has to provide a functionality that can be used by a compartment to verify the integrity of storage container it is allowed to access. This provides a complete chain of trust starting from the TSF down to storage container used by compartments.

In addition the TSF shall also provide a functionality that external entities can use to receive evidence of the integrity of the TSF, compartments operating under the control of the TSF and storage container. This evidence must be generated in a way that it can not be falsified by an attacker. This Protection Profile does not prescribe how this evidence is generated. It only requires that the function provides the external entity with a reliable statement if the entity it requested evidence of integrity for is not corrupted.

As a TOE compliant to this Protection Profile must be able to generate evidence of its own integrity or the integrity of specific compartments, it must also implement a policy that allows itself or a compartment to verify the integrity evidence of a remote IT product, or the user data or TSF data imported from an external entity. This policy must at least allow to verify the integrity of such imported data unambiguously. This requires that the TSF is able to verify that the generation of the evidence was performed by an entity it trusts, that the evidence is verifiably bound to the data or entity in a way that can not be bypassed by an attacker and that the data is not replayed in an unauthorized way.

1.2.4.6 Secure Communication

A TOE compliant to this Protection Profile must be able to establish a trusted channel between itself and an external entity where it authenticates the communication partner and where the data transferred via this channel is protected from unauthorized modification, replay and access. This Protection Profile does not prescribe the technique used for such a trusted channel nor when such a channel has to be established. Establishing such a trusted channel to an external entity also does not imply that the TOE places any trust into the external entity except that it trusts the external entity not to misuse data used for channel establishment in a way that would allow other entities to either falsify the peer authentication, or access data transferred over the channel in a way that would compromise the integrity or confidentiality of the data transferred.

Other trust in either the external entity communicated with over the trusted channel or trust into the data transferred over this channel has to be established in other ways.

For example such a trusted channel may be used to transfer integrity evidence produced by a third party. Use of the trusted channel ensures (under the assumptions made above) that the data has not been modified during transport and could not be intercepted in way that would compromise the confidentiality of the data transmitted. Ensuring that the data transmitted has its integrity properties needs additional security attributes to be transmitted with the data that satisfy the trust policy required for the data.

The TSF must be able to set up a trusted channel between a compartment and an external entity allowing those two parties to communicate via a communication object. When setting this up the TSF has to ensure that the communication object is used in accordance with the discretionary and mandatory access control policy. The requirement to set up a trusted channel then is one security attribute that can be assigned to a communication object. The TSF in this case just ensures that the channel used for communication is set up as a trusted channel, but then does not further control the data exchanged via the trusted channel.

If a compartment receives data from an external entity that requires further security attributes to be bound to such data, it either has to implement its own checks to ensure the correctness and validity of such security attributes (which is then a function outside of the TSF) or request the TSF to check the correctness and validity of such security attributes as part of the TSF that checks the correct integrity evidence of user data received from an external entity.

In a similar way the TSF has to verify separately the integrity evidence of TSF data it receives via such a trusted channel if it requires such data to be transmitted with evidence of its integrity.

1.2.4.7 TSF protection

A TOE compliant to this Protection Profile, with the assistance of its operational environment must protect itself from unauthorized access and modification of its own code and data from both compartments as well as external entities. Any access or modification of TSF data needs to be performed in accordance with a defined policy that allows the TSF to verify that the request for access or modification is valid and that new values for TSF data are secure. This Protection Profile does not further define the policies that ensure this but leaves those to the individual TOEs that claim compliance to the PP as long as there is such a policy and as long as this policy does not bring the TSF into an insecure state.

1.2.4.8 Management of TSF functions and TSF data

A TOE compliant to this Protection Profile must define policies that regulate the conditions under which TSF functions and TSF data can be managed. The Common Criteria components defined in part 2 "bind" management activities to "authorized identified roles". Of course it also possible to bind management activities to privileges that are presented by a subject that attempts to perform management activities. Those privileges can be identified with "roles".

It is left to the individual TOEs how such roles are defined and assigned. The use of privileges provided by an external entity (e. g. as part of an attribute certificate) is not excluded in the management model compliant with the Protection Profile.

1.2.5 TOE operational environment

The TOE is assumed to operate in an environment that provides the following security functionality:

- Support for a protected start-up of the TOE

This must ensure that the TOE itself is started in a way that ensures the integrity of the TSF and the TSF data (which includes a protection against replay of old versions). In addition the operational environment must ensure that no unauthorized read access to

TSF data is possible even when the TOE is not operational. This requirement can be achieved in a number of ways. One example is a tamper-proof device that hosts the TSF, the TSF data and the function that performs the start-up process. Since the TSF itself ensure that the TSF and TSF data can not be compromised or accessed in an unauthorized way when the TOE is operational, the TSF and TSF data are continuously protected. In this example the TSF itself must contain the ability to generate evidence of their own integrity (and potentially other attributes).

Another example is the integration of a secure, tamper-proof device in the operational environment that ensures that the TSF and TSF data are not compromised before starting the TOE. In this case the tamper-proof device may be part of the integrity evidence generation function to ensure an external entity that the TOE was started by such a known, tamper-proof device and that this device has controlled that the TOE was not compromised when it was started.

- Support for verification of evidence of integrity of data received from a remote trusted IT product

As a TOE compliant to this Protection Profile must be able to generate evidence of its own integrity and the integrity of compartments, it also requires that remote trusted IT products are able to generate evidence of their own integrity or the integrity of data they submit to the TOE. The TOE may decide to import TSF data or user data only when it comes from an external entity that can present evidence of its integrity (and potentially other attributes).

2 Conformance claim

2.1 CC conformance claim

This PP claims conformance the Common Criteria as follows:

CC Version:	3.1 Revision 2
CC Part 2:	extended
CC Part 3:	conformant
Packages:	EAL5 conformant

2.2 PP claim, Package claim

This PP claims no conformance to other protection profiles. This PP claims conformance to the EAL5 package of security assurance requirements defined in CC part 3.

2.3 Conformance rationale

This PP has been developed against the most recent version of the Common Criteria to ensure its usefulness in the future. It is fully conformant to CC part 3 by selecting the EAL5 package of security assurance requirements. EAL5 was chosen as a minimum level of assurance for different reasons:

- In general, assurance requirements must be commensurate with the likelihood of an attempted security policy compromise. This likelihood increases with
 - the exposure of systems to untrustworthy and unauthorized entities; for example, mobile devices will be more exposed to attackers than systems in a well-guarded environment, but exposure through communication channels may jeopardize even systems guarded in secure vaults.
 - the value of data stored and processed by the system.

Since the architecture addressed in this PP includes systems where both factors are likely to be high, a sufficient level of assurance must be selected to provide system users with appropriate assurance that the system will be able to withstand such threats.

- The TOEs claiming conformance to this PP are expected to provide high assurance against the threats assumed in this PP. Robust and reliable separation of compartments requires a level of assurance that includes the evaluation of possible covert channels between unrelated compartments.
- The EAL5 level was also deemed appropriate because it shall provide a platform for other secure services implemented in compartments managed by the TOE. Since such services may be certified at higher assurance levels, the underlying platform must not provide weaker assurance.
- The whole architecture of a security kernel managing compartments should be implemented in a lean, modularized fashion as required by the EAL5 assurance level. In this respect, the PP authors have made a conscious design decision against large and complex implementations, although they have been striving for flexibility everywhere else.

2.4 Conformance statement

Because of the flexibility that this PP leaves developers in the implementation of systems conformant to this PP, this PP calls for “strict” conformance. The requirements stated in this PP are seen as a minimum set that every implementation must fulfil.

3 Security problem definition

Before stating the threats, objectives and assumptions, this section provides an overview of the different entities (subjects and objects) interacting in a PP-compliant TOE and the security policies to govern these interactions.

3.1 Threats

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

Assets to be protected are the data stored and managed in the compartments, the compartment code, the storage container objects, the communication objects, the resources managed by the TSF as well as TSF functions and TSF data.

There is one generic threat of violating the security policies that the system is expected to enforce. This can be achieved in different ways by a threat agent:

- Gain access to protected assets by elevating privileges
 - Impose as another subject and use its privileges (replay, defeat I&A, spoof another identity)
- Change the security policy enforced by the system, by changing the TSF data which implements the policy decisions. This can be achieved in several ways:
 - Replace the whole TOE or parts of it, thus executing untrusted code instead of the trusted TSF (including replaying old versions of the TOE)
 - planting Trojan Horses in the TOE
 - start the TOE in an insecure initial state
- Circumvent TSF controls, and therefore escape the enforcement of the security policy, by
 - Exploiting implementation errors
 - Exploiting configuration errors
 - Gaining knowledge through covert channels
 - Gaining knowledge from residual data
- Interfere with the communication between the TOE and an external entity
 - Spoof an external entity
 - Intercept communication and read or modify critical data
 - Replay all or part of previous valid communication
 - Provide false security attributes (e. g. integrity status)

Threat agents are:

- External entities not authorized to access TSF services. Those may attempt to get access to TSF services either by masquerading as an authorized entity or by attempting to use TSF services without proper authorization.
- External entities authorized to access TSF services that attempt to get access to services they are not authorized to either by misusing services they are allowed to use or by masquerading as a different external entity.

- Untrusted compartments that may attempt to get access to services they are not authorized to either by misusing services they are allowed to use or by masquerading as a different compartment.

In the following, the term 'thread agent' is used to indicate that a threat can be performed by an unauthorized external entity, an authorized external entity, or an untrusted compartment. Threat agents are assumed to have moderate level of expertise, resources and motivation. This leads to the definition of the following threats:

3.1.1 Threats to be addressed by the TOE

T.MODIFY_TSF

A threat agent may try to violate the integrity of the TSF functions or TSF data in an undetectable way resulting in a situation where security policies can be bypassed.

T.ACCESS_TSFDATA

A threat agent may read sensitive information contained in TSF data in an unauthorized way when the data is stored or transferred.

T.UNAUTHORIZED_ACCESS

A threat agent may use the TSF directly or a compartment to read or modify objects without being allowed to access the object.

T.UNAUTHORIZED_ADMIN

A threat agent may use a management functionality of the TSF to grant itself or others access to sensitive TSF data or compartment data.

T.UNAUTHORIZED_INFOFLOW

A threat agent may get access to information without being authorized for this information by the information flow control policy.

Application Note: As explained in section 1.2.4.3 a TOE compliant to this Protection Profile needs to implement an information flow control policy. This Protection Profile does not prescribe the rules of such an information flow control policy but leaves the rules that define when information flow is allowed to the developer of the Security Target. The author of a Security Target has to define the information flow control policy by defining the type of information being protected by the policy as well as the rules that allow information to flow. Any information controlled by the information flow control policy that flows in contradiction to the rules of the policy constitutes a threat and this is expressed by T.UNAUTHORIZED_INFOFLOW.

T.MANIPULATE_COMPARTMENT

A threat agent may attempt to manipulate the code or data belonging to a compartment other than itself.

T.COMMUNICATION_ACCESS

A threat agent may access the data communicated between two other compartments or between a compartment and an external entity to read or modify the information transferred.

T.FALSE_EVIDENCE

A threat agent may influence the TSF to generate false evidence of the integrity of the TSF functions, TSF data, compartment code, or compartment data.

T.REPLAY

A threat agent may introduce false information by replaying previously TFS data or compartment data. This could result in reset the state of a compartment, e.g., the licence, by replaying an older state, e.g., a backup.

T.UNACCOUNT

A threat agent may influence the TSF in a way that it may not be possible to hold a subject accountable for performed management activities or rejected attempts to perform management activities.

T.MANIPULATE_USERDATA

A threat agent may manipulate compartment data when stored or transferred without the TSF or the recipient of this data being able to detect this modification.

T.ACCESS_USERDATA

A threat agent may read information contained in compartment data in an unauthorized way when the data is stored or transferred.

T.RESOURCE_EXHAUST

A threat agent may attempt to cause denial of service by exhausting resources like CPU cycles, main memory or memory for storage container.

3.1.2 Threats to be addressed by the TOE environment

TE.MODIFY_ENVIRONMENT

An external entity may try to violate security policies by manipulate the TOE environment like (directly or indirectly) installing a device driver that uses hardware functions (e.g., direct memory access) to access or violate the integrity of TSF data or TSF functions.

TE.OUTSIDE_CONTROL

An external entity may try to access TSF data or compartment data by starting the TOE outside its intended operational environment. An example is to start the TOE on top of a software component that is under control of an adversary thereby being able to control and/or influence the functions of the TOE such that all or some SFRs are no longer enforced.

TE.FALSE_REMOTE_EVIDENCE

An external entity may produce falsified evidence of its own integrity, the integrity of TSF data or user, or the integrity of one of its compartments in a way that is not detectable by the TOE when it is received by the TOE.

3.2 Organizational security policies

P.TRUST_POLICY

An organizational security policy must exist that determines how the evidence of integrity of the TSF, TSF data, a compartment, or user data is generated. This trust policy must allow an authorized recipient of such data to verify that this data has been produced by a trusted entity. The policy must also define the conditions when such evidence is required and the authorization required to request such evidence for defined items.

P.ROLES

An organizational security policy must exist that determines how management activities are distributed among authorized roles.

3.3 Assumptions

A.HW_OK

The underlying hardware (e.g., CPU, devices, other hardware used for secure start-up or generation of integrity evidence, etc.) does not contain backdoors, is non-malicious, and behaves as specified.

A.NO_TAMPER

Physical attacks against those parts of the underlying hardware platform that support the secure start-up, the generation of integrity evidence and the support for separation are not possible in the operational environment in a way that would allow to start the TOE in an insecure way without this being detectable. As a result, physical attacks that would allow to generate false evidence not detectable by the recipient or undermine the separation support without this being detectable shall not be possible in the operational environment of the TOE.

A.INTEGRITY_SUPPORT

The IT-environment provides a mechanism that supports the TOE in producing evidence of its own integrity.

A.SEPARATION_SUPPORT

The IT-environment provides mechanisms that allow the TSF (i) to separate itself from untrusted compartments and (ii) to keep compartments separate from each other allowing sharing of resources and communication between compartments only when the TSF have explicitly allowed this.

A.BIND

The operational environment offers a mechanism that allows the TOE to store information such that it cannot be accessed by a TOE where the configuration has been manipulated in an unauthorized way. Example mechanisms that can provide this are the sealing function offered by a TPM as specified by the TCG in combination with an authenticated start-up architecture, or a tamper-resistant storage in combination with a secure start-up architecture.

A.REMOTE_TRUST

Remote IT products are assumed to provide a function the TOE trusts that is able to generate evidence of the integrity of a remote trusted IT product, its TSF data, compartments or user data and to produce this evidence only if it is correct.

A.NO_EVIL

Subjects allowed to perform administrative functions of the TOE do not misuse their privileges.

4 Security objectives

4.1 Security objectives for the TOE

O.DISCRETIONARY_ACCESS_CONTROL

The TOE will control access to objects under its control based on security attributes of the objects, the security attributes of the subject that attempts to access the object and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access has to be controlled on a discretionary basis down to individual subjects and objects.

O.INFORMATION_FLOW_CONTROL

The TOE will control information flow between different subjects under the control of the TOE based on security attributes of the subjects and potentially other TSF data (e. g. security attributes of objects). This information flow control policy must be able to allow the isolation of individual compartments from other compartments controlled by the TOE.

O.AUDIT

The TOE must be able to audit defined potentially security critical events and to record the time and, where possible, the originator of the event as well as sufficient data to identify the type of event.

O.MANAGE

The TOE must restrict all management activities to authorized subjects. The TOE must have a well-defined policy how to identify if a subject has sufficient authority to perform a management activity.

O.INTEGRITY_USERDATA

The TOE must provide a function that ensures the integrity of user data and allows to verify that user data has not been tampered with or is replayed even when the TOE is not operational or when user data is transferred.

O.CONFIDENTIALTY_USERDATA

The TOE must provide a function that allows user data to be confidentiality protected even from entities that may access the storage container with this data off-line (i. e. accessing the storage container bypassing the TSF) or when the user data is transferred.

O.INTEGRITY_COMPARTMENTS

The TOE must provide a function that is able to ensure the integrity of compartment data (code and data loaded when a compartment is started). The TOE must verify the integrity of compartments when loading them if this is requested by the policy.

O.CONFIDENTIALTY_COMPARTMENTS

The TOE must provide a function that is able to confidentiality protect compartment data (code and data loaded when a compartment is started) even from entities that may access the storage container with this data off-line (i. e. accessing the storage container bypassing the TSF).

O.INTEGRITY_EVIDENCE

The TOE must provide a function that is able to verify the integrity of the TSF itself as well as the integrity of specific compartments and/or user data. The TSF must be able to present this evidence to external entities that allows those entities to verify the integrity of the TSF itself or the integrity of specific compartments and/or user data. The evidence data must allow the external entity to verify (based on a defined trust

policy) that the data has been correctly produced and was not falsified. The TOE shall present this evidence only when the integrity of the entity has been verified and only when the requester is authorized to request such evidence.

O.EXPORT

The TOE must have a function to export user data with security attributes. The TOE shall export the security attributes of user data correctly and in a form that can not be modified before import in a way that an authorized importing entity is not able to detect. The security attributes must be exported in a way that they can be correctly interpreted by an authorized recipient that imports that user data.

O.IMPORT

The TOE must have a function to import user data with security attributes. The TOE shall not use the security attributes of imported user data unless it has verified the integrity of the security attributes, verified that the security attributes are correctly bound to the user data and that the security attributes have been defined by an external entity trusted to have set them correctly.

O.TSF_PROTECTION

The TOE shall protect the TSF and the TSF data against unauthorized access and modification.

O.COMM_PROTECT

The TOE shall be able to protect TSF and user data from unauthorized access in case they are transferred to or imported from an external entity.

O.RESOURCE_CONTROL

The TOE shall be able to limit the amount of the resources CPU cycles and main memory to defined quota that can be used by a subject.

4.2 Security objectives for the operational environment

OE.SECURE_LOAD

The operational environment shall perform checks that ensure the integrity of the TOE before or during loading it, ensures protection against replay of older versions of the TOE and ensures that the TOE code and data, when stored, loaded and executed are protected against reading or loading by unauthorized entities in the TOE environment. If the TOE is started in a different environment or if the TOE is started even when the operational environment has detected a violation of the TOE's integrity, the operational environment shall ensure that the manipulated TOE when started is not be able to generate false evidence of its own integrity and the operational environment shall also not falsely generate evidence for the integrity of the TOE when it has not successfully verified the integrity of the TOE.

OE.SECURE_OPERATION

The operational environment shall ensure that the TOE code and data (when in operation) can not be manipulated or intercepted by entities not under the control of the TOE.

OE.SEPARATION_SUPPORT

The operational environment (usually the hardware) shall provide a function that enables the TSF to separate its own code and data from those of compartments and that also allows the TSF to separate individual compartments from each other as well as the separation of storage container and communication objects from direct access by compartments or external entities.

OE.INTEGRITY_SUPPORT

The operational environment shall provide a function the TOE can use to provide a base for the generation of evidence of its own integrity.

OE.REMOTE_TRUST

The operational environment shall provide functions that the TOE can use to verify the integrity of TSF and user data it imports with the request to have evidence provided for the integrity of the data. This includes the ability to verify that no old data is replayed by an attacker.

OE.ADMINISTRATION

The operational environment shall ensure that administrative roles and privileges are carefully assigned to trusted entities and that administrative actions are performed carefully to not undermine the security policy of the TOE.

4.3 Security objectives rationale

This chapter maps the security objectives for the TOE to the threats the TOE is supposed to counter and the organizational security policies. The security objectives for the TOE environment are mapped to the threats defined for the TOE environment, the organizational security policies and the assumptions.

4.3.1.1 Security objectives for the TOE

O.DISCRETIONARY_ACCESS_CONTROL

This objective addresses the threat T.UNAUTHORIZED_ACCESS. Note that it only addresses parts of this threat. Other aspects of T.UNAUTHORIZED_ACCESS are addressed by O.INFORMATION_FLOW_CONTROL

O.INFORMATION_FLOW_CONTROL

This objective addresses the threats T.UNAUTHORIZED_INFOFLOW and T.UNAUTHORIZED_ACCESS. Access to an object in a TOE compliant to this Protection Profile is given when both the rules for the discretionary access control policy as well as the rules of the information flow control policy allow access. So T.UNAUTHORIZED_ACCESS is on the one hand also addressed by O.INFORMATION_FLOW_CONTROL. On the other hand may the rules of the information flow control policy address other potential information container and therefore those rules may span beyond the definition of access control to defined objects. Those rules then address the threat T.UNAUTHORIZED_INFOFLOW.

O.AUDIT

This objective addresses the threat T.UNACCOUNT and the threats T.MODIFY_TSF and T.MANIPULATE_USERSATA. The last two threats are addressed with respect to the threat that such an attempted manipulation may not be detected. O.AUDIT ensures that the detection of such attempts can be reported and analyzed.

O.MANAGE

This objective addresses the threat T.UNAUTHORIZED_ADMIN and the OSP P.ROLES. O.MANAGE ensures that management activities can not be performed by unauthorized subjects which counters the threat T.UNAUTHORIZED_ADMIN.

O.INTEGRITY_USERDATA

This objective addresses the threats T.MANIPULATE_USERDATA and T.REPLAY. Note that O.INTEGRITY_USERDATA explicitly mentions the prevention of replay as part of the objective.

O.CONFIDENTIALTY_USERDATA

This objective addresses the threat T.ACCESS_USERDATA. The objective requires that user data is confidentiality protected when it is no longer under the control of the TSF, e. g., when stored in a device that may be read off-line.

O.INTEGRITY_COMPARTMENTS

This objective addresses the threat T.MANIPULATE_COMPARTMENTS

O.CONFIDENTIALTY_COMPARTMENTS

This objective addresses the threat T.ACCESS_USERDATA. The objective requires that code and data loaded from a device to start a compartment is confidentiality protected. Note that the data loaded when a compartment is started contains the user data as well as TSF data for this compartment. Since the values of the TSF data may allow to deduce the content of user data (because the value of the TSF data is derived from user data), the objective requires all code and data used to load a compartment to be confidentiality protected which ensures that all user data that is part of it is confidentiality protected.

O.INTEGRITY_EVIDENCE

This objective addresses the threat T.FALSE_EVIDENCE and the OSP P.TRUST_POLICY

O.EXPORT

This objective addresses the threats T.MANIPULATE_USERDATA and T.MODIFY_TSF. The TSF data protected against manipulation by this objective are the security attributes exported together with the user data.

O.IMPORT

This objective addresses the threats T.MANIPULATE_USERDATA and T.MODIFY_TSF. The TSF data protected against manipulation by this objective are the security attributes imported together with the user data. The objective ensures that the security attributes have not been modified and are correctly bound to the user data. This ensures that an attacker can not bypass the security policy by manipulating security attributes the TSF are going to import and interpret as TSF data.

O.TSF_PROTECTION

This objective addresses the threats T.MODIFY_TSF and T.ACCESS_TSFDATA

O.COMM_PROTECT

This objective addresses the threat T.COMMUNICATION_ACCESS

O.RESOURCE_CONTROL

This objective addresses the threat T.RESOURCE_EXHAUST.

4.3.1.2 Security objectives for the TOE environment

OE.SECURE_LOAD

This objective addresses the threat TE.OUTSIDE_CONTROL and the assumption A.BIND.

OE.SECURE_OPERATION

This objective addresses the threat TE.MODIFY_ENVIRONMENT and the assumptions A.NO_TAMPER and A.HW_OK

OE.SEPARATION_SUPPORT

This objective addresses the assumption A.SEPARATION_SUPPORT

OE.INTEGRITY_SUPPORT

This objective addressed the assumptions A.INTEGRITY_SUPPORT and A.BIND

OE.REMOTE_TRUST

This security objective addresses the threat TE.FALSE_REMOTE_EVIDENCE and the assumption A.REMOTE_TRUST

OE.ADMINISTRATION

This objective addresses the assumption A.NO_EVIL and the OSP P.ROLES

5 Extended components definition

This Protection Profile defines one extended component within the family FDP_DAU defined in part 2 of the Common Criteria.

FDP_DAU.3_EXP Controlled data authentication requires that the TSF is capable of generating evidence of the integrity of defined data under defined conditions.

Management: FDP_DAU.3_EXP

The following actions could be considered for the management functions in FMT:

- The assignment or modification of the objects for which integrity evidence data generation may apply could be configurable.
- The specification of the conditions under which such data is generated could be configurable.

Audit: FDP_DAU.3_EXP

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Successful generation of integrity evidence.
- Basic: Unsuccessful generation of integrity evidence, rejected request for generating evidence.
- Detailed: The condition that allowed or disallowed the generation of evidence.

FDP_DAU.3_EXP Controlled data authentication

Hierarchical to: FDP_DAU.1

Dependencies: no dependencies

FDP_DAU.3.1_EXP The TSF shall provide a capability to generate evidence that can be used as a guarantee **of the integrity of** [assignment: *list of objects or information types*].

FDP_DAU.3.2_EXP The TSF shall generate this evidence only [assignment: *list of conditions under which the evidence is generated*].

FDP_DAU.3.3_EXP The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the **integrity** of the indicated information.

6 Security requirements

6.1 Security functional requirements

6.1.1 SFR summary

The security functional requirements included in this Protection Profile have been drawn from CC V3.1 Release 2, part 2 with the exception of FDP_DAU.3_EXP, which is an extended SFR defined above in this Protection Profile. Operations performed on the SFRs are marked in ***bold and italics***. Refinements are marked in ***bold, italics and underlined***.

The following security functional requirements are included in this Protection Profile:

SFR	Title
-----	-------

SFR	Title
FAU_GEN.1	Audit data generation
FAU_SEL.1	Security audit event selection
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic Data Authentication
FDP_DAU.3_EXP	Controlled data authentication
FDP_ETC.2	Export of user data with security attributes
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_RIP.2	Full residual information protection
FDP_SDI.1	Stored data integrity monitoring
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data for COs
FMT_MTD.2	Management of limits on TSF data
FMT_MTD.3	Secure TSF data
FMT_REV.1	Revocation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITI.1	Inter-TSF detection of modification
FPT_ITT.1	Basic internal TSF data transfer
FPT_ITT.3	TSF data integrity monitoring

SFR	Title
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TST.1	TSF testing
FRU_RSA.1	Maximum quotas
FTP_ITC.1	Inter-TSF trusted channel

6.1.2 Audit (FAU)

A TOE compliant to this PP must have a minimum audit capability that allows to record events that may be security relevant. This PP defines only those events that are mandatory to auditable. A ST author usually will extend this list with specific events the TOE needs to audit in addition to the ones defined here.

For a TOE compliant with this PP, audit events may either be stored within the TOE or may be sent to an external entity when they are generated. If a TOE compliant with this PP maintains its own storage for audit records, the component FAU_STG.1 must be included in the ST requiring the protection of the audit records.

6.1.2.1 FAU_GEN.1 Audit data generation

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

- Start-up and shutdown of the audit functions;
- All auditable events for the *not specified* level of audit; and
- **All operations that modify the security policy enforced by the TOE**
- **Rejected attempts to perform management operations**
- **Detected integrity violations of TSF or user data**
- [assignment: *other specifically defined auditable events*].

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

6.1.2.2 FAU_SEL.1 Security audit event selection

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

- **Object identity, subject identity, event type** [selection: none, user identity, host identity]
- [assignment: list of additional attributes that audit selectivity is based upon]

Rationale for refinement:

The word "none" has been added to the possible selections to indicate that it is not required to have additional items selected. This PP has already instantiated some of the possible selections from the component as defined in part 2 of the CC and the author of a ST claiming compliance to this Protection Profile may or may not decide to add additional items.

6.1.3 Communication (FCO)

No components from this class are included in this Protection Profile.

6.1.4 Cryptographic support (FCS)

Although it is very likely that a TOE that claims compliance to this Protection Profile will use cryptographic functions to provide the functionality required, this Protection Profile does not prescribe if and which cryptographic algorithms shall be used. A TOE compliant to this Protection Profile may decide which cryptographic algorithms, key generation methods and key management/key distribution methods to use based on requirements not defined in this Protection Profile. National as well as sector specific regulations may prescribe or disallow specific algorithms of key management/key distribution methods and a product that seeks compliance with this Protection Profile may define the cryptographic functions it uses based on such policies that are beyond the scope of this Protection Profile.

6.1.5 User data protection (FDP)

6.1.5.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the *compartment access control SFP* on *compartments as subjects and storage containers, communication objects* [assignment: *list of additional objects*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application note:

Persistent storage containers and communication objects must be part of the list of objects. The ST author may decide to have also other objects that are subject to this access control policy.

Rationale for refinement:

The word "additional" has been added to the possible assignments to indicate that it is not required define other objects. This PP has already instantiated some of the objects which are mandatory and the author of a ST claiming compliance to this Protection Profile may or may not decide to add additional objects that are subject to the access control policy.

6.1.5.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *compartment access control SFP* to objects based on the following:

- *Subjects:*
 - *Compartments with the following SFP-relevant security attributes:*
 - *Compartment ID*
 - *Compartment privileges*
 - *[assignment: list of information flow control security attributes]*

- *[assignment: list of other SFP-relevant security attributes for compartments]*
- *[assignment: list of other subjects controlled under the compartment access control SFP with the security attributes that are used to enforce the policy]*
- **Objects:**
 - *Storage containers with the following SFP-relevant security attributes:*
 - *Container ID*
 - *Access control list*
 - *[assignment: list of information flow control security attributes]*
 - *[assignment: list of other SFP-relevant security attributes for storage containers]*
 - *Communication objects with the following SFP-relevant security attributes:*
 - *Communication object ID*
 - *Access control list*
 - *[assignment: list of information flow control security attributes]*
 - *[assignment: list of other SFP-relevant security attributes for communication objects]*
 - *[assignment: list of other objects controlled under the compartment access control SFP with the security attributes that are used to enforce the policy]*

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

- *Access of a subject to a storage container or communication object is allowed when the requested mode of access is allowed for the compartment by the access control list and there is no explicit entry in the access control list that forbids access for the compartment in the requested mode*
- *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].*

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

Application note:

This PP deliberately does not specify the access control rules for the discretionary access control policy between compartments and the objects in further detail, nor does it specify the structure and expressiveness of the ACLs. Those rules as well as additional capabilities of the ACLs need to be defined in a ST that claims compliance with this PP. This applies e. g. for specific rules based on subject privileges, rules in case of conflicting ACL entries, rules for specific TOE modes, ACL entries for groups of subjects, conditional ACLs etc. When the author of a ST that claims compliance to this PP adds additional subjects and/or objects, he has to specify the specific rules for those. As written in the SFR when the author of an ST adds additional subjects that are allowed to access storage container or communication objects, it must be possible to include those subjects in the ACLs and those subjects must also be bound by the access control restrictions defined in the object's ACL for those subjects.

This is for example the case when a TOE compliant to this PP allows external entities to directly access objects controlled by the SFP (i. e. without doing it via a compartment). In this case external entities have to be defined as a subject controlled by this SFP and the ACLs must allow to define the access rights those subjects have to the object.

6.1.5.3 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *storage containers*.

FDP_DAU.1.2 The TSF shall provide *compartments and external entities* with the ability to verify evidence of the validity of the indicated information.

Application note:

The validity of the storage container needs to include the integrity of the container as well as the "freshness", i. e. ensure that no old version of a valid container is presented. The TSF have to include a function that either on request of a compartment or by default generates the data required to check the validity of a storage container when a storage container is created and/or updated.

It is left to the individual TOEs claiming compliance with this Protection Profile how to implement this requirement. Especially it is left to each TOE if this requirement is by default implemented for each storage container or if it applies to dedicated storage container only. In the later case the Security Target has to specify how the containers for which this requirement applies are selected. Examples are:

By specification performed by an authorized administrator

By specification when the storage container is created

By rules defined through the SFPs (e. g. container with a specific security label are automatically protected for their data authenticity)

The Security Target has to specify the rules applied by the TSF to decide if a specific storage container is subject to this SFR.

Whenever the policy defines a storage container as being protected by this requirement, the TSF need to ensure the integrity of the storage container (including protection against replay of an old version). This requires that a subject allowed to open such a storage container can be assured that the container is as it was the last time a subject has modified a container. In the case the TSF detect an unauthorized modification, the decision how this is handled is left to the TOE design. In any case the subject that attempts to access a storage container that has been modified needs to be informed about this. It is left to the designer of a TOE if it still allows the subject to access the container or if it rejects all subjects access to such a container. A valid policy would for example be to allow specifically authorized subjects to read the content of such a container in order to analyze what unauthorized modifications have been performed.

When generating the evidence of the integrity of a compartment the TSF shall do this in a way that when this information (together with the content of the storage container) is sent by the compartment to an external entity, it allows the external entity to validate the integrity of the data (eventually in combination with the generation of evidence of the integrity of the TSF itself).

6.1.5.4 FDP_DAU.3_EXP Controlled data authentication

Hierarchical to: FDP_DAU.1

Dependencies: no dependencies

FDP_DAU.3.1_EXP The TSF shall provide a capability to generate evidence that can be used as a guarantee of the integrity of *the TSF, a compartment, or user data*.

FDP_DAU.3.2_EXP The TSF shall generate this evidence only *when it has verified the authority of the requester to request the generation of the evidence and when it has verified the integrity of the object the request has targeted.*

FDP_DAU.3.3_EXP The TSF shall provide *external entities* with the ability to verify evidence of the **integrity** of the indicated information.

Application note:

This SFR shall allow external entities to request the generation of evidence for the integrity of either of the TSF alone, dedicated compartment or dedicated user data. It is up to the implementation of a specific TOE if this also requires the support of an entity in the operational environment of the TOE to provide the integrity information in a way that allows the requesting external entity to validate the correctness of the information. In the case where the TOE is started from a tamper-proof device a self-attestation of the TSF may be sufficient for an external entity to establish the required trust in the integrity of the TSF itself. In the case of a tamper-proof device, the abstract machine test shall provide the TSF with sufficient evidence for its own integrity. In the case of a device in the operational environment of the TOE that supports the generation of the evidence for integrity of the TSF, a compartment or user data, it is up to this device to generate the information only when the integrity of the TSF has not been violated. A TOE with manipulated TSF code or data would then not be able to provide an external entity with a complete chain of trust going down to the generation of integrity evidence by the operational environment.

6.1.5.5 FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the *compartment access control policy and the kernel information flow policy* when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*].

6.1.5.6 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the *kernel information flow control SFP* on *compartments, external entities* [assignment: *list of other subjects and information*] and all operations that cause that information to flow to and from subjects covered by the SFP.

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

6.1.5.7 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *kernel information flow control SFP* based on the following types of subject and information security attributes: *compartments as subjects, storage containers and communication objects as objects and information flow control security attributes assigned to the subjects and objects* [assignment: *list of other subjects and information controlled under the indicated SFP, and for each, the security attributes*].

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

the security attribute-based relationship between two subjects such that information flow between the subjects is not permitted.

- FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].
- 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: ***no information flow shall be possible between subjects when the security attribute-based relationship or the rules of FDP_IFF.1.4 between the subjects do not permit information flow*** [assignment: ***other*** rules, based on security attributes, that explicitly deny information flows].

Application note:

A TOE compliant with this PP needs to support some kind of information flow control policy that at least allows to completely separate different compartments from each other.

6.1.5.8 FDP_ITC.2 Import of user data with security attributes

- FDP_ITC.2.1 The TSF shall enforce the ***compartment access control SFP and the kernel information flow control SFP*** when importing user data, controlled under the SFP, from outside of the TOE.
- FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.
- FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
- FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
- FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

6.1.5.9 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, deallocation of the resource from*] all objects.

Application note:

This requirement applies to resources capable to store information assigned to storage containers, storage resources assigned to communication objects as well as storage containers assigned to potentially additional objects defined in a ST compliant to this PP. This requirement also applies to resources capable of storing information assigned to compartments (e. g. memory regions assigned to a compartment, but also to processor registers when a processor is deallocated from a compartment and assigned to another compartment).

6.1.5.10 FDP_SDI.1 Stored data integrity monitoring

- FDP_SDI.1.1 The TSF shall monitor user data stored in containers controlled by the TSF for ***modifications, replay of old versions*** [assignment: ***other*** integrity errors] on all ***storage containers***, based on the following attributes: ***policy decision for integrity protection of the container*** [assignment: ***other*** user data attributes].

Application note:

This SFR is restricted to storage container objects and allows a TOE claiming compliance to this Protection Profile to define its own policy rules that decide when a storage container is protected for stored data integrity monitoring. The requirement in this Protection Profile is that a TOE compliant to this PP has such a policy. Protecting all storage containers at all times by

default is an acceptable policy compliant with this SFR. In the case the integrity protection of a storage container can be individually selected, the author of a ST compliant to this PP has to add an SFR for the management of this attribute that defines who can set and/or modify this security attribute of a storage container. This management has to be restricted to an authorized administrative role.

6.1.5.11 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the *compartment access control SFP and the kernel information flow control SFP* to be able to *transmit and receive* user data in a manner protected from unauthorised disclosure.

6.1.5.12 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the *compartment access control SFP and the kernel information flow control SFP* to be able to *transmit and receive* user data in a manner protected from *modification* [selection: *none*, *deletion*, *insertion*, *replay*] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification* [selection: *none*, *deletion*, *insertion*, *replay*] has occurred.

Rationale for refinement:

The word "none" has been added to the possible selections to indicate that it is not required to have additional items selected. This PP has already instantiated some of the possible selections from the component as defined in part 2 of the CC and the author of a ST claiming compliance to this Protection Profile may or may not decide to add additional items.

6.1.6 Identification and Authentication (FIA)

A TOE compliant to this PP has at least two types of entities that can request services from the TOE: compartments and external entities. Compartments are fully managed by the TOE and therefore do not need to be authenticated. External entities may need to be authenticated when the TOE provides services that depend on the identity of the external entity.

The TOE does always require a mechanism to verify the authorization of a service request from external entities. The verification mechanism may, however, be implemented in different ways. Some examples are

- Access through a dedicated device, e.g. the system console; in this case, the organizational environment must ensure that only authorized personnel can use the device.
- Authorization with a ticket, as e.g. in Kerberos; the TOE needs to verify the validity of the ticket, but does not necessarily need to know who presents the ticket.
- Identification and authentication of a user, and association of the user ID with a set of privileges, probably mediated by a role assigned to the user.

Only in cases where privileges are associated with an external entity, and service requests are made on behalf of this entity, the TOE needs to authenticate the identity of this "user". If such an implementation is chosen, the ST must claim the following SFRs of the FIA class:

6.1.6.1 FIA_ATD.1 User attribute definition

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

- a) *User identity*
- b) *User role(s)*

c) *User information flow control security attributes*

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

Application note:

A TOE compliant to this PP has at least two types of entities that can request services from the TOE: compartments and external entities. Compartments are fully managed by the TOE and therefore do not need to be authenticated. External entities may need to be authenticated when the TOE provides services that depend on the identity of the external entity. The Common Criteria allow to differentiate between "users" and "subjects" where a user may be bound to a subject. Access control policies are then defined for "subjects". In the type of products this Protection Profile targets, the classical "user" may not exist:

- Requests to the TSF may be submitted by compartments, which may not be "bound" to a local or remote user. An example is a legacy operating system operating within a compartment of a TOE compliant with this Security Target. Although there may be "users" managed by and operating on this legacy operating system, those users are not relevant for the security policy of the TOE targeted by this Protection Profile, since the TOE does not trust the legacy operating system. For the TOE it is just the compartment that requests a service.
- Requests to the TSF may be submitted by an external entity directly to the TSF (e. g. a request for access to a storage container or communication object, a request to perform a management activity, or a request for the generation of evidence of integrity for the TSF itself). Such requests will then be served by the TSF in accordance with its policy based on the identity of the external entity and the security attributes (which are partly mapped to roles) the external entity has.

Although this Protection Profile does not require that "users" can be bound to "subjects", a TOE compliant with this Protection Profile may still implement such a user-subject binding. An example is an external user that, after being successfully identified and authenticated, is then bound by the TSF to a compartment. All request this compartment submits to the TSF are then treated as if they were submitted by the external user. This resembles the case where a compartment acts as a proxy for the external user.

It is also worth to be noted that the authentication requested for an external user needs just to be sufficient to allow the TSF to assign the correct security attributes to this external user. An example would be an external user (potentially previously unknown to the TSF) that presents credentials issued by a party the TSF trusts and where the TSF can clearly verify that those credentials are correct and are correctly "bound" to the user presenting them. In this case the "user" is assumed to be identified and authenticated and the TSF will honor requests by such a user in accordance with the security attributes (including roles) it assign to this user based on the credentials he has presented.

6.1.6.2 FIA_UAU.1 Timing of authentication

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

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

6.1.6.3 FIA_UID.1 Timing of identification

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

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

Application note:

An ST compliant to this PP may define TSF-mediated actions allowed for an external user before this user is identified. For example a TOE may allow unidentified (anonymous) users to query some public data from the TOE, e. g. data that would allow the external user to identify the TOE. Such actions shall not provide the external user with any data protected under the SFPs enforced by the TOE.

6.1.6.4 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each **compartment** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note:

A compartment is an active entity within the TOE that is started and controlled by the TSF. Compartments therefore do not need to be authenticated and the TSF will need to keep the identity of a compartment it has started such that this identity can be associated with any service request the compartment issues to the TSF.

6.1.7 Security management (FMT)

6.1.7.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions **audit, compartment access control SFP, kernel information flow control SFP, stored data integrity policy, import of user data, export of user data, user identification and authentication**, [assignment: *list of other functions*] to [assignment: *the authorised identified roles*].

Application note:

The list above contains some policies where the author of a ST compliant to this PP has decided to enforce the policy by default (stored data integrity policy) and where he does not allow any management of the security functions behavior. This is still viewed as compliant to this PP, since the fact that nobody is able to change the behavior of a function in any way is viewed as compliant with this requirement.

In many STs that claim compliance to this PP the management of different functions will be assigned to different roles. Those STs should than have multiple instances of FMT_MOF.1 defining for each role what it is allowed to manage. A ST is conformant to this PP, when the roles are defined for the complete list of functions defined in FMT_MOF.1 in the PP.

6.1.7.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **compartment access control SFP and the kernel information flow control SFP** to restrict the ability to **change_default, modify, delete** [selection: **none**, *query*, [assignment: *other operations*]] the security attributes **user roles, security attributes of storage container, security attributes of communication objects**, [assignment: *list of other security attributes*] to [assignment: *the authorised identified roles*].

Application note:

In many STs that claim compliance to this PP the management of different security attributes will be assigned to different roles. Those STs should than have multiple instances of FMT_MSA.1 defining for each role what it is allowed to manage. A ST is conformant to this PP, when the roles are defined for the complete list of functions defined in FMT_MOF.1 in the PP.

6.1.7.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *the security attributes of user roles, security attributes of storage containers, security attributes of communication objects*, [assignment: *list of other security attributes*].

6.1.7.4 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the *compartment access control SFP and the kernel information flow 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*] to specify alternative initial values to override the default values when an object or information is created.

Application note:

Restrictive means:

For the compartment access control policy SFP the default security attributes for this policy (ACLs and potentially other ones) for a newly created object have to be defined such that initially access is restricted to the creator and potentially some authorized identified roles.

For the kernel information flow control policy the default security attributes for this policy have to be defined for a newly created object such that the object can not be used to violate the information flow control policy rules when used after creation.

For new subjects the default security attributes of the subject have to be defined to not include authorized roles not automatically required and not include values for security attributes relevant for the kernel information flow SFP that would allow the creator of the subject, the created subject or another untrusted subject to violate the kernel information flow security policy.

6.1.7.5 FMT_MTD.1(1) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, modify, delete* [selection: *none query, clear*, [assignment: *other operations*]] the *access control lists of objects, security attributes of subjects* [assignment: *list of other TSF data*] to [assignment: *the authorised identified roles*].

Application note:

Usually a Security Target compliant with the PP will require multiple instances of the FMT_MTD.1 to express the different rules for different types of operation on different TSF data. This PP does not define specific TSF data where those operations need to be managed by authorized roles. The only requirement is that whenever TSF data is able to be managed directly by a user the management function to do this has to be restricted to an authorized role. This could also be the role of an "object owner", who is allowed to perform some defined management operations on security attributes of the object he owns.

6.1.7.6 FMT_MTD.1(2) Management of TSF data for COs

FMT_MTD.1.1 The TSF shall restrict the ability to *define, change_default, modify, delete* [selection: *none query, clear*, [assignment: *other operations*]] the *security attributes of communication objects* to [assignment: *the authorised identified roles*].

Application note:

Communication objects must have specific security attributes that define the characteristics of those objects. Such attributes must include a characterization of the entities a compartment that access to such a communication object can communicate with using the device. They may also include a characterization of the protection of the communication link established using this device. For example a communication object may have an attribute "trusted channel" where the

TSF then enforce that every communication link established via this communication object over a physical link viewed as insecure is secured by TSF functions to provide integrity protection, confidentiality protection and authentication of the end point of the insecure link. Other examples of possible (but not mandatory) security attributes of communication objects are:

Filter rules for the communication

Address translation

A ST that claims compliance to this PP needs to define the security attributes it supports for communication objects, define their effect when used and define the authorized identified roles that are allowed to manage those security attributes.

Rationale for refinement:

The word "none" has been added to the possible selections to indicate that it is not required to have additional items selected. This PP has already instantiated some of the possible selections from the component as defined in part 2 of the CC and the author of a ST claiming compliance to this Protection Profile may or may not decide to add additional items.

6.1.7.7 FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for *memory assigned to a compartment, CPU time assigned to a compartment* [assignment: *list of other TSF data*] to [assignment: *the authorised identified roles*].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: *actions to be taken*].

Application note:

The actions taken by a TOE compliant to this PP when a compartment runs out of the resources assigned to it are deliberately not specified in this PP. Actions defined by the author of a ST compliant to this PP may not include an automated assignment of additional resources unless this has explicitly been specified by an authorized role.

6.1.7.8 FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for *memory assigned to a compartment, CPU time assigned to a compartment* [assignment: *list of other TSF data*].

6.1.7.9 FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke the security attributes *user roles, security attributes of storage container, security attributes of communication objects*, [assignment: *list of other security attributes*] associated with the *subjects and objects*, [assignment: *other additional resources*] under the control of the TSF to [assignment: *the authorised identified roles*].

FMT_REV.1.2 The TSF shall enforce the rules [assignment: *specification of revocation rules*].

6.1.7.10 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: *management of audit events*, [assignment: *list of other management functions to be provided by the TSF*].

6.1.7.11 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*].

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

Application note:

This PP does not define a specific role model. Instead it deliberately leaves the role model open for the specific TOE claiming compliance with this PP. The only requirement is that such a role model exists and that at least the functions implementing the SFRs that refer to authorized roles have those roles defined in FMT_SMR.1.

6.1.8 Protection of the TSF (FPT)

6.1.8.1 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: ***any modification with a probability of at least $1-10^{-10}$*** .

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform ***an audit of the event*** if modifications are detected.

Application note:

A TOE compliant to this PP needs to provide a function that can protect TSF data when exported to another trusted IT product or when stored in a container where modifications by entities external to the TOE can not be excluded. So this requirement also applies for TSF data "transmitted" to the TOE itself via some untrusted entity (e. g. a disk that may be manipulated when the TOE is shut down). The TOE may reject the modified TSF data as a response to the audit. However, in some cases users may want to accept modified TSF data, e.g., after a software update. In this case, the audit allows to detect this kind of manipulation.

6.1.8.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from ***modification and disclosure*** when it is transmitted between separate parts of the TOE.

Application note:

The inclusion of this requirement does not imply that the TSF have to be distributed. Instead the TSF may be "separated" by time when it is started. This requirement then states that modification of TSF data between two different starts of the TOE must be detectable and that the TSF data is confidentiality protected. If the TSF is distributed, this requirement applies the also for TSF data transmitted between different parts of the TSF.

6.1.8.3 FPT_ITT.3 TSF data integrity monitoring

FPT_ITT.3.1 The TSF shall be able to detect ***modification of data, substitution of data, replay of old data*** , [assignment: *other integrity errors*]] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: ***audit the event*** [assignment: *specify the additional action to be taken*].

Application note:

The inclusion of this requirement does not imply that the TSF have to be distributed. Instead the TSF may be "separated" by time when it is started. This requirement then states that modification, substitution of TSF data as well as replay of old TSF data between two different starts of the TOE must be detectable. If the TSF is distributed, this requirement applies the also for TSF data transmitted between different parts of the TSF.

6.1.8.4 FPT_STM.1 Reliable time stamps

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

6.1.8.5 FPT_TDC.1 Inter-TSF basic TSF data consistency

- FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *integrity evidence, information flow control related security attributes* [assignment: *list of other TSF data types*] when shared between the TSF and another trusted IT product.
- FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Application note:

At least integrity evidence and information flow control related security attributes need to be in a form agreed upon with the trusted IT product that is going to receive this data. In the same way a TOE compliant with the Protection Profile must be able to interpret such data received from another trusted IT product correctly. This requirement needs to be extended to other TSF data when the TOE is able to export user data with its security attributes or other TSF data than just the data mentioned in the SFR.

6.1.8.6 FPT_TST.1 TSF testing

- FPT_TST.1.1 The TSF shall run a suite of self tests *when loading a compartment that requires integrity evidence* to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].
- FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF data].
- FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Application Note:

If only parts of the TSF are chosen, ST authors need to ensure that the partial test is sufficient to provide the required trust in the integrity evidence.

6.1.9 Resource utilisation (FRU)

6.1.9.1 FRU_RSA.1 Maximum quotas

- FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: *processor time, memory* [assignment: *other controlled resources*] that *subjects* can use [selection: simultaneously, over a specified period of time].

6.1.10 Trusted path/channel (FTP)

6.1.10.1 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 disclosure.
- FTP_ITC.1.2 The TSF shall permit *the TSF or 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 *communication of an external entity to the TSF, a compartment initiating a communication link via a communication object to an external entity where the policy for the communication object requires a trusted channel* [assignment: *list of other functions for which a trusted channel is required*].

Application Note:

A trusted channel only establishes trust in the channel, not trust in the peers using the channel. A trust relationship between the peers using the channel, if required, must be established in addition. If this is required, the trusted channel may be used to exchange the credentials used to establish the trust.

6.2 Security assurance requirements

The security assurance requirements of this Protection Profile are those defined for the assurance level EAL5 in part 3 of Common Criteria version 3.1.

6.3 Security requirements rationale

6.3.1 Tracing security objectives to security functional requirements

This section traces each security objective for a TOE compliant to this Protection Profile to the security functional requirements implementing the objective.

O.DISCRETIONARY_ACCESS_CONTROL

The TOE will control access to objects under its control based on security attributes of the objects, the security attributes of the subject that attempts to access the object and the type of access attempted. The rules that determine access may be based on the value of other TSF data. Access has to be controlled on a discretionary basis down to individual subjects and objects.

This security objective is implemented by the SFRs FDP_ACC.2 and FDP_ACF.1 in the following way:

FDP_ACC.2 requires that a discretionary access control policy must be implemented that controls access of at least compartments and external entities as subjects to at least storage container and communication objects as objects. This access control policy must cover all the operations defined between those subjects and objects. It is left to individual Security Targets claiming compliance to this PP to define additional subjects and/or objects that are subject to the rules of this discretionary access control policy.

FDP_ACF.1 then requires that the rules that determine access are based on the subject identity and subject security attributes as well as the object identity and object security attributes. The object security attributes need to include an access control list in some form. The precise rules of the discretionary access control policy are not defined in the PP but left to the author of an ST claiming compliance to this PP, as long as it possible to define access down to individual subjects.

O.INFORMATION_FLOW_CONTROL

The TOE will control information flow between different subjects under the control of the TOE based on security attributes of the subjects and potentially other TSF data (e. g. security attributes of objects). This information flow control policy must be able to allow the isolation of individual compartments from other compartments controlled by the TOE.

This security objective is implemented by the SFRs FDP_IFC.2 and FDP_IFF.1 in the following way:

FDP_IFC.2 requires that an information flow control policy must be implemented that controls the information flow between at least compartments and external entities as subjects between which information flow is controlled. If a TOE compliant to this PP includes other subjects, the information flow control policy needs to cover also those subjects (FDP_IFC.2.2).

FDP_IFF.1 then requires that the rules that determine information flow is based on the subject and object information flow related security attributes. It is mandatory that those rules allow to

completely isolate specific compartments within the TOE (no information flow within the TOE is allowed to any other compartment controlled by the TOE). Other rules as well as the structure and content of the information flow related security attributes and how they are evaluated as part of the information flow control rules is left to a TOE claiming conformance to this Protection Profile.

This deliberately allows for the implementation of very different information flow policies. In the simplest form it would implement just a simple separation policy based on a single security attribute, where compartments are allowed to communicate only when the value of this attribute is the same for the compartments. A more complex example is the implementation of a mandatory access control policy based on the Bell-LaPadula model [BLP]. Other more complicated models may base the information flow rules on security properties received by remote entities together with their evidence of integrity and assigned to compartments, thus allowing an external trusted entity to control the information flow within the TOE.

O.AUDIT

The TOE must be able to audit defined potentially security critical events and record the time and, where possible, the originator of the event as well as sufficient data to identify the type of event.

This security objective is implemented by the SFRs FAU_GEN.1 and FAU_SEL.1, supported by FMT_SMF.1 and FPT_STM.1. The security objective is met in the following way:

FAU_GEN.1 requires that a TOE compliant to this PP is able to generate audit minimum list of critical events, which can be extended by a ST that claims compliance with this PP. For each of this events the TSF is required to include the data that is at least required to perform a useful analysis of the audit record. Other data (including event specific data) may be added by the author of a ST claiming compliance to this PP.

FAU_SEL.1 then requires that it is possible to define which of the events a TOE compliant to this PP is able to audit are actually audited. It must be able to base this selection on the object identity, subject identity and the event type. This allows to audit just those events that are viewed to be critical in a given situation. The author of a ST claiming compliance with this PP may add additional criteria that allow to have a more fine grained way of selecting the audit records that are actually generated.

FMT_SMF.1 requires that only an authorized role is able to define the events that are audited (selection criteria are defined in FAU_SEL.1).

FPT_STM.1 allows a TOE compliant with this PP to include the correct time and date in the audit record.

O.MANAGE

The TOE must restrict all management activities to authorized subjects. The TOE must have a well-defined policy how to identify if a subject has sufficient authority to perform a management activity.

This security objective is implemented by the SFRs FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FIA_UID.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.2, FMT_REV.1, FMT_SMF.1, FMT_SMR.1 in the following way:

FIA_ATD.1 supports management by allowing to assign user (subject) security attributes which include the user roles.

FIA_UAU.1, FIA_UID.1 and FIA_UID.2 support management by allowing to identify the user (subject) and thereby assigning the correct security attributes that define the management activities allowed for the subject.

FMT_MOF.1 requires that any change in the behavior of any of the security functions is restricted to an authorized role. The author of a ST claiming compliance with this PP may assign different roles to different management activities related to FMT_MOF.1 (using multiple instantiations of FMT_MOF.1) as long as all the security functions where that have a behavior that can be managed are covered.

FMT_MSA.1 requires that all operations that in some way modify security attributes related to the security function policies of entities managed by the TSF can only be performed by an authorized role. Similar to FMT_MOF.1, the author of a ST claiming compliance with this PP may assign different roles to different management activities related to FMT_MSA.1 (using multiple instantiations of FMT_MSA.1) as long as modifications to all the security attributes are covered.

FMT_MSA.2 supports management by requiring that only secure values are accepted for security attributes.

FMT_MSA.3 requires that any change to the default values of security attributes can only be performed by an authorized role.

FMT_MTD.1(1) requires that specific TSF data is only modifiable by authorized roles.

FMT_MTD.1(2) is related to specific security attributes of communication objects (which are not related to a SFP). In addition to what FMT_MTD.1(1) requires for other TSF data, also the definition of the security attributes of communication objects is required to be restricted to authorized roles.

FMT_MTD.2 requires that the management of resource limits is restricted to authorized roles.

FMT_REV.1 requires that revocation of security attributes associated with the subjects and objects is restricted to authorized roles. This implies that in the case a ST defines additional subject and objects, FMT_REV.1 also must apply to those for the revocation of security attributes.

FMT_SMF.1 requires that the management of audited events is restricted to authorized roles.

O.INTEGRITY_USERDATA

The TOE must provide a function that ensures the integrity of user data and allows to verify that user data has not been tampered with even when the TOE is not operational.

This security objective is implemented by the SFRs FDP_DAU.1, FDP_DAU.3_EXP, FDP_SDI.1, FDP_UIT.1 and FTP_ITC.1 in the following way:

FDP_DAU.1 requires that a TOE compliant with this Protection Profile is able to generate evidence of the integrity of user data stored in storage container.

FDP_DAU.3_EXP requires that a TOE compliant with this Protection Profile is able to generate evidence of the integrity of (among other) compartments and user data upon request of an authorized external entity.

FDP_SDI.1 requires that a TOE compliant with this Protection Profile protects the integrity of user data with respect to modification and replay.

FDP_UIT.1 requires that a TOE compliant with this Protection Profile protects user data, when transmitted or received, against modification.

FTP_ITC.1 requires that a TOE compliant with this Protection Profile protects the integrity of data transferred via a trusted channel.

O.CONFIDENTIALTY_USERDATA

The TOE must provide a function that allows user data to be confidentiality protected even from entities that may access the storage container with this data off-line (i. e. accessing the storage container bypassing the TSF).

This security objective is implemented by the SFRs FDP_RIP.2 and FDP_UCT.1 in the following way:

FDP_RIP.2 ensures that user data is not passed in an unauthorized way when a resource that contains user data and has been released is assigned to a new object.

FDP_UCT.1 ensures that user data can be confidentiality protected when transmitted or received.

In addition of course also the information flow control policy implemented by the SFRs FDP_IFC.1 together with FDP_IFF.1 ensure that it is possible to prohibit information flow between subjects, thus allowing to keep user information confidential in accordance with the rules of the information flow control policy.

O.INTEGRITY_COMPARTMENTS

The TOE must provide a function that is able to ensure the integrity of compartment data (code and data loaded when a compartment is started). The TOE must verify the integrity of compartments when loading them if this is requested by the policy.

This security objective is implemented by the SFRs FPT_ITT.1 and FPT_ITT.3 in the following way:

FPT_ITT.1 ensures that TSF data (which includes compartments) is integrity protected between different start-ups of the TOE as well as when transferred between different part of the TSF (in the case the TSF is distributed).

FPT_ITT.3 ensures that it is not possible modify or substitute TSF data or replay old versions of TSF data between different start-ups of the TOE as well as when transferred between different part of the TSF (in the case the TSF is distributed).

O.CONFIDENTIALTY_COMPARTMENTS

The TOE must provide a function that is able to confidentiality protect compartment data (code and data loaded when a compartment is started) even from entities that may access the storage container with this data off-line (i. e. accessing the storage container bypassing the TSF).

This security objective is implemented by the SFR FPT_ITT.1 in the following way:

FPT_ITT.1 ensures that TSF data (which includes compartments) is confidentiality protected between different start-ups of the TOE as well as when transferred between different part of the TSF (in the case the TSF is distributed).

O.INTEGRITY_EVIDENCE

The TOE must provide a function that is able to verify the integrity of the TSF itself the integrity of specific compartments and/or user data. The TSF must be able to present this evidence to external entities that allows those entities to verify the integrity of the TSF itself, the integrity of specific compartments and/or user data. The evidence data must allow the external entity to verify (based on a defined trust policy) that the data has been correctly produced and was not falsified. The TOE shall present this evidence only when the integrity of the entity has been verified and only when the requester is authorized to request such evidence.

This security objective is implemented by the SFR FDP_DAU.3_EXP in the following way:

FDP_DAU.3_EXP ensures that an external entity, provided it is authorized to issue the request, can obtain data that allows it to verify the integrity of the TSF, specific compartments or user data.

O.EXPORT

The TOE must have a function to export user data with security attributes. The TOE shall export the security attributes of user data correctly and in a form that can not be modified before import in a way that an authorized importing entity is not able to detect. The security attributes must be exported in a way that they can be correctly interpreted by an authorized recipient that imports that user data.

This security objective is implemented by the SFRs FDP_ETC.2 and FPT_TDC.1 in the following way:

FDP_ETC.2 ensures that the TOE is able to export user data with its associated security attributes. The Protection Profile does not define all the security attributes that may be assigned to user data, but at least its integrity status and the information flow related security attributes need to be exportable together with the user data.

FPT_TDC.1 ensures that the security attributes are exported in a way that allows the recipient to correctly interpret them.

O.IMPORT

The TOE must have a function to import user data with security attributes. The TOE shall not use the security attributes of imported user data unless it has verified the integrity of the security attributes, verified that the security attributes are correctly bound to the user data and that the security attributes have been defined by an external entity trusted to have set them correctly.

This security objective is implemented by the SFRs FDP_ITC.2 and FPT_TDC.1 in the following way:

FDP_ITC.2 ensures that the TOE is able to import user data with its associated security attributes. The Protection Profile does not define all the security attributes that may be assigned to user data, but at least its integrity status and the information flow related security attributes need to be importable together with the user data.

FPT_TDC.1 ensures that the security attributes imported can be correctly interpreted.

O.TSF_PROTECTION

The TOE shall protect the TSF and the TSF data against unauthorized access and modification.

This security objective is implemented by the SFRs FMT_MTD.3, FPT_ITI.1, FPT_ITT.1, FPT_TDC.1, and FPT_TST.1 in the following way:

FMT_MTD.3 ensures that only secure values are accepted for TSF data. This protects the TSF from being corrupted by insecure values of TSF data.

FPT_ITI.1 ensures that modifications of TSF data during transmission are detected.

FPT_ITT.1 ensures that TSF data is protected when being transferred.

FPT_TDC.1 ensures that security attributes that are imported are correctly interpreted such that the TOE can not be corrupted due to the false interpretation of imported security attributes.

FPT_TST.1 ensures that compartments that require integrity protection are checked when loaded.

O.COMM_PROTECT

The TOE shall be able to protect TSF and user data from unauthorized access in case they are transferred to or imported from an external entity.

This security objective is implemented by the SFRs FDP_UCT.1, FDP_UIT.1, FPT_ITI.1, FPT_ITT.1 and FPT_ITC.1 in the following way:

FDP_UCT.1 and FDP_UIT.1 ensure the confidentiality and integrity of user data during transfer
 FPT_ITI.1 ensures the integrity of TSF data during transfer to an external entity
 FPT_ITT.1 ensures the protection of data during transfer between different parts of the TSF
 FTP_ITC.1 ensures that the TSF is able to establish a trusted channel to remote trusted IT product that can be used to securely transfer TSF and user data.

O.RESOURCE_CONTROL

The TOE shall be able to limit the amount of the resources CPU cycles and main memory to defined quota that can be used by a subject.

This security objective is implemented by the SFRs FMT_MTD.2 and FRU_RSA.1 in the following way:

FMT_MTD.2 allows an authorized administrator to define quotas for CPU cycles and main memory that a subject is allowed to use.

FRU_RSA.1 enforces that a subject can not use more of those resources than the quota assigned to it.

6.3.2 Security requirements dependency analysis

This section addresses the dependencies of the security functional requirements and checks if they are resolved.

SFR	Dependencies	Resolved?
FAU_GEN.1	FPT_STM.1	yes
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	yes
FDP_ACC.2	FDP_ACF.1	yes
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	yes
FDP_DAU.1	-	n/a
FDP_DAU.3_EXP	-	n/a
FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	yes
FDP_IFC.2	FDP_IFF.1	yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	yes
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1	yes
FDP_RIP.2	-	n/a
FDP_SDI.1	-	n/a
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	yes
FDP_UIT.1	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	yes
FIA_ATD.1	-	n/a

SFR	Dependencies	Resolved?
FIA_UAU.1	FIA_UID.1	yes
FIA_UID.1	-	n/a
FIA_UID.2	-	n/a
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	yes
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	yes
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	yes
FMT_MTD.1(1)	FMT_SMR.1, FMT_SMF.1	yes
FMT_MTD.1(2)	FMT_SMR.1, FMT_SMF.1	yes
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	yes
FMT_MTD.3	FMT_MTD.1	yes
FMT_REV.1	FMT_SMR.1	yes
FMT_SMF.1	-	n/a
FMT_SMR.1	FIA_UID.1	yes
FPT_ITI.1	-	n/a
FPT_ITT.1	-	n/a
FPT_ITT.3	FPT_ITT.1	yes
FPT_STM.1	-	n/a
FPT_TDC.1	-	n/a
FPT_TST.1	-	n/a
FRU_RSA.1	-	n/a
FTP_ITC.1	-	n/a

This table shows that all the dependencies between security functional requirements are satisfied. The dependencies between the security assurance requirements are satisfied because of the selection of the EAL5 package of security assurance requirements, which has all its dependencies satisfied. There are no dependencies of security functional requirements to security assurance requirements for any security functional requirement included in this Protection Profile and there are no dependencies of security assurance requirements within the EAL5 package to security functional requirements.

Therefore all dependencies as defined in the CC are satisfied.

7 References

- [BLP] David E. Bell, Leonard J. La Padula: Secure Computer System: Unified Exposition and Multics Interpretation, ESD-TR-75-306, The MITRE Corporation, March 1976
- [CC-Part1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2006 Version 3.1 Revision 1, CCMB-2006-09-001
- [CC-Part2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2007, Version 3.1 Revision 2, CCMB-2007-09-002
- [CC-Part3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2007, Version 3.1 Revision 2, CCMB-2002-09-003
- [HLA] Rainer Landfermann, Hans Loehr, Michael Scheibel, Stefan Schulz and Christian Stüble: The PERSEUS Security Framework - High-Level Software Architecture. Requirements, Analysis, and Design. Ruhr-University Bochum, Sirrix AG, March 5, 2007.