A CC Approach to Secure Workflow Systems

Rune Friis-Jensen

Kongens Lyngby 2007
IMM-THESIS-2007-11

Technical University of Denmark
Informatics and Mathematical Modelling
Building 321, DK-2800 Kongens Lyngby, Denmark
Phone +45 45253351, Fax +45 45882673
reception@imm.dtu.dk
www.imm.dtu.dk

Abstract

Secure workflow systems are used to maintain secure and non-repudiable records of possibly very complex transactions or other business processes within a business or organisation. Such systems are coming more and more into focus, as requirements for electronically documentable business practices increase. Possible applications include areas as diverse as maintaining secure accounting records, processing of examination answers and handling laboratory records.

This thesis analyses the security requirements of such a system using an approach based on the Common Criteria for Information Technology Security Evaluation(CC). A Protection Profile(PP) is developed which in an implementation-independent manner describes the security requirements of a Secure Workflow System. On the basis of the PP a Security Target(ST), which conforms to the PP is developed. The ST identifies and describes the security requirements of a specific Secure Workflow System, which uses a centralised architecture. The ST is used to produce concrete specifications for this system which may be used for implementing a concrete system.

Keywords: Common Criteria, Protection Profile, Security Target, Security Evaluation, Workflow, Workflow system

Resume

Sikre workflowsystemer bliver brugt til at opretholde sikker og uafviselig dokumentation for muligvis meget komplicerede transaktioner eller arbejdsgange indenfor et forretningsområde eller en organisation. Som følge af stigende krav til dokumenterbare elektroniske forretningsprocesser efterspørges disse systemer i højere og højere grad. Anvendelsesmulighederne er så forskellige som udarbejdelse og revision af regnskaber, håndtering af eksamensafleveringer og håndtering af laboratoriejournaler.

Denne afhandling analyserer sikkerhedskravene af et sådant system ved hjælp af Common Criteria for Information Technology Security Evaluation(CC). Der udarbejdes en Protection Profile(PP), der på en implmentationsuafhængig måde beskriver sikkerhedskravene for et sikkert workflowsystem. Baseret på PP'en udarbejdes et Security Target, der er i overensstemmelse med PP'ens krav. ST'en identificerer og beskriver sikkerhedskravene for et specifikt sikkert workflowsystem, der benytter sig af en centraliseret arkitektur. ST'en benyttes til at udvikle konkrete specifikationer for systemet, som kan bruges til at implementere et konkret system.

Nøgleord: Common Criteria, Protection Profile, Security Target, sikkerhedsevaluering, forretningsprocesser, workflowsystem

Preface

This M.Sc thesis was carried out at the Informatics and Mathematical Modelling department at the Technical University of Denmark. The project was completed in the period from September 4, 2006 to February 5, 2007 under the supervision of Professor Robin Sharp.

I would like to thank Robin Sharp for his guidance and support throughout the project. I would also like to thank my parents for their endless support. Special appreciation goes to my father for proofreading this thesis and my girlfriend for her support during the entire project.

Rune Friis-Jensen
Kongens Lyngby, February 2007

Contents

Acronyms

API	Application Programming Interface
CC	Common Criteria
CORBA	Common Object Request Broker Architecture
CSP	Cryptographic Service Provider
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IIOP	Internet Inter-ORB Protocol
IP	Internet Protocol
IPC	Inter-Process Communication
ISO	International Organisation for Standardization
IT	Informative Technology
OMG	Object Management Group
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
RMI	Remote Method Invocation

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol
ST	Security Target
SWFS	Secure Workflow System
SWFSPP	SWFS Protection Profile
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
WAPI	Workflow Application Programming Interface
WfMC	Workflow Management Coalition

Chapter 1

Introduction

1.1 Motivation

Workflow systems are becoming increasingly popular. This is due due to their effective technical solution for increasing productivity, reducing operating costs and improving customer service (within organisations and businesses). The idea behind workflow systems is to separate the business processes from the applications and data. This improves the support for dynamic business changes and makes it easier and faster to adapt to a new business environment. Furthermore workflow systems can be given their own highly intuitive graphical interface, which hides much of the background complexity of the inhomogeneous application interfaces.

Like any other IT system a workflow system comes at a cost of increased requirements on IT security. The goal of this thesis is to design a Secure Workflow System (SWFS), which meets the security requirements, identified through the use of the Common Criteria for Information Technology Security Evaluation.

1.2 Problem statement

The aim of this project is to design a Secure Workflow System(SWFS) using an approach based on the Common Criteria for Information Technology Security Evaluation(CC). The first step in the design process will be to analyse the

security requirements of SWFSs, and on this basis to develop a Protection Profile for SWFSs. From this Protection Profile, a Security Target for a specific SWFS should be developed and used to produce concrete specifications for this system.

1.3 Thesis structure

The thesis is structured as follows:

Chapter 1 describes the motivation and aim of the project. General introductions to workflow, workflow systems and the Common Criteria are presented.

Chapter 2 describes the development and content of the Protection Profile (PP) for Secure Workflow Systems, which has been developed.

Chapter 3 describes the development and content of the Security Target(ST), which conforms to the Secure Workflow Systems Protection Profile.

Chapter 4 contains concrete specifications of the system specified in the ST.

Chapter 5 discusses the most significant change from CC 2.x to CC 3.1.

Chapter 6 discusses possibly the future work to be done based on this thesis.

Chapter 7 gives an overall conclusion of the thesis.

Appendix A contains the developed PP.

Appendix B contains the developed ST.

Appendix C contains the list of TSFIs and related commands identified in chapter 4.

1.4 Workflow

A workflow encompasses how a process obeying a set of defined operating rules is conducted, with the assistance of IT. A workflow consists of tasks which each represent one logical step within the workflow. Typically a workflow will consist of a combination of automatic tasks and tasks that require human intervention. An example of a workflow which describes the process of ordering some commodity is shown in figure 1.1.

The 'Prepare Order' and 'Approve' task require human interaction, while the remaining tasks may be performed automatically. An instance of the workflow

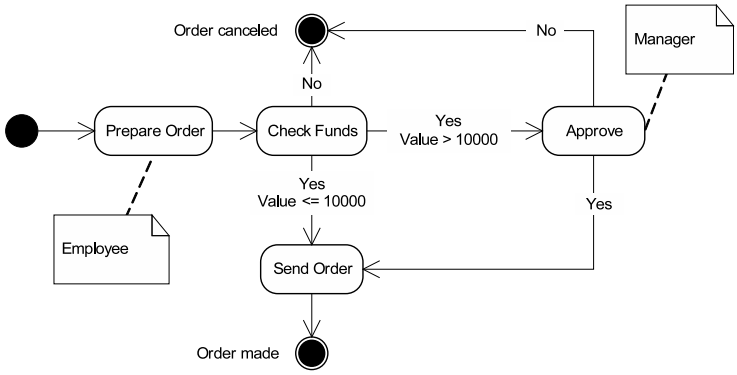

Figure 1.1: Workflow example

may have two outcomes; either the order is made or it is canceled. The sequence of tasks within an instance of the workflow is dependent on whether there is sufficient funds and the value of the order. If the value of an order is 10.000 or below order is sent after it has been confirmed there is sufficient funds. If the value of an order is above 10.000, it cannot be sent before a manager has approved it.

1.5 Workflow systems

Many applications have workflow technology embedded into them. Normally this is used to move information between users of the application in a structured manner. Such applications do rarely support information exchange with outside applications, which means that the workflow is limited to the application itself. The workflow and the rules surrounding it are often hard coded into the application or may only support very limited changes, which makes it difficult for users to perform changes in the workflow.[22]

A workflow system improves upon the shortcomings of applications with embedded workflow technology by separating the workflow technology from the application. A workflow system sits on top of the applications and coordinates and supports the exchange of information between them according to the definition of the workflow. This enables the support of workflows across multiple applications and thereby given results in better support for cross organisational workflows.

Since workflow systems focus entirely on the execution of workflows they are much more flexible in regard to both the configuration and the management of workflows. To support easy configuration of workflows and operating rules a

workflow is usually represented in a computer processable definition language, which can be interpreted by the workflow system. The definition can be created by a tool which provides a graphical representation of the workflow, which means that even persons who are not trained extensively in programming can make changes. [17]

To decrease complexity and support reuse, workflows are usually defined using abstract entities, such as roles rather than using specific ones, such as users. It is the responsibility of the workflow system to link the abstract entities with specific ones. The abstract definition is referred to as the process definition. A process definition includes all necessary information about the process in order for it to be executed by the workflow system. This may include the definitions of tasks, process rules and perhaps references to another process definition, which describes a subprocess.[13]

A workflow system executes a workflow by creating a workflow instance, which represents one execution of the process described by the process definition. Several workflow instances of the same process definition may therefore be executed simultaneously(figure 1.2). Each workflow instance has its own instance data, which describes among other things the status of the workflow and how references in the process definition has been resolved.

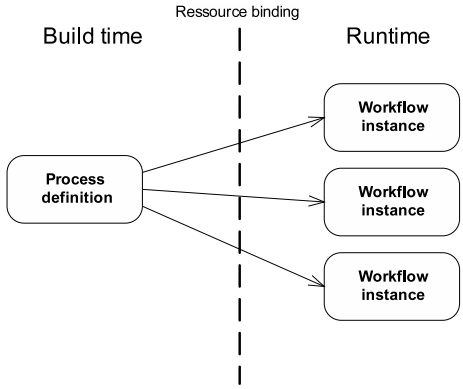

Figure 1.2: From the process definition, defined at build time, several workflow instances can be created. Each workflow instance executes independently of each other.

When a task is to be executed it is offered to the users who may execute the task. A task is offered to a user in form of a workitem. This means that for each task multiple workitems exists. Each user is associated with a worklist to which workitems are put and retracted. The worklist works as an electronic 'in basket' from which the user can select to execute a workitem. When a user executes a

workitem of a task, all workitems associated with the task are retracted from the worklists and the user becomes the assigned executor of the task. The worklist concept is illustrated in figure 1.3.

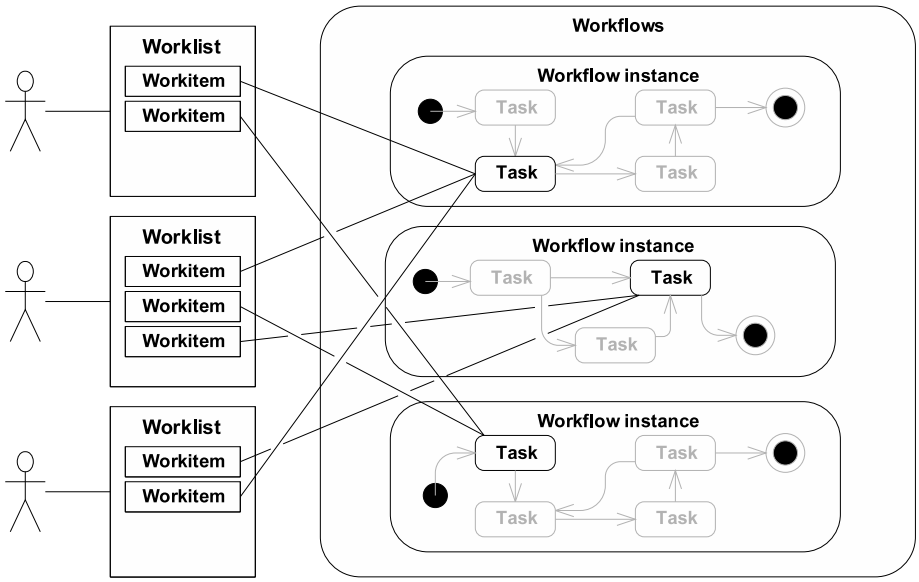

Figure 1.3: Illustrates how workitems on the user worklists are associated with tasks of workflow instances.

In general a workflow system consists of one or more workflow engines which provides the run-time execution environment for workflow instances. Typically workflow engines are software applications layered on an underlying system, e.g. a host OS. The workflow system may use a centralised or distributed architecture. In a centralised architecture a single workflow engine is responsible for managing the entire execution of a workflow instance. In a distributed architecture multiple workflow engines may each manage a part of the execution of the workflow instance.

When a workflow instance has been created the workflow system will ensure that the workflow is executed in accordance to the rules of its process definition. This includes routing of data between workflow clients, invocation of applications, i.e. text processors, databases etc. and data exchange with other workflow systems. Workflow clients may both be human beings or machines and the data routed can be anything from documents to tasks which assists in achieving the objective of the process.

1.6 Workflow standards

Several organisations are involved in creating standards used in context with workflow systems. The perhaps most recognised entity within workflow standardisation is the Workflow Management Coalition (WfMC). WfMC was founded in 1993 and is a global non-profit organisation. Its mission is to increase the value of workflow technology, decrease the risk of using workflow products and increase the awareness for workflow. As part of this the WfMC has developed several standards for interoperability of the various components of a workflow system. The WfMC Reference Model[20], depicted in figure 1.4, defines a common architecture for workflow systems and gives an overview of how the different standards fit together. Each interface is associated with one or more WfMC standards.

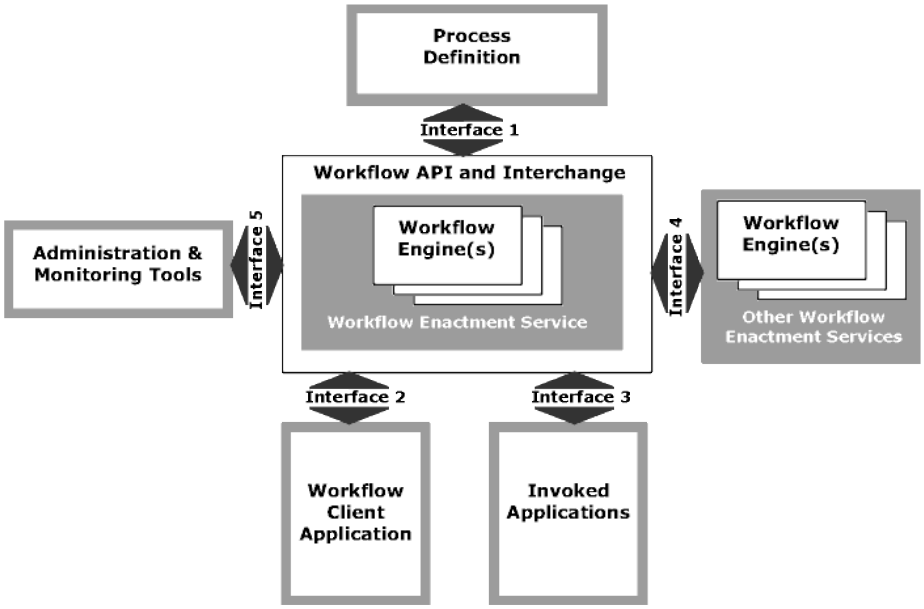

Figure 1.4: The WfMC Reference Model

The standards organisation The Object Management Group (OMG) is also involved in workflow standardisation. They have e.g. defined the Workflow Management Facility specification[3] which is based on the WfMC Reference Model. The Workflow Management Facility specification provides an object-oriented framework to enable different workflow products to work together. The framework uses Common Object Request Broker Architecture (CORBA), which is OMG's solution to provide systems interoperability.

Additional several workflow related standards exists which have been developed with support from large corporations such as Sun, Oracle, Microsoft, SAP and IBM etc.

1.7 The Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) is the defacto criteria for evaluating the security of any set of software, firmware and/or hardware including possible guidance. The current version of CC is 3.1, which was released in September 2006. The CC version 2.1 is recognised as the international standard ISO/IEC 15408.

The CC uses the term Target of Evaluation (TOE) in order to refer to what is evaluated. The TOE may be an IT product, a part of one or a set of IT products, but it may also be a technology which may never become a product or may be a combination of these.

1.7.1 Target audience

The target audience of the CC are mainly three groups with general interest in the security evaluation: consumers, developers and evaluators.

Consumers can use the results of evaluations to help decide whether a TOE fulfills their security needs. Consumers can also use the evaluation results to compare TOEs. Finally consumers can use the CC to specify their security requirements in an implementation-independent manner to vendors of products or to system integrators. In CC this specification is called a Protection Profile (PP).

Developers can use the CC to specify a secure TOE and in preparing them for evaluation. The security requirements to be met by a TOE is defined in the Security Target (ST). The ST is implementation dependent and may conform to one or more PPs. In the context of evaluation the CC assists in determining the responsibilities of developers in order to fulfill a certain level of assurance that the TOE conforms to the ST.

Evaluators can use the CC to make judgments on whether a TOE conforms to a ST. The CC does this by describing a set of general actions which the evaluator is to carry out.

1.7.2 CC Organisation

The CC is divided into the three parts listed below:

Part1, Introduction to the general model contains the introduction to the CC. The general concepts and principles of the CC and the general model of evaluation is presented.

Part2, Security functional components contains a set of functional components which serve as a template for specifying the security functional requirements(SFRs) of the TOE.

Part3, Security assurance components contains a set of assurance components which serve as a template for specifying the security assurance requirements(SARs) of the TOE. Furthermore it presents the evaluation criteria for PPs and STs and seven Evaluation Assurance Levels (EALs). The EALs are pre-defined sets of assurance requirements where level 1 through 7 represents an increased level of effort in assuring that the TOE in reality conforms to the PPs and STs it claims conformance to.

1.7.3 Protection Profile

The intended use of a Protection Profile (PP) is to describe security requirements of a TOE of a certain type. This could be a firewall, a pin-entry device, an information flow control model or a workflow system. The same PP may therefore be conformed to by several different STs and a PP may conform to other PPs. Several entities may have interest in writing a PP. User communities may use it for agreeing upon requirements of a specific TOE type. Developers may use it for defining minimum requirements for a certain type of TOE. Governments, organisations or large corporations may use it for specifying their requirements when acquiring of IT products and systems.

To demonstrate that a PP is complete and consistent, a PP must be evaluated according to the CC Protection Profile evaluation criteria, APE, of CC Part 3[10].

A PP must contain the following main sections:

PP Introduction which includes a PP reference which uniquely identifies the PP and a TOE overview which describes the TOE type, its usage and its major security features. Lastly a list of the required non-TOE hardware/software/firmware must be given.

Conformance claims which describes how the PP conforms to other PPs and packages. It must also contain a conformance description which specifies how conforming PPs and STs may conform to the PP. Either one of the types of conformance 'strict' or 'demonstrable' can be required. If 'strict' conformance is required the conforming PP or ST shall contain all statements of the PP, but may contain more. 'Demonstrable' conformance requires that the conforming PP or ST either provides 'strict' conformance

or a rationale is given on why the conformance is equivalent or more restrictive than the PP.

Security problem definition which specifies the security problem to be addressed by the TOE. This includes listing the assumptions on the operational environment, the threats which are to be countered and the organisational policies (OSPs) to be enforced.

Security objectives which describes in a natural language the security objectives of the TOE and its operational environment and gives a security objectives rationale. The rationale shall for each security objective of the TOE describe how and which threats are countered and which organisational security policies(OSPs) are enforced in whole or in part by the TOE. The rationale shall include a similar description of how the security objectives of the operational environment achieves this with respect to the operational environment and additionally specify how the assumptions are addressed.

Extended components definition which includes the definitions of components which are not based on components of CC Part 2 [9] or CC Part 3 [10]. Extended components may be defined when requirements cannot be based on already existing components of the CC and should be specified in a similar manner to the existing CC components.

Security requirements which includes the security functional requirements (SFRs) which satisfies the security objectives for the TOE. The SFRs shall ensure that the security objectives are translated into a standardised language. The main purpose of this is to ensure that a more exact description of the functionality of the TOE is provided and to allow for easier comparison between PPs or STs. The CC Part 2 provides the catalog of predefined SFRs[9].

The section shall also include a list of security assurance requirements (SARs) which are required by the PP. The SARs are used to describe how the TOE is to be evaluated in a standardised language, which as for the SFRs provides an exact description and easier comparison.

Finally a rationale must be included which shows which SFRs address which security objectives of the TOE and the justification of this. All security objectives of the TOE must be addressed. The security requirements section shall also include a rationale to why the selected set of SARs was deemed appropriate.

1.7.3.1 PP development

Although the structure of the PP follows the natural development process the actual development of the PP at least for persons new to CC is an iterative process. Often new requirements will appear during the PP development as one becomes more familiar with the CC and when reading SFRs and SARs of Part 2 [10] and Part 3 [10] of the CC respectively.

1.7.4 Security Target

The intended use of a Security Target is to describe the security requirements of a specific TOE. Several entities may have an interest in a ST. Developers may wish to write a ST to develop a TOE, which can be evaluated and certified to fulfill certain security requirements specified by consumers or by regulatory entities e.g. governments. Consumers may be interested in STs to ensure that their security requirements can be met by the TOE and also to compare the security of TOEs with similar functionality.

The structure of a ST is very similar to the structure of a PP, described in section 1.7.3, with few exceptions. The 'Security problem definition', 'Security objectives', 'Extended components definition' and 'Security requirements' sections are identical to those of the PP with the exception that the operations of SFRs and SARs must be fully completed. The main sections of the ST is given below. The sections which are identical to those of the PP are in bold and italic.

ST Introduction which includes all the sections of the PP and additionally a TOE description. The TOE description should provide a more detailed description of the security capabilities of the TOE compared to the TOE overview. It should be detailed enough to give evaluators and potential consumers a general understanding of the security capabilities of the TOE. Both the physical scope of the TOE as well as its logical scope should be discussed.

Conformance claims which states how the ST conforms to the CC, any PPs and any packages.

Security problem definition

Extended components definition

Security requirements

TOE summary specification which summarizes how the TOE satisfies all the SFRs and provides the general technical mechanisms for achieving this. The section should be detailed enough to enable potential consumers to understand the general form and implementation of the TOE.

Chapter 2

Protection Profile

This chapter describes the development and content of the Protection Profile (PP) for Secure Workflow Systems (SWFSs). The Secure Workflow Systems Protection Profile (SWFSPP) is attached as appendix A.

2.1 PP development

The development of the SWFSPP is based on the PP content requirements as specified in appendix B of Common Criteria (CC) Part 1[8] and which are summarised in section 1.7.3.

The goal is to develop a PP which defines the minimum set of security requirements which must be fulfilled in order for a workflow system to be considered a Secure Workflow System(SWFS). The PP should be general enough such that a wide range of workflow systems can claim conformance independently of their architecture and the technologies used.

The first step is to derive a general Target of Evaluation(TOE) model which describes the common features of almost any workflow system. The Workflow Management Coalition(WfMC) Reference Model[20] shown in section 1.6 provides a good starting point. The model does however not consider the implications of providing security. A generalised SWFS model which builds upon the WfMC Reference Model has therefore been developed and used as the Target of Evaluation(TOE) in the SWFSPP.

The full TOE identification is given in section A.1.2, while a summary is given in section 2.2.

The succeeding sections of this chapter describes the main sections of the PP. Finally a conclusion is given on the PP development.

No certified PP related to workflow or a workflow system is available from the official CC website's[1] list of PPs. PPs which address TOEs which provide similar or related functionality has however been useful in the development of the SWFSPP. Inspiration to the structure and contents of the PP has been found in the following PPs:

- Database Management System Protection Profile[24]
- Labeled Security Protection Profile[2]
- Discretionary Information Flow Control (MU) Protection Profile[18]
- Role-Based Access Control Protection Profile[23]

Additionally inspiration has been found in the master thesis 'Security in POS Systems'[21], which in a similar manner to this thesis has developed a PP and ST for Point-of-Sale systems.

Common for all of the above PPs are that they were created using earlier versions of CC. More specifically version 2.0 and 2.1. Although much of the content required by the current CC 3.1 resembles the requirements of CC 2.x, changes have still been made which affects the PP development. E.g. it is no longer possible to specify security functional requirements(SFRs) for the IT environment and additional SFRs have been included.

2.2 The Target of Evaluation

The purpose of any workflow system is to control the execution of business processes, workflows. The workflows may consist of a combination of manual and/or automated tasks. To achieve this a typical workflow system supports the interaction with human users, third party applications and perhaps other workflow systems.

What separates a SWFS from any other workflow system is that it provides security mechanisms which ensures that the execution of workflows is done in a secure manner. The main objectives of a SWFS is to ensure that individual users can be held accountable for their actions and that the SWFS assets are protected both physically and logically. To achieve accountability of users it is required

[1] http://www.commoncriteriaportal.org

that access is limited to authorised users only and that all security relevant events are audited in a way which ensure that users can be held accountable for their actions.

Audit records, which are associated with the identity of the user which caused it, are generated and stored.

2.2.1 SWFS model

A SWFS will typically consists of one or more workflow engines which are software applications layered on top of an OS. The workflow engines provide the execution environment for the workflows. As any other workflow system a SWFS provides functionality to:

- instantiate process definitions
- control workflow instances
- generate audit data for monitoring
- communicate with users
- invoke applications
- communicate with other SWFSs

To ensure that a wide range of workflow system may claim conformance to the SWFSPP no requirements are made on the amount of workflow engine(s) the TOE should consist of and on whether a distributed or centralised architecture is used.

2.2.1.1 TOE assets

In order for something to be considered a TOE asset, its confidentiality, integrity and/or availability must be considered vital to the sound operation of the TOE. The primary TOE assets identified are:

Process definitions A process definition is a computer processable definition of a business process. A process definition defines how information within a workflow is to be handled such as:

- starting and completion conditions
- which tasks the workflow consists of

- the rules for navigating between tasks
- references to applications, which may be invoked
- definitions of workflow relevant data which may need to be referenced

Control data Control data consists of data internally managed and maintained by the TOE such as:

- state information of workflow instances
- other internal status information
- checkpointing and recovery/restart information used by TOE to coordinate and recover from failure

Workflow relevant data Workflow relevant data, is used to determine transition conditions which influences the state transitions within the workflow instances. Workflow relevant data may be accessible to invoked applications, clients or other SWFSs, but only in a very limited and highly constrained way.[20]

Application data Application data is application specific data and only relevant to applications and clients during the execution of a workflow instance.[20]

Worklists Worklists consists of workitems which each are associated with a task. workitems are assigned by the TOE and are to be processed by clients during the execution of workflow instances.[20]

Audit data Audit data is generated by the TOE during operation. The purpose of the audit data is to provide a non-repudiable trace of the history of the workflow instances as well as being able to gather statistics.

2.2.1.2 SWFS roles

Users have different responsibilities in any SWFS. It is therefore useful to categorize users into roles. Each role resembles a specific set of responsibilities related to the upholding of the security of the TOE. The following roles have been identified:

Administrator A person who has privileges to install, configure and maintain the TOE and its security functions. This includes e.g. the ability to:

- manage the group of authorised users and the associated authentication data
- maintain and review the generated audit data
- manage the various Security Function Policies (SFPs)

Manager A person who has privileges to create, modify and delete process definitions and manage workflow instances within the TOE. This includes e.g. the ability to:

- associate clients with workflow roles
- assignment and re-assignment of workitems
- monitoring the progress of task instances and workflow instances

Client A person or application which can participate in one or more workflows through the processing of tasks.

Other roles may be identified by making a more detailed division of users. The above roles has been deemed the minimum set of roles which are required in order to fulfill the requirements of a SWFS.

For each SWFS role of number of interfaces exist which allow users to fulfill their responsibilities. This includes:

- Client interfaces which allow clients to access the worklists, the workflow relevant data and the application data which they are authorised for.
- Workflow management interfaces which allow managers to manage process definitions and workflow instances.
- Administrative interfaces which allow administrators to install, configure and manage the TOE and the TOE security functionality(TSF).

Applications which interfaces with the SWFS through any of these interfaces are referred to as user applications. An application which allows a client, manager or administrator to interface with the SWFS are referred to as a client application, manager application or administrator application respectively.

The SWFS model used as the TOE in the SWFSPP is shown in figure 2.1.

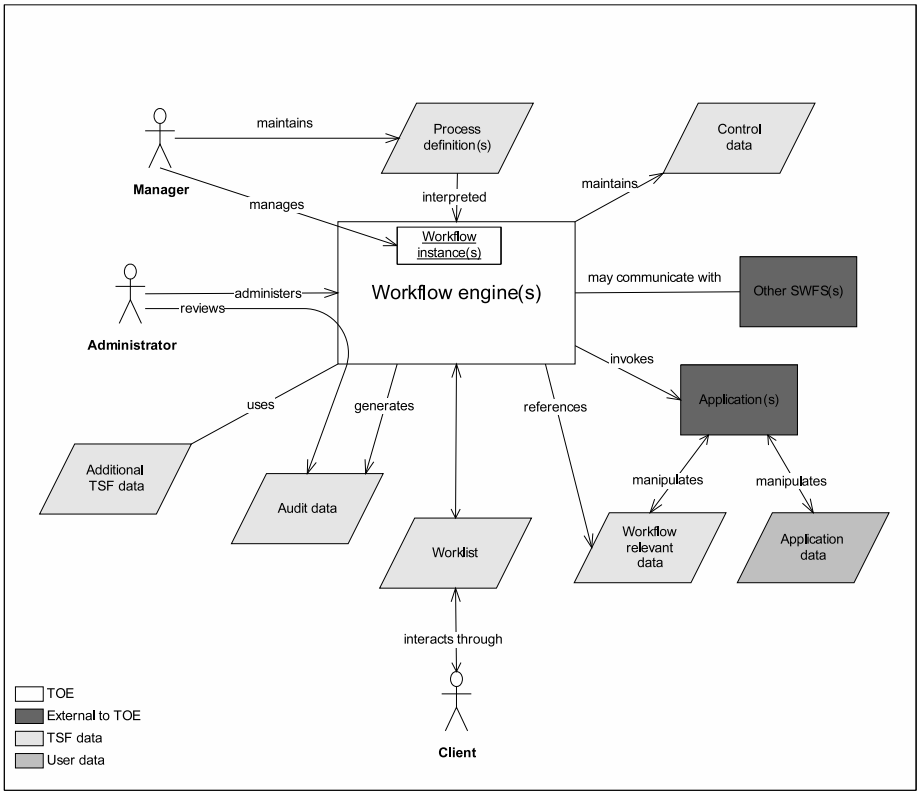

Figure 2.1: The SWFS model

2.2.2 Security functionality

An SWFS provides the security related functionality completely or in co-operation with the IT environment by implementing the following security features:

Identification and authentication of all SWFS roles, invoked applications and SWFSs.

Access control to application data through the specification of access SFPs (security functional policies).

Information flow control of application data through the specification of flow SFPs.

Audit generation to capture all auditable events, thereby providing capability to hold users accountable for their actions and detect malicious behaviour.

Secure audit storage which stores all records for all security relevant operations performed on the TOE.

Secure audit review which allows administrators to review stored audit records and detect potential and actual security violations.

Authorised administration through the administrator role. This allows administrators to configure and manage the access SFPs, flow SFPs, the identification and authentication of users and the auditing functions.

Backup of data such that corrupted or deleted data may be recovered.

2.2.2.1 Protection of application data

Due to the dynamic nature of workflows the security requirements for application data can become very complicated. Client privileges may depend on the state of the workflow, whether the client is assigned to a specific workflow role or whether the client has processed a specific task etc. To support these requirements the SFWSPP defines two types of access SFPs which have to be implemented; a SWFS access SFP and a Workflow access SFP.

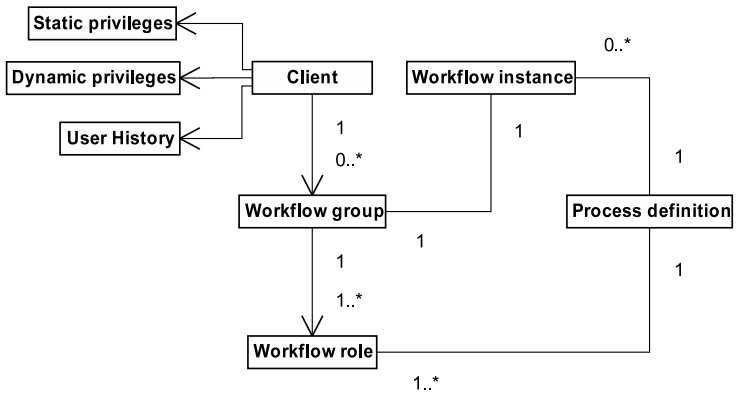

Figure 2.2: SWFSPP conventions.

To enforce the two types of policies the SWFSPP uses the conventions shown in figure 2.2. Each client is associated with zero or more workflow groups, in each of which the client has one or more workflow roles.

A client has a set of static privileges and a set of dynamic privileges. The static privileges are privileges which have been assigned to the client permanently or at least until they are revoked. Dynamic privileges are privileges which are assigned to the client as a result of the active binding of the client. I.e.

privileges can be granted dynamically to a client when he activates a specific workflow role or specific task. The dynamic privileges are revoked when the binding is terminated.

Finally each client is associated with a client history, which contains the relevant history of the client's interactions within the workflow instances. This could be consumed workflow groups, workflow roles, privileges etc.

Since there may be constraints on what a client can do simultaneously, a client is associated with a set of active privileges when a session is established. The set of active privileges is the subset of the client's static privileges and dynamic privileges which the client is allowed to use.

The SWFS access SFP enforces the access control requirements, which is applicable to all workflow instances executed within the SWFS. This could be requirements such as specific clients may not be members of the same workflow group or certain privileges may not be possessed by the same client at the same time.

The Workflow access SFP enforces the access control requirements of the workflow instance's access SFP. This SFP is an instantiation of the process access SFP defined at the process definition level. Figure 2.3 shows the relation between the policies.

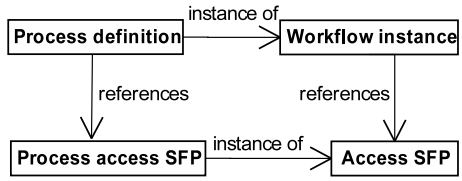

Figure 2.3: Relation between process access SFP and the workflow instance's access SFP.

The process access SFP should specify the access control requirements within the process definition. This could e.g. be which workflow roles have access to a specific object or task and separation of duty constraints such as if client A has processed task 1 then he cannot process task 5.

The specification of access control SFPs within a SWFS does however usually not provide sufficient protection of the application data. A SWFS will typically control multiple shared resources containing application data. This will often lead to requirements on how application data may flow from one resource to another. This may be between the SWFS and the applications which it interacts with, specific application data objects etc.

To control the flow of information the SWFSPP therefore additionally requires

that two types of flow SFPs are implemented.

An application flow SFP should be specified for each user application, invokable application and SWFS which the SWFS interacts with. These policies should be used to enforce requirements such as certain types of information should only be handled by specific applications.

Secondly a Workflow flow SFP shall be implemented which analogous to the Workflow access SFP shall enforce the information flow requirements of the workflow instance's flow SFP. Figure 2.4 shows the SWFSPP SFP framework.

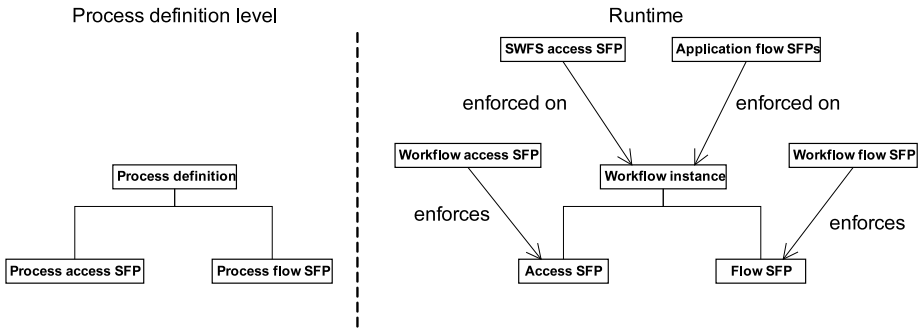

Figure 2.4: The SWFSPP policy framework

Since the policies very much depend on the type of the SWFS, the SWFSPP only provides the basic policy requirements and leaves the decision on how fine grained the four types of SFPs are required to be in order to achieve a sufficient level of security for a specific SFWS.

2.2.3 Conformance

The SWFSPP is both CC Part 2[8] and CC part 3[9] conformant of CC version 3.1. This means that all of the SWFSPP security functional requirements(SFRs) and security assurance requirements(SARs) are all based on components in CC. Additionally the SWFSPP is EAL3 augmented, since it contains all of the SARs of the EAL3 package from CC Part 3[10] and the additional SAR ALC_CMS.4.

The SWFSPP specifies that strict conformance is required. This ensures that conforming PPs/STs meet all of the SWFSPP security requirements in a stringent manner.

2.3 Security problem definition

This section describes the development of the security problem definition of the SWFSPP. The security problem definition shall describe the security problem to be addressed. All assumptions on the operational environment must be described, the threat agents and the related threats to be countered must be identified and the set of organisational security policies(OSPs) to be enforced must be defined. All of these are to create the basis of the identification of the TOE security objectives.

2.3.1 Assumptions

In order for the TOE to be considered secure the operational environment has to meet the assumptions listed in this section.

AP.ADMIN *The administrators of the TOE are qualified in managing and maintaining the TOE and can be trusted not to abuse their privileges.*

This assumption is made to ensure that at least one user of the TOE can be trusted to be able to manage and maintain the TOE's security functions and security data. It would be possible to setup the TOE in a manner where this assumption would not need to be met. This would however require the system to be setup in manner where the OS root/administrator account is disabled and replaced with named administrator accounts in order to be able to hold individual administrators accountable. The administrator role could hereby be divided into several administrative roles e.g. an audit administrator and a security administrator. An assumption that this setup is created by trusted personnel must however still be made.
To avoid making too strict requirements upon the set of administrative roles required it has been deemed that a reasonable level of security can be obtained with the current assumption.

AC.RESOURCE *The TOE has sufficient resources available to function properly and securely.*

This assumption is made to ensure that the TOE and its security functions are able to operate reliably. It

may not necessarily be a simple task to accomplish and could cause slow response times, e.g. when new resources are being acquired. It is however considered a reasonable assumption that the operational environment is able to fulfill this requirement.

AC.OS *The underlying operating system and network services which the TOE relies upon are installed, configured and managed in a secure manner.*

Since the TOE is implemented in software it relies upon the underlying OS and hardware. This assumption therefore has to be made to guarantee that the TOE will operate in a secure manner. Alternatively these underlying services should be included within the TOE. This issue is discussed in chapter 5.

AC.TIME *The underlying operating system shall provide the TOE with a clock which is synchronized with a reliable hardware clock.*

This assumption is made to ensure that a reliable timestamp can be associated with each audit record. A reliable hardware clock could e.g. be a clock which is synchronized via GPS.

2.3.2 Security threats

This section describes the threat agents and the threats against the TOE and its assets.

2.3.2.1 Threat agents

Threat agents are the source of threats. Threats may be caused by human beings or due to environmental circumstances.

In the SWFSPP threat agents are categorized as shown below. Note that administrators are not considered a threat agent, because of the assumption AP.ADMIN.

Authorized user An authorized manager or client.

Unauthorized user An entity which is **not** authorized to access the TOE.

External events Interruption of TOE operation due to failure of hardware, storage, power supply, fire, water damage etc.

Both authorised and unauthorised users are assumed to have different levels of resources and motivation. Resources may e.g. be specialized knowledge, access to IT or TOE facilities etc. Motivation may be economic gain, destructive behavior or perhaps personal revenge.

In the following the term attacker will be used to denote any of the threat agents.

2.3.2.2 Threats

All threats pose a threat to either primary assets as listed in section 2.2.1.1 or secondary assets such as TOE security functionality(TSF) security attributes. The following threats have been identified with the earlier described assumptions in mind.

T.ACCESS *Unauthorized access to the TOE.*

This threat is included since it poses a major threat against the security of the TOE. Access may be gained by an unauthorised user which is able to bypass the security mechanisms of the TOE. Another type of unauthorised access is when an authorised user is able to impersonate another authorised user e.g. one with different privileges or a higher privileged user such as an administrator.

T.DATA *Unauthorized access to application data.*

The threat appears in the situation where an attacker is able to gain unauthorised access to application data. Unauthorised access may be gained by bypassing the access control mechanisms of the TOE or though impersonation of an authorised user. Unauthorised access may however also be gained through more subtle ways e.g. an authorised user could copy data from one document to another thereby giving another user access to application data which he is not permitted to access.

T.DATAFLOW *The integrity of the information flowing from or to the TOE is compromised.*

Compromise of the integrity of information may happen deliberately or accidentally through changing its content. If an attacker compromises the integrity of the information transmitted from and to the TOE its contents cannot be relied upon. This means that the data used within the workflows will become unreliable and the TOE will be unable to provide its services in a trustworthy manner.

T.MODIFY *Information protected by the TOE is modified maliciously by an attacker.*

As opposed to T.ACCESS this threat deals with the case where the attacker actually tries to make malicious changes to the data protected by the TOE. If data is maliciously modified or deleted the security of the TOE is seriously compromised. Not only may the TOE security mechanisms be compromised, but the workflows may be damaged or become unreliable.

T.UNATTENDED *An attacker gains access to the TOE by the use of an unattended session.*

If an authorised user leaves a session open without shutting it down an attacker could takeover the session and gain unauthorized access to the TOE and its assets.

T.PHYSICAL *The underlying OS/network services are physically damaged in a way that prevents the TOE from functioning properly or results in loss of data.*

As the TOE relies upon an underlying infrastructure it poses a threat if this is physically damaged. Damage may occur due to external events such as fire or water damage. Damage may also be inflicted deliberately by unauthorised or authorised users which have gained physical access to the hardware on top of which the TOE runs.

T.MALFUNCTION *Malfunction in the TOE or underlying OS/network services prevents the TOE from functioning properly or results in loss of data.*

Malfunction comprises all software and hardware errors which are the cause of interruption of the operation of the TOE and may cause TOE assets to be lost or corrupted.

T.TRUSTED *The TOE invokes a trusted application or exchanges information with a SWFS which has been compromised or is being impersonated by an attacker.*

This threat deals with that an invokable application or SWFS may be compromised without detection by the TOE. Such a compromise could result in unreliable results from the invokable application or SWFS.

2.3.3 Organisational security policies

The organisational security policies(OSPs) states the rules, procedures and guidelines to be enforced by the TOE and its operational environment in order to ensure that the TOE operates in a secure manner. The following OSPs have been found necessary:

P.ACCESS *Only authorized users and administrators may access the TOE.*

This policy exists to ensure that only administrators and authorised users may access or interact with the TOE. The policy hereby prevents anonymous access to the TOE and unauthenticated communication with the TOE.

P.TRAINING *Authorized users and administrators shall be continuously trained in using the TOE properly and securely.*

The purpose of this policy is to ensure that authorised users and administrators of the TOE are capable of operating the TOE in a secure manner. This means that users are trained to interact with the TOE as intended. This is especially important for users in the manager and certainly in the administrator role, since their actions may severely compromise the security or sound operation of the TOE.

P.ACCOUNT *Authorized users shall be held accountable for their interactions with the TOE.*

The policy is to ensure that all authorized users can be held accountable for their actions and that fraud and malicious intents can be acted upon by the administrators of the TOE.

P.APPLICATION *All applications which the TOE can invoke shall be run on trusted machines which configuration can only be changed by highly trusted persons who are authorised to do so and can be held accountable.*

The invokable application may play a major part in the sound operation of the TOE and its workflows. It is therefore important that these applications can be trusted upon.

P.WORKFLOW *Managers shall be able to manage the security mechanisms of the workflows which they are responsible for.*

This policy assures that managers are able to manage the SFPs related to specific workflows, when, how and which workflows should be executed and so forth.

2.4 Security objectives

This section describes the security objectives of the SWFSPP, which are to address the assumptions, counter the threats and enforce the OSPs defined in section 2.3. Every assumption, threat and OSP shall be addressed by at least one security objective and each security objective shall address at least one assumption, threat or OSP. The security objectives are divided into two categories, those of the TOE and those of the operational environment. Assumptions may only be addressed by security objectives of the operational environment.

The mapping between security objectives and assumptions, threats and OSPs is shown in table 2.1.

2.4.1 Security objectives of the TOE

The following security objectives of the TOE are identified:

O.AUTH *The TOE shall provide means for identifying and authenticating users before allowing access to the TOE*

	AP.ADMIN	AC.RESOURCE	AC.OS	AC.TIME	T.ACCESS	T.DATA	T.DATAFLOW	T.MODIFY	T.UNATTENDED	T.PHYSICAL	T.MALFUNCTION	T.TRUSTED	P.ACCESS	P.TRAINING	P.ACCOUNT	P.APPLICATION	P.WORKFLOW
O.AUTH					x	x		x					x		x		
O.ACCESS						x		x									
O.FLOW						x											
O.MANAGE					x	x	x	x					x		x	x	
O.WORKFLOW																	x
O.AUDIT					x	x		x							x		
O.DATAFLOW							x										
O.RECOVER								x		x	x						
O.SESSION									x						x		
O.TRUSTED												x					
OE.PHYSICAL										x							
OE.ADMIN	x																
OE.BACKUP								x		x	x						
OE.TRAINING	x								x					x			
OE.RESOURCE		x															
OE.APPLICATION												x				x	
OE.OS			x														
OE.TIME				x													

Table 2.1: Mapping of security objectives to assumptions, threats and OSPs.

and its resources.

The objective is mainly identified to counter T.ACCESS by ensuring that users are identified and authenticated before they can access the TOE. Unauthorised access is hereby prevented. Furthermore the objective is a precondition for countering T.DATA and T.MODIFY. In addition the objective addresses P.ACCESS since this OSP requires that users shall be authorised to access the TOE. P.ACCOUNT is partly addressed since the objective makes it possible to identify users such that they can be held accountable for their actions.

O.ACCESS *A SWFS control SFP shall be specified which enforces the TOE access control requirements. Furthermore a workflow control SFP shall be specified which shall enforce the access SFP of workflow instances.*

The objective is mainly identified to counter T.DATA and T.MODIFY since the enforcement of the TOE access control requirements ensures that data cannot be directly accessed by an attacker. An attacker is hereby also prevented from maliciously modifying data.

O.FLOW *Each user application, invokable application and SWFS which the TOE interacts with must be covered by an application flow SFP. Furthermore a Workflow flow SFP shall be specified which shall enforce the flow SFP of a workflow instance.*

The objective is identified to counter T.DATA by ensuring that application data cannot be transferred to users which are not authorised to access the data.

O.MANAGE *The TOE shall provide means of enabling administrators to manage the security mechanisms of the TOE and restrict these mechanisms from unauthorized use.*

The objective is identified to assure that the TOE's security functions can only be managed by administrators. The objective indirectly counters T.ACCESS, T.DATA, T.DATAFLOW and T.MODIFY by ensuring that the TOE supports management of e.g. ac-

cess and flow SFPs, user security attributes such as role, user identity and authentication credentials. The management functions in addition assist in ensuring that the OSPs P.ACCESS, P.ACCOUNT and P.APPLICATION are enforced.

O.WORKFLOW *The TOE shall provide means of enabling managers to manage the security mechanisms of the workflows which they are are responsible for.*

The objective is identified to directly enforce P.WORKFLOW by ensuring that managers are able to manage the workflows and the related security mechanisms of the TOE.

O.AUDIT *The TOE shall provide means of recording security relevant events in sufficient detail to help an administrator to detect attempted security violations and hold users accountable for any actions that are relevant to the security of the TOE.*

The objective is identified mainly to address P.ACCOUNT by ensuring that security relevant events are audited such that users can be held accountable for their actions. Additionally the objective assists in the mitigation of T.ACCESS, T.DATA and T.MODIFY since it provides administrators with means to detect attempted violations of access rights and thereby may be able to prevent that a violation actually occurs. In the event of compromise the objective may assist in the identification of the extent of compromise. This of course is highly dependable on whether the audit records have been compromised.

O.DATAFLOW *The integrity of all data which is received and sent through the TOE interfaces must be protected.*

The objective is identified to counter T.DATAFLOW. It ensures that the TOE protects the integrity of all data sent and verifies the integrity of all data received.

O.RECOVER *The TOE shall provide administrators with functionality which ensures the that the TOE can recover effectively after a system failure without compromising the security of the TOE. This includes providing functionality which ensures that backups of the TOE assets*

and TOE security functional data are made regularly and that the confidentiality, integrity and availability of these backups are adequately protected.

The objective is identified to mitigate T.MODIFY, T.MALFUNCTION and T.PHYSICAL. It ensures that the TOE provides backup and recovery mechanisms such that data may be recovered in the event of compromise or corruption.

O.SESSION *The TOE shall provide functionality that allows an authorised user or the TSF to invalidate or lock the user's current session after some reasonable period of inactivity. To unlock the session the user must re-authenticate.*

The objective is identified mainly to counter T.UNATTENDED by ensuring that an inactive session automatically is invalidated or locked. The risk that an attacker gets access to an unattended session is hereby decreased. Whether the session is invalidated or locked after a given time interval of inactivity or by the use of some kind of physical token the strategy and mechanisms to ensure this should be chosen based upon a threat analysis. E.g. if a physical token is used the locking of the session may be initiated by the removal of the token. If users always remove the token when they are not attending the session the time interval may be set to a very high value. If however username and password is used it may be reasonable to set the time interval to a lower value even though users are expected to lock the session when they leave it. The objective also addresses P.ACCOUNT since it assists in ensuring that the user using the session is in fact the user who was authenticated.

O.TRUSTED *The TOE shall provide means for additional assurance of the authenticity of trusted applications which are invoked and trusted SWFSs which the TOE exchanges information with.*

The objective is identified to mitigate T.TRUSTED. By ensuring that additional assurance of the authenticity of invoked applications and SWFSs exists at-

tackers are prevented from impersonating a trusted application.

2.4.2 Security objectives of the operational environment

The following security objectives of the operational environment are identified:

OE.PHYSICAL *The operational environment shall ensure that the TOE and its underlying services are sufficiently protected from physical damage by an attacker.*

The objective is identified to counter T.PHYSICAL. It ensures that the TOE is physically protected, e.g. the machine which upon the TOE runs is located in a room which is protected against environmental threats like fire and water damage and where only authorised personnel are allowed access.

OE.ADMIN *The operational environment shall ensure that only highly qualified and trusted users are given administrative privileges.*

The objective is identified to address AP.ADMIN. It ensures that administrators are selected throughly such that the risk of administrators being incompetent or abuse their privileges are significantly reduced.

OE.BACKUP *The operational environment shall ensure that backups of the TOE assets and TSF data are stored physically separate from the TOE and are protected from physical damage.*

The objective is identified to mitigate T.MODIFY, T.PHYSICAL and T.MALFUNCTION. It ensures that backups of TOE assets and TSF data are available even when the TOE is physically damaged, severely compromised or a malfunction occurs.

OE.TRAINING *The operational environment shall ensure that all authorised users of the TOE and the administrators are continuously trained in the proper and secure use of the TOE.*

The objective is identified to address AP.ADMIN and

P.TRAINING. It ensures that all users are continuously trained in the secure use of the TOE such that they remain qualified to interact with the TOE. Furthermore the objective addresses T.UNATTENDED by ensuring that users are aware of how to interact with the TOE in order to preserve its security. E.g. users are learned to log off or lock their session when they do not use it or leave it physically.

OE.RESOURCE *The operational environment shall ensure that the TOE always has sufficient resources to operate properly and securely.*

The objective is entirely identified to address AC.RESOURCE by ensuring that the operational environment monitors the TOE's use of resources and arrange for additional resources if necessary.

OE.APPLICATION *The operational environment shall ensure that all invokable applications and SWFSs which the TOE communicates with run on trusted machines whose configuration can only be changed by authorised personnel and who can be held accountable.*

The objective is identified to counter T.TRUSTED. It ensures that the invokable applications and SWFSs are run on machines with a trusted configuration such that the risk of compromise is significantly decreased.

OE.OS *The operational environment shall ensure that the TOE, the underlying OS and hardware are installed, configured and operated in a way that maintains the security of the TOE. This includes that a security domain is provided which ensures that the TOE cannot be tampered with by other applications since the OS/hardware makes the interfaces through which the TOE can be accessed inaccessible to other applications. Furthermore it must be ensured that the OS and hardware will faithfully execute the commands of the TOE and will not tamper with the TOE in any manner.*

This objective is entirely identified to address AC.OS. It ensures that the underlying OS and hardware can be trusted to maintain the security of the TOE. E.g.

the OS will ensure that interfaces through which the TOE may be accessed by other applications on the OS are made inaccessible.

OE.TIME *The operational environment shall ensure that the underlying OS provides the TOE with a reliable clock which is synchronized with a reliable hardware clock.*

The objective is identified to address AC.TIME. It ensures that the TOE is provided with a reliable clock, such that the timestamps associated with the audit records can be relied upon.

2.5 Security functional requirements

The security functional requirements(SFRs) refine upon the security objectives of the TOE and provides a standardised language to ensure that a more exact description of the security functionality of the TOE is provided. The CC Part 2[9] provides a catalog of predefined SFRs.

The SFRs of the CC are divided into 11 classes which each includes a number of families containing one or more SFR components. Each class addresses a general functional area such as FAU (Security audit), FDP (User data protection) and FMT (Security management). A family addresses a specific domain within a class such as Access control functions(FDP_ACF) in the class FDP. A SFR component contains a minimum set of security functional requirements which can be selected in order to fulfill a security objective e.g. FDP_ACF.1 Security attribute based access control.

Components may be leveled hierarchically. A hierarchical component provides a set of SFRs which are more strict than those of the lower level component. Components may also have dependencies on other components. E.g. the component FDP_ACF.1 (Security attribute based access control) has dependencies on FDP_ACC.1 (Subset access control) and FMT_MSA.3 (Static attribute initialisation). A dependent component or a component which is hierarchical to it shall be included in the PP/ST unless a reasonable explanation can be given to why the dependency does not need to be fulfilled.

The CC provides 4 operations, assignment, selection, iteration and refinement. These allow PP and ST authors to modify the SFRs to provide a more accurate translation of the security objectives of the TOE.

The assignment operation allows for the specification of parameters which can be set by the PP/ST author.

The selection operation allows for the specification of a list of items from which the PP/ST author may select one or more items. Unlike the ST author the PP author may besides completing the assignment or selection do one of the following:

- For assignments:
  - leave the assignment uncompleted
  - narrow the assignment in order to limit the range of values which may be assigned
  - transform the assignment to a selection such that the assignment is narrowed
- For selections:
  - leave the selection uncompleted
  - restrict the selection by removing some choices, but leaving two or more

The iteration operation allows for the iteration of a component such that multiple requirements can be specified based on the same component.

Finally the refinement allows for a PP/ST author to refine upon a SFR. A refinement may be done for clarification or for expressing a more strict requirement which still relates to the original SFR. If more significant changes are made or one wishes to express a requirement which is not part of CC Part 2[9] the CC also allows for the creation of new SFRs, referred to as extended SFRs.

To assist in the selection of SFRs, CC Part 2 provides an appendix for each class containing additional guidance for the use of the class, its families and their components. Additionally much help has been found through the studying of the PPs mentioned in section 2.1 and their selection and specification of SFRs.

2.5.1 TOE security functional requirements

This section describes the SFRs which have been found suitable for satisfying the security objectives of the TOE. All SFRs are based on SFRs from CC Part 2[9]. All security objectives are addressed by at least one SFR and each SFR addresses at least one security objective.

The tracing of the security objectives to SFRs can be seen in table A.4 of appendix A.

2.5.1.1 Security audit

The security objective O.AUDIT requires that the TOE provides functionality to record security relevant events in sufficient detail such that individual users can be held accountable for their actions and attempted security violations can be detected.

The class FAU (Security audit) offers components to achieve this by providing families which provides components for recording, storing and reviewing audit data.

The FAU_GEN family defines requirements for recording the occurrence of security relevant events. When security auditing is implemented the CC lists which security relevant events should be audited for every CC Part 2 SFR component. The events are categorised into three groups, minimal, basic and detailed. The groups are hierarchical which means that if basic audit generation is desired, all auditable events of both minimal and basic shall be included. The PP/ST author may also specify alternative security relevant events or add events which are to be audited.

The FAU_GEN.1 (Audit data generation) component specifies requirements on which auditable events are to be recorded and which information is to be associated with each audit record. In the SWFSPP it has been chosen to leave the assignments and selections of the component uncompleted. It is hereby the task of the conforming PP/ST to choose the level of audit and whether other audit relevant information than the date and time of the event, type of event, subject identity and the outcome of the event should be associated with each audit record.

To fulfill the requirement that an audit record should have a date and time associated, FAU_GEN.1 has a dependency on FPT_STM.1 Reliable time stamps. FTP_STM.1 requires that the TOE security functionality(TSF) provides reliable time stamps. The SWFSPP does not include FTP_STM.1, but since the underlying OS will provide the reliable clock as described in OE.TIME the dependency is satisfied indirectly.

FAU_GEN.2 (User identity association) is implemented such that users can be held accountable for their actions. FAU_GEN.2 achieves this by requiring that each auditable event is associated with the identity of the user who caused it.

In order for the administrator to detect attempted or successful security violations and to identify users who caused specific events the SWFSPP implements FAU_SAR.1 (Audit review) and FAU_SAR.2 (Restricted audit review). FAU_SAR.1 gives administrators the capability to read any information from the audit records and ensures that the information is suitable for interpretation. FAU_SAR.2 ensures that only administrators can read the audit records.

To uphold the security of the audit records it must be ensured that they are sufficiently protected from unauthorised access. If the audit records are compromised it is not possible to hold users accountable and attackers will be able to cover their tracks. The component FAU_STG.1 (Protected audit trail storage) is therefore implemented to protect the audit records from unauthorised deletion as well as preventing unauthorised modification. Prevention has been chosen over detection since the audit records and the ability to hold users accountable is considered a vital part of the security of the TOE.

2.5.1.2 Access control

The security objective O.ACCESS requires that the two following access SFPs are implemented:

- A SWFS access SFP which enforces the TOE's overall access control requirements.
- A Workflow access SFP which enforces the each workflow instance's access SFP.

For specifying this the two components FDP_ACC.1 and FDP_ACF.1 is chosen from the two families Access control policy(FDP_ACC) and Access control functions(FDP_ACF). FDP_ACC.1 (Subset access control) identifies the access SFP by name and defines its scope of control, i.e. which subjects, objects and operations among these shall be covered by the SFP. FDP_ACF.1 (Security attribute based access control) describes the rules for a specified access control SFP in FDP_ACC.1.

To fulfill the requirement of O.ACCESS the components FDP_ACC.1 and FDP_ACF.1 has been iterated for each of the access SFPs. FDP_ACC.1(1) and FDP_ACF.1(1) defines and specifies the rules of the SWFS access SFP, while FDP_ACC.1(2) and FDP_ACF.1(2) does the same for the Workflow access SFP.

In order to enforce the SFPs the SWFSPP implements the two components FIA_ATD.1 (User attribute definition) and FIA_USB.1 (User-subject binding).

FIA_ATD.1 ensures that all users are associated with at least the following security attributes, other than the user's identity:

- user authentication credentials
- user role
- user history
- workflow groups

- workflow roles
- static privileges
- dynamic privileges

Each workflow role which belongs to the user must be associated with a workflow group which the user belongs to. The attributes are used in the enforcement of the SFPs.

FIA_USB.1 ensures that these security attributes are associated with the subjects which act on behalf of the user.

SWFS access SFP
Since the SWFS access SFP is applicable to the entire TOE, FDP_ACC.1(1) specifies that the SFP should be enforced on all subjects, all SWFS controlled objects and all operations among them. FDP_ACF.1(1) specifies that the access to objects shall be enforced based on at least the following:

- user identity, user role, workflow groups and user history associated with the subject
- the static privileges held by the subject to the object
- the dynamic privileges held by the subject to the object
- the set of active privileges held by the subject to the object

In order for an operation to be allowed the FDP_ACF.1.2 of FDP_ACF.1(1) specifies that the subject has the required privilege for the requested operation in its set of static or dynamic privileges and it must be possible to add the privilege to the subject's set of active privileges. FDP_ACF.1.3 specifies that if the subject already has the required privilege on the object in its set of active privileges it shall explicitly allow the operation. The FDP_ACF.1(1) is implemented such that a conforming PP/ST can specify additional rules and capabilities.

Workflow access SFP
The Workflow access SFP is specified similarly to the SWFS access SFP. The difference is that FDP_ACC.1(2) only specifies that the SFP should be enforced on subjects and objects referenced in a workflow instance's access SFP and on all operations between these subjects and objects. FDP_ACF.1(2) specifies that that access to objects shall be enforced based on at least the following security attributes related to the execution of workflows:

- workflow groups, workflow roles and user history

- the static privileges held by the subject to the object
- the dynamic privileges held by the subject to the object
- the set of active privileges held by the subject to the object

Although a workflow instance may not be aware of other workflow instances requirements can still be specified on workflow groups. E.g. it may be desired that a client does not simultaneously participate in workflows which are instances of the same process definition. Workflow roles are included for obvious reasons, since they specify the responsibilities within a workflow. User history is included such that binding or separation of duty requirements can be specified based on the history of the workflow.

The remaining rules of FDP_ACF.1(2) are equivalent to those of FDP_ACF.1(1).

2.5.1.3 Information flow control

The security objective O.FLOW requires that each user application, invokable application and SWFS the TOE interacts with is covered by a flow SFP. Additionally a Workflow flow SFP must be implemented which shall enforce each workflow instance's flow SFP.

The family Information flow control policy(FDP_IFC) and Information flow control functions(FDP_IFF) provides components for specifying this. Since the SWFSPP does not specify how the information flow control is to be enforced and how detailed it should be the SWFSPP suffices by including the two basic components FDP_IFC.1 (Subset information flow control) and FDP_IFF.1 (Simple security attributes). It is left to the conforming PP/ST to decide upon if these are sufficient or if hierarchical components should be chosen and if additional components of FDP_IFF should be included.

The requirement of the specification of application flow SFPs is implemented by FDP_IFC.1(1) and FDP_IFF.1(1). FDP_IFC.1(1) defines that application flow SFPs shall be enforced on subjects which cause information to flow to and from user applications, invokable applications or SFWSs. The SWFSPP does not make any requirements on how many application SFPs should be specified. It only requires that all applications and SWFSs are covered by a SFP and for each iteration of FDP IFC.1(1) a corresponding iteration of FDP IFF.1(1) must be made. All operations of FDP_IFF.1(1) have been left uncompleted, with the exception of the first assignment has been narrowed to an application flow SFP.

The Workflow flow SFP is implemented by FDP_IFC.1(2) and FDP_IFF.1(2). FDP_IFC.1(2) defines that the Workflow flow SFP shall be enforced on subjects and objects referenced in a workflow instance's flow SFP and all operations between these subjects and objects. Since the SWFSPP does not make any

specific requirements on how the information flow control is to be enforced FDP_IFF.1(2) suffices by specifying that the workflow SFP shall be enforced on at least the workflow groups and the workflow roles associated with the subject. Additional rules may be specified by the conforming PP/ST.

O.FLOW is additionally supported by the components FIA_ATD.1 and FIA_USB.1 described in section 2.5.1.2.

2.5.1.4 Identification and authentication

The objective O.AUTH requires the TOE to provide means for identifying and authenticating users before allowing access to the TOE and its resources. The class FIA (Identification and authentication) provides SFRs which can be used for ensuring this.

The families User identification(FIA_UID), User authentication(FIA_UAU) and User attribute definition(FIA_ATD) provides components to fulfill the objective. FIA_UID.2 (User identification before any action) and FIA_UAU.2 (User authentication before any action) are used for identifying and authenticating users.

FIA_UAU.7 (Protected authentication feedback) is implemented to ensure that the feedback given to the user during authentication is limited such that the risk of authentication data, and hereby the TOE being compromised, is decreased.

2.5.1.5 Session locking and re-authentication

The security objective O.SESSION requires functionality to make it possible to lock a session. The class FTA (TOE Access) provides the family Session locking(FTA_SSL) that provides components to address this. To fulfill the objective the components FTA_SSL.1 (TSF-initiated session locking) and FTA_SSL.2 (User-initiated locking) are implemented.

FTA_SSL.1 ensures that the TSF locks a session when a user has been inactive after some specified time interval. The SWFSPP leaves it to the conforming PP/ST to decide upon a reasonable time interval. It is noted that the time interval should be defined with respect to the implementation of the user-initiated locking (FTA_SSL.2). E.g. if the user-initiated locking is activated by the removal of a physical token, e.g. a smart card or a USB key, the time interval of user inactivity may be set to a very high value. The locking of the session is done by clearing the display devices and disabling any other user functionality other than unlocking the session. FTA_SSL.1 additionally requires that the user shall re-authenticate prior to unlocking the session.

FTA_SSL.2 ensures that the user is able to lock the user's own session. The

locking and unlocking is done analogously to FTA_SSL.1.

Since it is required that the user is able to re-authenticate, the component FIA_UAU.6 (Re-authenticating) is implemented. The component specifies that re-authentication at least is required when the session has been locked or terminated.

2.5.1.6 Backup and recovery

The objective O.RECOVER requires that administrators are provided with functionality which ensures the that the TOE can recover effectively after a system failure without compromising the security of the TOE. To ensure this the TOE shall among other things provide functionality supporting backups. The CC does not directly specify components to address backups and backup routines. The CC class FPT (Protection of the TSF) does however specify components which address TSF failure and recovery.

The component FPT_RCV.1 (Manual recovery) ensures that the TSF, in the event of failures specified by the conforming PP/ST, will enter a maintenance mode from where it can return to a secure state. E.g. if data is corrupted or lost an administrator use the backup to restore the data such that the TSF can return to its normal and secure operation. A secure state is a state where all SFPs are enforced, TSF and user data is consistent and the TOE is fully operational.

FPT_RCV.4 (Function recovery) ensures that the TSF provides additional protection in the event of a failure by ensuring that functions specified by the conforming PP/ST either completes successfully or recovers to a consistent and secure state.

Finally the component FPT_FLS.1 (Failure with preservation of secure state) ensures that the TSF in the event of a failure will preserve a secure state where all SFRs are enforced.

2.5.1.7 Protection of data flows

To protect the integrity of data flowing from and to the TOE as specified by O.DATAFLOW it must first be determined which types of data are transmitted. Between the TOE and user applications, trusted invokable applications and trusted SWFSs mostly application data will be transmitted. Application data, which is user data, can be protected with components from the class FDP (User data protection).

To protect the integrity of the application data transmitted the component FDP_UIT.1 (Data exchange integrity) is implemented. FDP_UIT.1 ensures that

the defined application flow SFPs are enforced to protect the integrity of all application data transmitted from the TOE and that the integrity of all application data is verified by the TOE upon receipt.

Additionally the components FDP_ITC.2 (Import of user data with security attributes) and FDP_ETC.2 (Export of user data with security attributes) ensure that one or more application flow SFPs are enforced when user data is imported or exported by the TOE respectively. Both components state that any associated security attributes are unambiguously associated with the user data. The components also allows for the specification of additional rules to be enforced during import/export. The reason for choosing these components, which supports security attributes, is that most SWFSs most likely will have to support this feature. This is especially convenient when e.g. application data are to be exported to trusted applications and re-imported later on.

FDP_ITC.2 has a dependency on FPT_TDC.1 (Inter-TSF basic TSF data consistency). FPT_TDC.1 ensures that security attributes shared between the TSF and other trusted applications is interpreted consistently and that a list of interpretation rules can be applied.

Although mainly application data will be transmitted, TSF data may also need to be transmitted. E.g. process definitions and other workflow related TSF data may need to be exchanged with other SWFSs. Such protection is provided by the class FPT (Protection of the TSF).

The component FPT_ITI.1 (Inter-TSF detection of modification) ensures that the TSF is capable of detecting modifications to all TSF data transmitted or received by the TSF.

2.5.1.8 Trusted applications

The objective O.TRUSTED requires that additional assurance of the trusted invokable applications and SWFSs is given. This can be directly achieved by implementing the component FTP_ITC.1 (Inter-TSF trusted channel). The component ensures that the TSF provides a trusted communication channel which is logically distinct from other communication channels and provides assured identification of its end points.

The TSF shall permit the TSF and/or one or more SWFSs to initiate communication via the trusted channel. The TSF shall use the trusted channel for at least establishing a connection with a SWFS or an invokable application.

2.5.1.9 Security management

Both the security objective O.MANAGE and O.WORKFLOW requires that certain management functionality is provided. CC provides the class FMT (Security management) to address this. Some of the components can be selected directly based on the security requirements of the TOE. Other components are more easily selected when the SFRs of other classes have been selected, since they may have dependencies on management components. E.g. both FDP_ACF.1 and FDP_IFF.1 has a dependency on FMT_MSA.3 (Static attribute initialisation) which again has dependencies on FMT_MSA.1 (Management of security attributes) and FMT_SMR.1 (Security Roles).

FMT_MSA.3 specifies that the TSF shall enforce the defined SFPs in order to provide restrictive default values for the security attributes used to enforce the SFPs. Additionally it is stated that administrators are allowed to override the default initial values with alternative ones.

To fulfill the management requirements of O.MANAGE and O.WORKFLOW the component FMT_MSA.1 is iterated three times.

FMT_MSA.1(1) specifies that the SWFS access SFP shall restrict the ability to modify at least the following user attributes to administrators:

- user identity
- user role
- user history
- static privileges

FMT_MSA.1(2) specifies that the Workflow access SFP shall restrict the ability to modify at least the following user attributes to managers:

- workflow group
- workflow role

Finally FMT_MSA.1(3) specifies that the Workflow access SFP shall be enforced to restrict the client who owns the session from modifying the session's set of active privileges.

The component FMT_SMR.1 specifies the security roles which users can be associated with. As described in section 2.2.1.2 the TOE supports the following roles:

- Administrator

- Manager
- Client

The component of FMT_MTD.1 (Management of TSF data) allows for users to manage TSF data. In relation to O.MANAGE, FMT_MTD.1(1) restricts the ability to perform one or more operations specified by a conforming PP/ST on the audit data to administrators. FMT_MTD.1(2) restricts the ability to query and/or modify the set of audited events to administrators. FMT_MTD.1(3) restricts the ability to perform operations on TSF data which is related to the overall security of the TOE to administrators. Such data includes:

- SFWS access control SFP
- application flow SFPs
- Workflow access SFP
- Workflow flow SFP
- identification and authentication data
- mapping of authorised users to roles

In relation to O.WORKFLOW, FMT_MTD.1(4) restricts the ability to manage process definitions and perhaps other workflow related TSF data to managers. FMT_MTD.1(5) restricts the ability to manage workflow instances to managers and perhaps other authorised identified roles.

Through the implementation of FMT_MOF.1 (Management of security functions behaviour) administrators are additionally restricted with the ability to manage the behavior of at least the security functions:

- implementing the user identification and authentication mechanisms
- implementing the association between TOE roles and individual users
- controlling the behaviour of the audit generation
- implementing the SWFS access SFP
- implementing the Workflow access SFP
- implementing the application flow SFPs
- implementing the Workflow flow SFP
- implementing the TOE backup and recovery routines

- implementing the session locking methods

The component FMT_SMF.1 (Specification of management functions) which FMT_MSA.1, FMT_MTD.1 and FMT_MOF.1 has dependencies on specifies the management functions which the TSF shall be capable of performing. The component is necessary since the other management components only specify restrictions on who may use the different management functions. The identified management functions are:

- assign and maintain lists of authorised users
- manage object security attributes
- manage user security attributes
- manage and review the audit data
- manage the SFWS access SFP
- manage the Workflow access SFP
- create manage the application flow SFPs
- manage the Workflow flow SFP
- manage process definitions and workflow instances
- monitor workflow instances
- create and recover backups
- manage the session locking methods

2.6 Security assurance requirements

To assure that a TOE meets the set of specified SFRs the TOE must be evaluated. In the context of CC the evaluation is based on the fulfillment of security assurance requirements(SARs). CC Part 3[10] provides an extensive catalog of predefined SARs, which a PP/ST may require the TOE to be evaluated against in order to assure that it is conformant. CC Part 3 is organised into classes, families and components in the same manner as CC Part 2. Each assurance component contains a number of action elements which belong to one of the following three sets:

Developer action elements which defines the activities to be performed by the developer.

Content and presentation of evidence elements which defines the required evidence, what the evidence shall demonstrate and what information the evidence shall convey.

Evaluator action elements which defines the activities to be performed by the evaluator.

To assist in the selection of SARs CC Part 3 defines 7 packages of SARs, the so called Evaluation Assurance Levels(EALs). Each EAL provides an increasing level of assurance. The goal of the EALs is to provide an increasing scale that balances the level of assurance with the cost and feasibility of acquiring the chosen level.[10]

To provide flexibility an EAL may be augmented with SARs which expresses a higher level of assurance than the original SARs or by adding additional SARs.

2.6.0.10 SWFSPP security assurance requirements

Since it is expected that the TOE of the SWFSPP is deployed in an environment with a medium level of risk, it has been found that the level of EAL3 augmented with ALC_CMS.4 provides a sufficient level of assurance.

EAL3 provides a moderate level of independently assured security. EAL3 has been chosen over EAL2 because it requires more complete testing coverage of the security functionality and mechanisms/procedures which ensure a higher level of security in the development environment. The augmented assurance required provides added assurance that flaws are tracked and resolved during development. The chosen assurance requirements are listed in table 2.2.

2.7 PP conclusion

A Protection Profile for a Secure Workflow System has been developed. The PP fulfills the content requirements which are outlined in CC Part 1[8] and clearly specified in the class APE: Protection Profile evaluation of CC Part 3[10].

A high level model defining a Secure Workflow System(SWFS) has been created. The model has on purpose been created such that almost any type of workflow system where data protection and user accountability are priorities can claim conformance.

In the defined SWFS model emphasis is particularly put on the protection of application data through the specification of both access SFPs and flow SFPs. This is especially important since a workflow system integrates multiple applications and supports the execution of business processes which may require

Assurance class	Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 2.2: Security assurance requirements of EAL3 augmented with ALC_CMS.4.

to be kept separate. Most likely this would both give rise to access control requirements on data as well as information flow control requirements.

EAL3 augmented with ALC_CMS.4 has been chosen as the appropriate assurance level. ALC_CMS.4 has been included since it is found important that flaws in the TOE are consistently tracked such that they can be resolved during development. This may assist to ensure that a TOE with less flaws and thereby a more secure TOE is developed.

An important issue in the PP development has been to ensure that the security requirements have been specified such that different STs can claim conformance. Additionally much effort has been put into ensuring that the security requirements are within a realistic scope. This is especially important for the PP since its main goals is to provide a basic set of security requirements for a specific TOE type which STs can and will claim conformance to.

For future versions of the SWFSPP it might be considered to remove the assumption AC.RESOURCE, since it perhaps requires too much of the IT environment. This will require the TOE to implement security functionality which is able to counter and mitigate resource exhaustion. CC Part 2 includes several SFRs which may assist in accomplishing this.

Chapter 3

Security Target

This chapter describes the development and content of the Security Target(ST) for a centralised Secure Workflow System, which conforms to the Secure Workflow Systems Protection Profile(SWFSPP). The Centralised Secure Workflow System Security Target is attached as appendix B.

3.1 ST development

The next step in the process of developing a Secure Workflow System(SWFS) using the CC is to create a Security Target(ST). The development of the ST is based upon the ST content requirements as specified in appendix A of Common Criteria (CC) Part 1[8] and which are summarised in section 1.7.4.

The goal is to develop a ST for a Secure Workflow System which is based on a centralised architecture. The ST shall conform with the earlier developed SWFSPP(appendix A).

The first step is to identify the specific Target of Evaluation(TOE) which the ST is to be developed for. This is done in section 3.2. The remaining sections of the chapter describes chronologically the sections of the developed ST.

The official CC website[1] provides a comprehensive list of products evaluated against certified STs. No ST has been found to directly target the area of

[1] http://www.commoncriteriaportal.org

workflow or workflow systems. STs related to application integration is however available. This includes WebSphere MQ EAL4 Security Target[12] used for evaluating IBM WebSphere MQ 6.0.1.1 and the ST used for evaluating webMethods Fabric 6.5[7]. The workflow functionality of these two products has not been considered part of the TOE in their STs. They do nevertheless provide similar functionality and have therefore been found helpful in the development of the ST. Other STs which have been used for inspiration include:

- Security Target for Citrix MetaFrame XP Presentation Server[5]
- Security Target for IBM z/VM Version 5 Release 1[6]
- Microsoft Windows 2003/XP Security Target[11]

Additionally inspiration has been found in the master thesis Security in POS Systems[21], which in a similar manner to this thesis has developed a PP and ST for Point-of-Sale systems.

3.2 The TOE

The TOE shall fulfill the requirements of the SWFSPP, while specifying a specific TOE. To keep within the time available for developing the ST it is chosen that the TOE shall employ a centralised architecture. The advantage of a centralised architecture is that it provides a less complex model than that of a distributed one. The specific security problems within a distributed environment, such as synchronisation of data, are hereby also avoided.

Since the ST must conform to the SWFSPP the ST TOE provides all of the security functionality of the SWFSPP TOE (section 2.2.2). Table 3.1 shows which security functionality will be provided completely by the TOE and which will be provided in co-operation with the IT environment.

Completely	**In co-operation**
Identification and authentication	Secure audit storage
Access control	Backup
Information flow control	
Audit generation	
Secure audit review	
Authorised administration	

Table 3.1: Overview of which security functionality will be provided by the TOE and which will be provided in co-operation with the IT environment.

The TOE of the ST will additionally provide:

Adaptive recovery through the editing of process definitions and workflow instances.

In addition the TOE will in co-operation with the IT environment provide:

Cryptographic support for ensuring that sensitive information can be adequately protected when it is transferred from and to the TOE.

The TOE roles (section 2.2.1.2) and the primary TOE assets(section 2.2.1.1) remain unchanged.

3.2.1 TOE model

The SWFS model(section 2.2.1) describes the TOE at a very high abstraction level. It is the task of the ST to give a more specific although still a high level model of the TOE. This is done in the TOE description(section B.1.3) of the ST.

The TOE of the Centralised Secure Workflow System ST consists of two components:

The Workflow System Application which provides the main functionality of the TOE. The Workflow System Application is hosted on a server and manages the execution of workflows and implements all of the security functions of the TOE. Interfaces are provided for both the Trusted Client Application as well as other user applications. Furthermore interfaces are provided for invocation of applications and communication with other SWFSs.

The Trusted Client Application which ensures that when the application is running it provides the only visible graphical user interface on the machine. The Trusted Client Application is run on trusted client machines and ensures that the information flow policies of the TOE are enforced. E.g. it should not be possible for a client to copy information from the Trusted Client Application to a local application using the OS window manager's cut/copy and paste functionality and vice versa. The Trusted Client Application is the only client application which may send and receive application data which has a sensitivity level above public (see section 3.2.1.1).

Figure 3.1 illustrates the physical scope of the TOE. The shaded components are the TOE, while the remaining ones are part of the IT environment.

In the following sections it is described how the TOE implements the information flow control policies required by the SWFSPP. In addition the added TOE

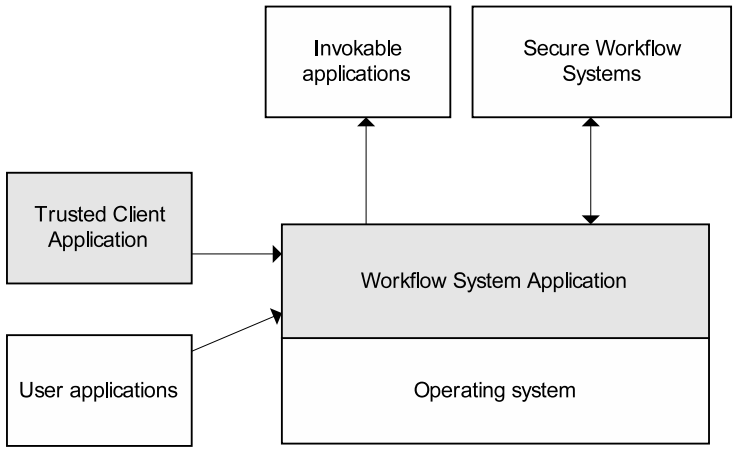

Figure 3.1: The physical scope of the TOE. The shaded components are the TOE. The unshaded components is the IT environment. The direction of the arrows indicate which component initiates communication.

security functionality is described in more detail. The full description of the TOE security functionality is available in section B.1.3.2.

3.2.1.1 Information flow control

The SWFSPP specifies that information flow control shall be used to protect application data from unauthorised access through the specification of a workflow SFP. In addition it is required that all invokable applications and SWFSs which the TOE communicates with are covered by an application flow SFP. This section describes how this is is accomplished.

For the enforcement of information flow control, the TOE provides support for the classification of data with a sensitivity label. The TOE supports two labels 'public' and 'private'. The 'private' label is associated with a set of workflow groups in which the data should be kept private. I.e. it should not be possible to make private data available outside of the specified workflow groups. Data which is classified as 'public' have no restrictions and may flow from and to any TOE user. Figure 3.2 illustrates the hierarchical structure of the sensitivity labels within a system with three workflow groups.

The sensitivity labels form a partial ordering which employs the concept of no-read up, no-write down. The partial ordering of sensitivity labels is defined by the following rules:

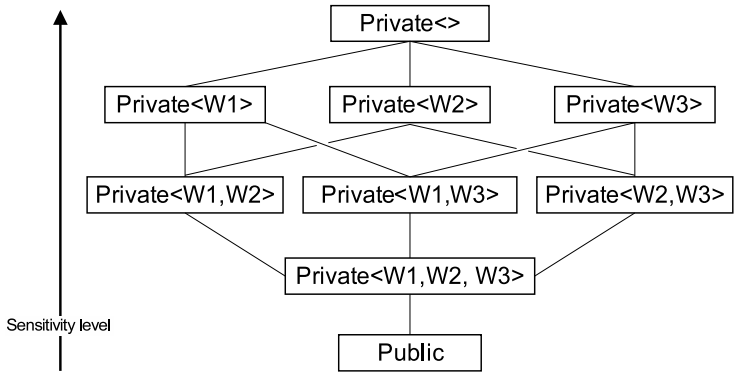

Figure 3.2: Sensitivity levels which can be assigned to application data within a system with three workflow groups.

- The sensitivity label of an object A is greater than that of object B if one of the following conditions exist:
  - The sensitivity label of A is private$\langle X \rangle$, where X is the set of workflow groups where the object is private and the sensitivity label of object B is public.
  - The sensitivity label of A is private$\langle X \rangle$ and the sensitivity label of B is private$\langle Y \rangle$ and X is a proper subset of Y ($X \subset Y$).
- The sensitivity label of an object A is equal to that of object B if one of the following conditions exist:
  - The sensitivity label of A is public and the sensitivity label of B is public.
  - The sensitivity label of A is private$\langle X \rangle$ and the sensitivity label of B is private$\langle Y \rangle$ and the set X is equal to the set Y.
- The sensitivity label of an object A and object B is incomparable if they are not equal and neither has a greater sensitivity label than the other.

The classification of application data is specified within the process definition's process flow SFP. The process flow SFP specifies how data created during the workflow is to be classified. Classification may be controlled entirely by the process flow SFP or it may specify that certain roles may classify data according to specified rules. Additionally it may be specified when and how data may be declassified, that is lowering the sensitivity level of data.

A workflow example where declassification could be required is the publishing of a report. It may be required that the report should be kept private during

its preparation while the published report should be public. To obtain this the flow SFP may specify that the executor of the final task of releasing the report may declassify the report from private to public.

To conform to the Secure Workflow Systems Protection Profile each user application, invokable application and SWFS, which the TOE may communicate with, has to be covered by an application flow SFP. The TOE of this ST fulfills this requirement by defining the following application flow SFPs:

- Limited application flow SFP
- Basic application flow SFP
- Advanced application flow SFP

In order that an application may interact with the TOE it is required that it is covered by one of these SFPs.

If an application is covered by the Limited application flow SFP the TOE may only send information of public sensitivity to it. All information received from the application shall by default be classified as public.

If an application is covered by the Basic application flow SFP the application must be CC certified at EAL3 or higher. The TOE may only send information of public sensitivity to the application. Information of any sensitivity level may be received from the application.

If an application is covered by the Advanced application flow SFP the application must be CC certified at EAL3 or higher and be capable of enforcing the Workflow flow SFP. Information of any sensitivity level may be sent and received by the TOE.

The Trusted Client Application provides protection of application data by enforcing the Workflow flow SFP and the Advanced application flow SFP such that clients are prevented from bypassing the information flow control rules of the TOE.

3.2.1.2 Cryptographic support

All communication with the Workflow System Application is done across an insecure network. The SWFSPP only specifies that the integrity of transmitted data shall be protected. This may be sufficient when no confidentiality requirements exists on the application data and when TSF data is only transferred using local interfaces. If TSF data or confidential application data is to be transmitted across a network the following options to protect the confidentiality of the data may be considered:

- The network in which the data flows is secured in a way that prevents eavesdropping.
- The data is logically secured using cryptography.

The second option was chosen because it is more viable and mainly comes at a cost of increased computation and thereby also a delay in the transmission of the data. The cryptographic support is provided in co-operation with the IT environment or more precisely the operating system(OS). To ensure that both the integrity and confidentiality of data is properly protected the OS is required to provide a cryptographic service provider (CSP) which is FIPS140-2 certified. It is the task of the Workflow System Application to ensure that only FIPS140-2 compliant algorithms are used. Cryptographic support is in addition used to mutually authenticate TOE components, invokable applications, SWFSs and users.

3.2.1.3 Adaptive recovery

To make the TOE more resistant against semantic failures the TOE provides managers with the capability to modify workflow instances. Semantic failures are caused due to failures in the execution of workflow instances e.g. unavailability of resources, internal decisions or failure in an invoked application. By providing the possibility to modify workflow instances it may be possible to recover from an error, caused due to a semantic failure.

The modification of a workflow instance is either achieved by propagating changes in workflow instance's process definition to the workflow instance or by directly modifying the workflow instance. A more detailed description of the modification of workflow instances is given in the Security management paragraph of section B.1.3.2.

3.3 Security problem definition

This section describes the security problem definition of the Centralised Secure Workflow System ST. All assumptions, threats and organisational security policies(OSPs) of the SWFSPP are part of the ST.

Because the ST is developed for a specific TOE this may give rise to new threats and OSPs. Since the ST is to conform to the SWFSPP the Common Criteria(CC) allows for no additional assumptions to be made on the operational environment. The full security problem definition can be seen in section B.3.

In the following section the new threats to be countered by the TOE and its operational environment and the OSPs to be enforced are identified.

3.3.1 Threats

T.TRUST_CLIENT *An attacker may impersonate the Trusted Client Application and thereby be able to disclose confidential information.*

Since the Trusted Client Application is specifically trusted to fulfill the application data information flow requirements an attacker may try to impersonate it. By impersonation the attacker may be able to receive sensitive data from the Workflow System Application, which believes it is communicating with the authentic Trusted Client Application.

T.TRUST_SERVER *An attacker may impersonate the Workflow System Application and gain access to user authentication information, which can be used to gain unauthorised access to the Workflow System Application.*

The threat appears since it is a security risk if an application believes it is communicating with the Workflow System Application when it is not. Such a situation may lead to disclosure of user authentication data which can be used to get unauthorised access to the TOE. Also sensitive data may be disclosed.

T.SECRET_FLOW *The confidentiality of information flowing across a network from and to the TOE is disclosed to an attacker.*

The threat is included since sensitive data may be transmitted from and to the TOE.

T.CRYPTO_KEYS *An attacker compromises the security of the TOE by disclosing cryptographic keys used for securing information flowing to and from the TOE.*

The disclosure of cryptographic keys will compromise the security of the TOE. If keys are obtained by an attacker the confidentiality and integrity of the transmitted information will be compromised.

3.3.2 Organisational security policies

P.FIPS140 *All cryptographic functions used by the TOE shall be FIPS PUB 140-2 compliant.*

The policy is specified such that all cryptographic functions shall be compliant to FIPS PUB 140-2. This shall ensure that trusted algorithms are used and the cryptographic functions implement them as intended.

P.TRUST_CLIENT *The Trusted Client Application shall be installed and configured in a manner that maintains the security of the TOE.*

The policy is specified to ensure that the Trusted Client Application can be trusted to operate in the manner it was intended.

P.USER_AUTH *Administrators and managers shall be required to authenticate using token and token PIN.*

The policy is specified to ensure that the authentication credentials of administrators and managers are of a sufficient quality. Since the administrators and managers manage the security of the TOE it is deemed that two-factor authentication is appropriate.

3.4 Security objectives

This section describes the security objectives of the ST. Besides the security objectives of the SWFSPP a number of new security objectives have been stated to counter the new threats and enforce the new OSPs.

The mapping between security objectives and threats and OSPs is shown in table 3.2.

It can be seen from table 3.2 that the new security objectives besides of countering the new threats and enforcing the new OSPs also assists in the countering and enforcing of some of the SWFSPP threats and OSPs.

3.4.1 Security objectives of the TOE

The following new security objectives of the TOE, relative to the SWFSPP, are identified:

	T.ACCESS	T.DATA	T.DATAFLOW	T.TRUST_CLIENT	T.TRUST_SERVER	T.SECRET_FLOW	T.CRYPTO_KEYS	P.FIPS140	P.TRUST_CLIENT	P.USER_AUTH
O.AUTHENTIC	x				x		x			
O.AUTH_CLIENT		x		x			x			
O.FIPS140			x	x	x	x	x	x		
O.SECRET_FLOW						x				
O.USER_AUTH										x
OE.CRYPTO_KEYS							x			
OE.FIPS140			x	x	x	x	x	x		
OE.TRUST_CLIENT									x	

Table 3.2: Tracing of additional security objectives to threats and OSPs.

O.AUTHENTIC *The Workflow System Application shall authenticate itself to the user before allowing any communication.*

The objective is identified to counter T.TRUST_SERVER by ensuring that the Workflow System Application always authenticates itself to the applications it communicates with. The objective indirectly counters T.ACCESS and T.CRYPTO_KEYS since the risk of disclosure of authentication data and cryptographic keys are minimized.

O.AUTH_CLIENT *The Trusted Client Application and the Workflow System Application shall mutually authenticate using a trusted channel before allowing any communication.*

The objective is identified to counter T.TRUST_CLIENT by ensuring that it is not possible to impersonate the Trusted Client Application. The objective hereby also counters T.CRYPTO_KEYS, since the risk of cryptograhic keys being compromised is decreased.

O.FIPS140 *The cryptographic functions used by the TOE shall be FIPS140-2 compliant.*

The objective is mainly identified to enforce P.FIPS140

in order to ensure that all cryptographic functions used are FIPS140-2 compliant. Additionally it indirectly counters T.DATAFLOW, T.TRUST_CLIENT, T.TRUST_SERVER, T.SECRET_FLOW and T.CRYPTO_KEYS since it is ensured that the cryptographic functions used to counter these threats are of a sufficient quality.

O.SECRET_FLOW *The confidentiality of all data which is received and sent through the TOE interfaces must be protected.*

The objective is identified to counter T.SECRET_FLOW by ensuring that the confidentiality of all data is protected during transmission.

O.USER_AUTH *The TOE shall provide the following authentication mechanisms where the use of username and password is restricted to clients:*

- *token and token PIN*
- *username and password*

The objective directly counters O.USER_AUTH by requiring that administrators and managers shall use token and token PIN for authentication. Additionally it specifies that username and password may be used for client authentication.

3.4.2 Security objectives of the operational environment

The following new security objectives of the operational environment, relative to the SWFSPP, are identified:

OE.CRYPTO_KEYS *Cryptographic keys must be securely administered and protected from disclosure.*

The objective is identified to counter T.CRYPTO_KEYS by ensuring that the cryptographic keys which are entirely managed by the operating system are properly protected.

OE.FIPS140 *The operational environment shall ensure that the cryptographic service provider (CSP) provided to the TOE by the OS is FIPS140-2 compliant.*

The objective is identified to enforce P.FIPS140. Since the cryptographic support of the TOE is provided in co-operation with the operating system this objective is necessary to ensure that only FIPS140-2 implemented algorithms are used. As for O.FIPS140 the objective indirectly counters T.DATAFLOW, T.TRUST_CLIENT, T.TRUST_SERVER, T.SECRET_FLOW and T.CRYPTO KEYS.

OE.TRUST_CLIENT *The operational environment shall ensure that the Trusted Client Application is installed and configured on client machines which are installed and configured by an administrator in a way that maintain the security of the TOE.*

The objective is identified to directly enforce P.TRUST_CLIENT.

3.5 Security functional requirements

As new security objectives have been defined relative to the SWFSPP new security functional requirements(SFRs) have been derived from these. The mapping between all of the STs security objectives to SFRs are shown in table B.5. Table 3.3 lists the SFRs which are new relative to the SWFSPP.

In the following sections it is described how the uncompleted assignments and selections of the SWFSPP are completed in the ST. It is described which components of the SWFSPP have been iterated to fulfill the security objectives and the the new SFRs are described. As in section 2.5.1 the SFRs are divided into the TOE's security functional areas. The full list of SFRs is available in section B.5.1.

3.5.0.1 Security audit

The assignments of the components FAU_GEN.1 has been completed such that all auditable events for the detailed level of audit are to be recorded. This ensures that administrators have a detailed audit trail available for detecting attempted or successful security violations as well as for holding users accountable for their actions.

SFR	Description
FCS_COP.1	Cryptographic operation
FDP_IFC.1(1.1)	Subset information flow control (Limited application flow SFP)
FDP_IFC.1(1.2)	Subset information flow control (Basic application flow SFP)
FDP_IFC.1(1.3)	Subset information flow control (Advanced application flow SFP)
FDP_IFF.1(1.1)	Simple security attributes (Limited application flow SFP)
FDP_IFF.1(1.2)	Simple security attributes (Basic application flow SFP)
FDP_IFF.1(1.3)	Simple security attributes (Advanced application flow SFP)
FDP_IFF.2	Hierarchical security attributes (Workflow flow SFP)
FDP_ETC.1	Export of user data without security attributes (Limited)
FDP_ITC.1	Import of user data without security attributes (Limited)
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.3	Integrity monitoring
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_SOS.1	Verification of secrets
FIA_UAU.5	Multiple authentication mechanisms
FMT_MSA.1(4)	Management of security attributes (Workflow flow SFP)
FMT_MTD.1(6)	Management of TSF data (Modification of instances)
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITT.1	Basic internal TSF data transfer protection
FTP_ITC.1(2)	Inter TSF trusted channel (Client–Server)

Table 3.3: New SFRs which are required by the TOE in addition to those specified in the SWFSPP. Components marked in italic are iterations of SWFSPP components. Components in bold are components where a hierarchical component has been chosen over the original SWFSPP component.

3.5.0.2 Access control

The assignments of the components FDP_ACC.1(1), FDP_ACF.1(1), FDP_ACC.1(2), FDP_ACF.1(2), FIA_ATD.1 and FIA_USB.1 have been completed such that no changes to the SFRs related to access control are made compared to the SWFSPP.

3.5.0.3 Information flow control

To fulfill the objective of O.FLOW it has been necessary to iterate FDP_IFC.1(1) and FDP_IFF.1(1) one time for each of the three application flow SFPs specified in the ST. FDP_IFC.1(1.1) specifies the requirements of the Limited application flow SFP, FDP_IFC.1(1.2) those of the Basic application flow SFP and FDP_IFC.1(1.3) those of the Advanced application flow SFP.

The components FDP_ITC.2 and FDP_ETC.2 have been assigned such that when information is imported from and exported to applications covered by either the basic or Advanced application flow SFP the security attributes associated with the information are used. To ensure a consistent interpretation of the sensitivity labels of objects FTP_TDC.1 ensures that the sensitivity label of an object imported by the TSF from a trusted application is verified against the partial ordering of sensitivity labels. If the sensitivity label is invalid it shall be interpreted as being public and changed to public. This ensures that no invalid sensitivity labels are imported into the TOE.

Since the Limited application flow SFP covers applications which are only trusted to handle public information it is reasonable to assume that the applications are not trusted to be able to handle the associated security attributes. Therefore the components FDP_ITC.1 and FDP_ETC.1 have been assigned such that it is ensured that the associated security attributes are removed and ignored.

In relation to the enforcement of the Workflow flow SFP the component FDP_IFF.2 Hierarchical security attributes replaces FDP_IFF.1(2). This is allowed since the new component is hierarchical to the old one. FDP_IFF.2 is chosen such that the Workflow flow SFP may enforce the information flow rules described in section 3.2.1.1 based on the sensitivity labels of objects.

3.5.0.4 Identification and authentication

The identification and authentication SFRs of the SWFSPP remain unchanged with the exception of FIA_UAU.7. The assignment of the component is completed such that only obscured feedback is given during user authentication. This means that the TSF does not produce a visible display of any of the actual

authentication data.

The component FIA_UAU.5 (Multiple authentication mechanisms) is selected to fulfill the requirements of O.USER_AUTH. FIA_UAU.5 ensures that the required authentication mechanisms are provided and that username and password authentication is restricted to clients. FIA_SOS.1 (Verification of secrets) is refined and assigned such that the administrators are able to define a password policy which all passwords should satisfy. This is done to ensure that only passwords of a sufficient quality are used.

The objective O.AUTHENTIC requires that the Workflow System Application authenticates itself to those who connects to it. Although this specifies a very common requirement within IT systems no SFR directly deals with this. The requirement has therefore been fulfilled indirectly by FDP_UAU.5, even though it addresses which authentication mechanisms shall be provided to the user. A satisfactory result has been obtained by stating, in the rules describing how the multiple authentication provide authentication, that the Workflow System Application should authenticate itself to the user. Additionally the component ensures that the Workflow System Application authenticates itself using a X.509 certificate.

3.5.0.5 Session locking and re-authentication

No additional requirements have been made on when re-authentication is required. The TSF initiated session locking has been assigned to happen after an administrator specified time interval of user inactivity, which may be dependent on the authentication mechanism used.

3.5.0.6 Backup and recovery

The assignments of the components FPT_FLS.1, FPT RCV.1 and FPT RCV.4 are completed such that failures are divided into system failures and semantic failures. System failures includes failures in the underlying infrastructure such as the OS or hardware and failures of TOE components. Semantic failures are failures which are associated with the execution of workflow tasks e.g. unavailability of resources or internal decisions.[14]

The components ensure the following:

- In the event of a system failure or semantic failure the TSF will preserve a secure state.
- After a system failure the TSF will enter a maintenance mode where the ability to return to a secure state is provided.

- In the event of a system failure the backup and recovery functions will either complete successfully or recover to a consistent and secure state.

3.5.0.7 Protection of data flows

The addition of the objective O.SECRET_FLOW requires that components are selected which protects the confidentiality of the transmitted data. The components FDP_UCT.1 (Basic data exchange confidentiality) and FPT_ITC.1 (Inter-TSF confidentiality during transmission) achieve this for user data and TSF data respectively.

Because the TOE is separated into two components which communicate over an insecure network it is necessary to add the components FDP_ITT.1 (Basic internal transfer protection) and FPT_ITT.1 (Basic internal TSF data transfer protection) in order to fulfill the objectives of O.DATAFLOW and O.SECRETFLOW. The components ensure that the integrity and confidentiality of application data (user data) and TSF data transmitted between the Workflow System Application and the Trusted Client Application is protected. The component FTP_ITT.3 (Integrity monitoring) provides additional guarantee that integrity errors are handled.

3.5.0.8 Mutual authentication between TOE components

The objective O.AUTH_CLIENT requires that the Trusted Client Application and the Workflow System Application mutually authenticate before any communication is allowed. CC Part 2 contains the component FTP_ITC.1 Inter-TSF trusted channel which may be used to fulfill this requirement between the TSF and a remote trusted IT product. No SFR has however been found to achieve this between separate parts of the TOE. The FTP_ITC.1(2) component has therefore been refined such that it specifies that the TSF shall provide a trusted channel between the Trusted Client Application and the Workflow System Application. The required mutual authentication can hereby be specified.

It may be argued that a better solution would have been to create an extended component since the refinement changes the originally Inter-TSF component into being an Internal TOE trusted channel. It is however considered that since the extent of the refinement is quite small it may be allowed.

The objective is additionally supported by FCS_COP.1 which ensures that the cryptographic functions used for the authentication are FIPS140-2 compliant.

3.5.0.9 Cryptographic support

The component FCS_COP.1 (Cryptographic operation) is chosen to fulfill O.FIPS140, but also to support O.SECRET_FLOW and O.AUTH_CLIENT. The component ensures that all data sent from the TOE are encrypted and that cryptographic functions are used to perform mutually authentication between the two TOE components. It is specified that cryptographic operations shall meet the requirements of FIPS140-2 and that one of the following TLS cipher suites are to be used:

- ***TLS_RSA_WITH_AES_128_CBC_SHA, or***
- ***TLS_RSA_WITH_AES_256_CBC_SHA.***

FCS_COP.1 has a dependency on FCS_CKM.4 (Cryptographic key destruction) which is not satisfied by the TOE. The dependency is however indirectly satisfied by the OS which provides the cryptographic service.

3.5.0.10 Security management

Since additional security functionality has been added, it is required that changes are made to some of the management SFRs of the SFWSPP in order to fulfill O.MANAGE. This includes the addition of functions for controlling the cryptographic functions used and defining the password policy, which is specified in FMT_SMF.1. FMT_MOF.1 ensures that these functions are restricted to administrators.

Because sensitivity labels are used in the enforcement of the Workflow flow SFP the component FMT_MSA.1(4) is added. It ensures that only those who are authorised by the workflow instance's flow SFP are allowed to modify the sensitivity label of a workflow object.

The remaining assignments and selections of the FMT components are completed such that:

Administrators are restricted to:

- Create, move and delete audit logs (FMT_MTD.1(1))
- Query and modify the set of audited events (FMT_MTD.1(2))
- Initialize and modify the(FMT_MTD.1(3)):
  - SFWS access control SFP
  - application flow SFP(s)

  - Workflow access SFP
  - Workflow flow SFP
  - identification and authentication data
  - mapping of authorised users to roles
  - password policy

Managers are restricted to:

- Create, modify and delete process definitions (FMT_MTD.1(4))
- Modify workflow instance (FMT_MTD.1(6))

Managers and users which have been explicitly authorised for a specific set of workflow instances are restricted to:

- Create, suspend, terminate, monitor and delete workflow instances (FMT_MTD.1(5))

3.6 Security assurance requirements

The TOE now supports the transmission of sensitive data and additional security objectives have been identified. This does nevertheless not change that the overall threat level is considered to be medium. EAL3 augmented with ALC_CMS.4 therefore still provides a reasonable level of assurance.

3.7 TOE summary specification

The TOE summary specification describes the general mechanisms used by the TOE to satisfy the SFRs. The identified security functions are derived from the identified security functional areas. Table 3.4 lists the required ST security functions. Since the security functions are closely related to the already described SFRs and the concrete specifications of the TOE described in chapter 4 these are not described here. The full TOE summary specification is available in section B.6.

3.8 ST conclusion

A Security Target for a centralised Secure Workflow System has been developed, which conforms to the Secure Workflow Systems Protection Profile(SWFSPP).

Security functions	Sub-functions
Security audit	Audit generation and recording Audit review Audit protection
Cryptographic support	
Protection of data	Access control Information flow control Backup and recovery
Identification and authentication	User attributes Mutual authentication Session locking and re-authentication Protected authentication feedback
Security Management	Security Roles Administrative interface Workflow management interface Client interface
Secure communication	User applications Trusted external applications Trusted Client Application Importation and exportation

Table 3.4: Overview of TOE summary specification security functions.

The ST fulfills the content requirements which are outlined in CC Part 1[8] and clearly specified in the class ASE (Security Target evaluation) of CC Part 3[10].

A more refined model of the SWFS model of the SWFSPP has been defined and described. The refined model describes the TOE and its boundaries in relation to the IT environment. Since the ST TOE only allows for remote access across an insecure network it was necessary to add the Trusted Client Application to the model in order to enforce the flow control requirements of sensitive data. The TOE hereby consists of a Workflow System Application, which provides the functionality of the SWFS, and a Trusted Client Application which ensures that the ST information flow control requirements are enforced. The refined model gives rise to a number of new threats and OSPs. To counter the new threats and enforce the new OSPs, new security objectives have been identified and new SFRs have been specified.

The assurance level of EAL3 augmented with ALC_CMS.4 specified by the SWFSPP is still found appropriate, since it is considered that the level of threat against the TOE has not been increased. CC Part 3 may however be subject to a more thorough examination in order to identify assurance requirements which are considered relevant.

The requirement that the ST shall conform to the PP has made the ST devel-

opment easier and has helped in making the ST more organised and consistent.

For future versions one might consider developing more detailed application flow SFPs. This could be done by categorising applications into groups of functionality e.g. data repositories, word processors, financial application etc.

A relevant addition may also be configuration management of the primary TOE assets. This will ensure that data can be reverted to a previous version when erroneous changes are made or when unforeseen failures occur.

Chapter 4

Design

In this chapter concrete design specifications of a centralised Secure Workflow System is given. The design is to be compliant with the Centralised Secure Workflow System Security Target (appendix B).

4.1 Introduction

To obtain compliance with a Security Target(ST) the Common Criteria(CC) requires the developer to provide several development documents describing the security functionality of the Target of Evaluation(TOE). For Evaluation Assurance Level(EAL) 3 the CC requires a functional specification(ADV_FSP.3), a specification of the architectural design(ADV_TDS.2) and a security architecture description(ADV_ARC.1). This chapter will focus on the first two documents.

4.2 Functional specification

The functional specification is to refine upon the TOE summary specification contained in the ST by identifying and describing the TSF interfaces(TSFI). A TSFI provides means by which external entities to the TSF can invoke services from the TSF and receive the corresponding responses.

The TOE consists of two main components as described in section 3.2.1; the Workflow System Application and the Trusted Client Application. The Workflow System Application provides the main functionality of the TOE and runs on a centrally located server. The Trusted Client Application runs at client machines through which users may request the services of the Workflow System Application.

The external interface groups of the Workflow System Application and Trusted Client Application are shown in figure 4.1 and figure 4.2 respectively. Solid lines indicate requests while punctured lines indicate return values/services from the TSF. Since the TOE components have not been decomposed the TSF is equal to the TOE at this point.

Physical interfaces provided by the hardware and interfaces provided by the operating system(OS) are practically inaccessible because of the security objectives OE.PHYSICAL, OE.OS and OE.TRUST_CLIENT of the ST. These interfaces are therefore not TSFIs.

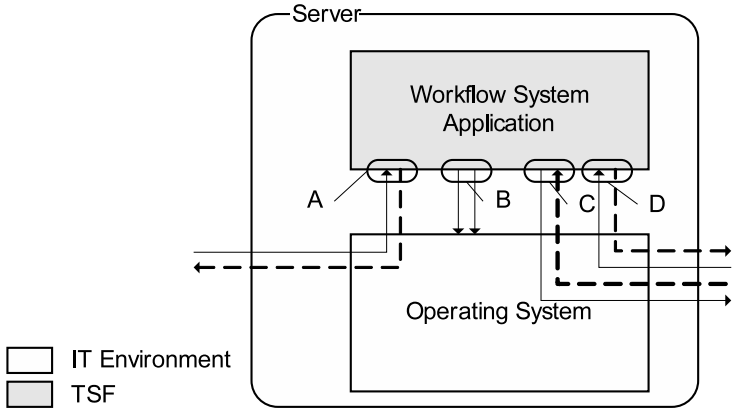

Figure 4.1: Workflow System Application interfaces

A description of each interface group shown in figure 4.1 and figure 4.2 is given below:

Group A represents the interfaces used by user applications to remotely access the Workflow System Application. User applications can be applications which are used for administration, management or participating in workflows. One or more application protocols are used to obtain services. The communication passes through the IT Environment, which provides the supporting protocols (e.g. Ethernet, IP, TCP).

Group B represents the interfaces used by the Workflow System Application

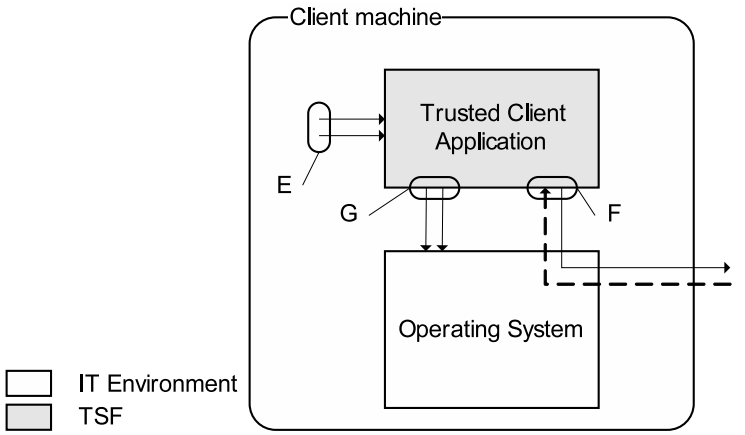

Figure 4.2: Trusted Client Application interfaces

to obtain functionality from the OS, which is part of the IT environment.

Group C represents the interfaces used for invoking applications. For communication with remote applications an application protocol will most likely be used, while local applications could be invoked using e.g. local IPC(Inter-Process Communication).

Group D represents the interfaces used by another workflow engine or another Secure Workflow Systems(SWFS) to obtain services from the Workflow System Application.

Group E represents the most obvious set of interfaces namely the interfaces used directly by users to invoke the services of the Trusted Client Application.

Group F represents the interfaces through which requests to the Workflow System Application are sent using an application protocol.

Group G represents the interfaces used by the Trusted Client Application to obtain functionality from the OS, which is a part of the IT Environment.

In order to be considered a TSFI an interface must provide means to invoke TSF services or be used to send responses to such requests. This means that both group A and D represents sets of TSFIs, where each application protocol which can be used to obtain TSF services are TSFI. Group E represents a set of TSFIs consisting of the set of commands or user interface controls which the user has access to.

The remaining interfaces represent interfaces to functionality in the IT Environment and are therefore not TSFI. They only need to be discussed and analysed if the TOE is part of a composite evaluation(ACO class in CC Part 3[10]).

In this section we will focus on the group A interfaces. The group D and E interfaces should be analyzed similarly.

The interfaces of group A provide the largest number of interfaces to the Workflow System Application, its security functionality and resources. The ST requires all network communication external to the TOE to be protected by the TLS protocol. While the TOE controls which algorithms to use the actual implementation is provided by the cryptographic service provider provided by the OS. The TLS protocol is therefore not a TSFI. It is rather the protocols which run on top of TLS, which provide TSFIs to the Workflow System Application. This could e.g. be HTTP, RMI, IIOP or SOAP depending on how the Workflow System Application is implemented and the type of client application used.

To abstract from the protocols used, the Workflow System Application uses a set of service wrappers which translate from/to a given application protocol to/from a Common API. Figure 4.3 illustrates this.

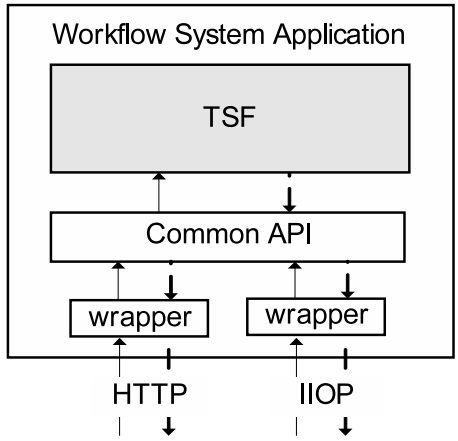

Figure 4.3: Workflow System Application provides access to a common API by use of service wrappers.

The service wrappers merely function as interfaces to the Common API which provides the set of TSFIs. The Common API provides the following 4 interfaces, which are derived from the 'TOE summary specification'(section B.6) of the ST:

Common Interface which provides access to functionality which is applicable to any user. This e.g. includes authentication, re-authentication, locking of session etc.

Administrative Interface which provides access to administration functionality as described in section B.6.5.2 of the ST. This includes e.g. start-up, shutdown, editing of user roles and security functional policies (SFPs) and access to the audit log.

Workflow management Interface which provides access to the workflow management functionality described in section B.6.5.3 of the ST. This includes e.g. management of user to workflow role mappings, creation, modification and deletion of process definitions and workflow instances.

Client Interface which provides access to client functionality. This includes e.g. functionality to execute workitems from the client's worklist, import and export of application data and requests to invoke an application.

For each TSFI a set of commands are identified. This identification of commands is based on information stated in the 'TOE summary specification' and the Workflow Management Application Programming Interface (WAPI)[1] defined by the Workflow Management Coalition(WfMC).

The WAPI defines a standard API for interacting with client applications and invokable applications. The WAPI mainly provides commands which may be used by users associated with the manager or client role and is therefore not sufficient on its own. The WAPI is however useful for obtaining better interoperability with client applications.

An excerpt of the list of identified commands is given in table 4.1. The full list is available in table C.1 in appendix C. Each command is accompanied with a short description of its purpose. All commands prefixed with 'WM' are taken from the WAPI specification.

Common Interface Commands
WMConnect *Purpose: Enables a user to establish a connection to the Workflow System Application.*
Administrative Interface Commands
ChangeUserAttribute *Purpose: Assign an attribute, remove an attribute or change the value of an attribute for a specified user.*
Workflow management Interface Commands
ChangeWFRoleMapping *Purpose: Change the mapping between a workflow role and a client.*
Client Interface Commands
WMGetWorkItem *Purpose: Retrieves a workitem. The workitem is not necessarily locked or retracted from other users worklists, but it might be.* *Note: Any dynamic privileges associated with this workitem will be assigned to the client.*

WMCompleteWorkItem *Purpose: Tell the system that this workitem has been completed.* *Note: Any dynamic privileges associated are revoked and the workitem is retracted from all worklists.*
ImportAppData *Purpose: Imports application data or part of some application data into the TOE.*

Table 4.1: Excerpt of the list of identified commands given in table C.1 in appendix C.

EAL3 requires that the purpose, method of use and all parameters of each interface are described. Two examples of how each command is to be described is given below.

- **WMConnect**
  - Purpose: Enables a user to establish a connection to the Workflow System Application.
  - Method of Use:

```
WMTErrRetType WMConnect (
in WMTPConnectInfo pconnect_info,
out WMTPSessionHandle psession_handle
);
```

  - Parameters: See table 4.2.

pconnect_info	A reference to a connection information object containing the required information to establish a connection with the Workflow System Application. The connection information object contains: **Mechanism** The mechanism to be used for authentication e.g. password or X.509 certificate. **User ID** The user's identification information (e.g. user name). **Authentication data** The user's authentication information such as password, PIN, or long term key.

Table 4.2: Parameters of the WMConnect command (continued on next page).

psession_handle	Reference to an object containing the user's credentials and session information for this session. The information can be passed to the Workflow System Application on all subsequent API calls, if required.
Return parameter	The return parameter specifies the result of the operation. WM_SUCCESS is returned if the user is successfully authenticated and the session handle has been properly initialised.

Table 4.2: Parameters of the WMConnect command.

– Actions: Establishes a connection with the Workflow System Application if the authentication of the user is successful and the session is successfully created.

– Error messages: WM_CONNECT_FAILED is returned if the method fails e.g. if the user could not be identified or authenticated.

- **ChangeWFRoleMapping**

– Purpose - Change the mapping between a workflow role and a client.

– Method of Use:

```
boolean ChangeWFRoleMapping(
in WMTPSessionHandle psession_handle,
in MapID pmap_id,
in UserID pmap_id,
in WFRoleID pwfrole_id,
);
```

– Parameters - See table 4.3.

psession_handle	Reference to an object containing the clients credentials and session information for this session.
pmap_id	A reference to the map id which is associated with a workflow role and a client id.
puser_id	A reference to client's user id.
pwfrole_id	A reference to the workflow role which should be added to or removed from the client's list of workflow roles.

Table 4.3: Parameters of the ChangeWFRoleMapping command (continued on next page).

Return parameter	TRUE if the change is successful.

Table 4.3: Parameters of the ChangeWFRoleMapping command.

- Actions - Changes the mapping between a workflow role and a client.
- Error messages - FALSE is returned if the mapping could not be changed.

4.3 Architectural design

The next step of the design process is to describe the architectural design of the TOE by decomposing the TOE into subsystems. At EAL3 the CC requires that all elements of ADV_TDS.2 of CC Part 3[10] is fulfilled. To keep within the scope of this chapter we will suffice by giving an overview of how the TOE could be designed and summarise the behaviour of each TSF subsystem. The two TOE components are described separately.

4.3.1 Workflow System Application design

In this section the Workflow System Application is decomposed into subsystems and each TSF subsystem is described. An overview of the subsystems is given in figure 4.4. The directed connectors indicate which subsystems request services from each other.

4.3.1.1 Application Subsystem

The Application Subsystem is responsible for handling the invocation of applications. This both includes the handling of invocation requests either received directly through the Common API or from the Engine as well as the handling of responses from the invoked applications. The subsystem handles the mapping of applications to application agents, which like the service wrappers provide connectivity to applications using different mechanisms and protocols.

4.3.1.2 Audit Subsystem

The Audit Subsystem is responsible for providing the TOE's audit functionality, such as audit generation, audit review and audit protection. The subsystem listens on audit events sent by the Security Subsystem and records the security relevant events which according to the audit configuration should be audited.

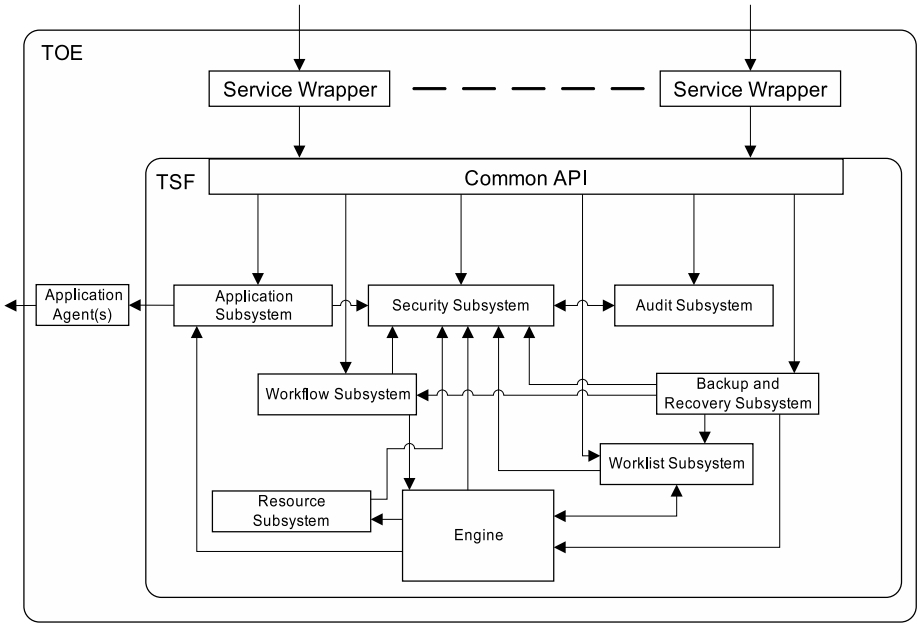

Figure 4.4: Workflow System Application architecture.

Services such as reading the audit log and changing the audit configuration can be done through the Common API.

4.3.1.3 Backup and Recovery Subsystem

The Backup and Recovery Subsystem is responsible for creating backups and recover data using these backups. Workflow related data is retrieved from the Workflow Subsystem, Worklist Subsystem and the Engine. The remaining TSF data is obtained from the Security Subsystem.

4.3.1.4 Engine

The Engine provides the execution environment for the workflow instances. The subsystem maintains the workflow control data and workflow relevant data. It is responsible for assigning tasks to client worklists and invoke applications. Application data is obtained through the Resource Subsystem.

4.3.1.5 Resource Subsystem

The Resource Subsystem is responsible for maintaining the mapping between application data and workflow instances.

4.3.1.6 Security Subsystem

The Security Subsystem is responsible for enforcing the majority of the security functional requirements(SFRs). The subsystem manages the identification data, authentication data and attributes belonging to users and applications. Also the security functional policies(SFPs) are managed through here.

The subsystem enforces the access control and flow SFPs thereby ensuring that the TOE assets are properly protected. All subsystems either directly or indirectly obtains services from the Security Subsystem in order to assert if an operation or set of operations are permitted or not. Services such as changing SFPs or user attributes can be done directly through the use of the Common API.

4.3.1.7 Workflow Subsystem

The Workflow Subsystem is responsible for managing process definitions and deploying workflow instances to the Engine. The subsystem provides services such as import and export of process definitions, editing of process definitions and workflow instances, creation of workflow instances and retrieval of workflow instance status information though the Common API.

4.3.1.8 Worklist Subsystem

The Worklist Subsystem provides clients with access to their worklist through the Common API. The subsystem ensures with help from Security Subsystem that clients can only access and execute workitems on their worklist. The subsystem is also responsible for notifying the Engine when tasks have been completed and remove the corresponding workitems from all worklists.

4.3.2 Trusted Client Application design

The Trusted Client Application shall provide an environment which ensures that the flow SFPs are enforced when a client manages sensitive application data. The Trusted Client Application has been decomposed into the subsystems shown in figure 4.5. The directed connectors shows which subsystems request services from each other.

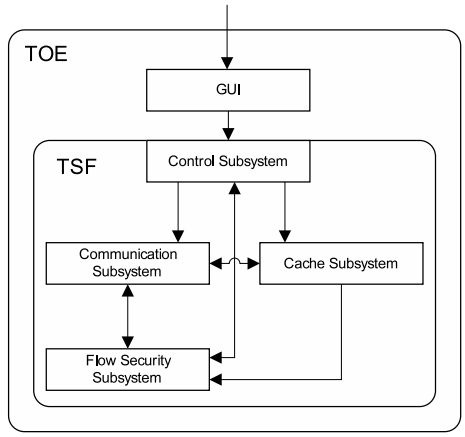

Figure 4.5: Trusted Client Application architecture.

4.3.2.1 GUI

The Graphical User Interface(GUI) is the only subsystem which is outside of the TSF. It provides the client with a simple and intuitive graphical user interface.

4.3.2.2 Control Subsystem

The Control Subsystem provides the set of TSFIs responsible for controlling the behaviour of the Trusted Client Application. The subsystem communicates with the Cache Subsystem and Communication Subsystem in order to retrieve information to be displayed onto the GUI.

4.3.2.3 Communication Subsystem

The Communication Subsystem is responsible for passing data from and to the Workflow System Application. The connection to the Workflow System Application is initially established with the help of the Flow Security Subsystem and the operating system's cryptographic service provider, which ensure that a secure TLS connection is established. When connected the subsystem ensures that the Flow Security Subsystem is provided with the information necessary to enforce the Workflow flow SFP.

4.3.2.4 Cache Subsystem

The Cache Subsystem is responsible for synchronizing data between the Trusted Client Application and the Workflow System Application and protect the integrity and confidentiality of the cached data in co-operation with the OS.

4.3.2.5 Flow Security Subsystem

The Flow Security Subsystem ensures that the client cannot interact with the Trusted Client Application before the necessary information to enforce the Workflow flow SFP has been received from the Communication Subsystem. When the subsystem is ready the Control Subsystem is notified and the client is allowed to interact with the application. In order to enforce the subsystem's main objective of enforcing the Workflow flow SFP the subsystem or part of the subsystem may need to run in kernel mode within the the OS. The subsystem needs to prevent the OS window manager from executing commands such as 'Print Screen' which could compromise the Workflow flow SFP.

4.4 Conclusion

The chapter has given concrete specifications of a TOE which is compliant with the Centralised Secure Workflow System ST. The TSFI groups of both the Workflow System Application and Trusted Client Application has been identified. A partial functional specification of the group of TSFIs(group A) which are used by user applications to interact with the Workflow System Application has been created. This includes the identification of the TSFIs within the group and an example of how commands are to be described in the functional specification.

Finally an example of how the TOE, consisting of the Workflow System Application and the Trusted Client Application, could be designed has been given and the subsystems of the TOE have been summarised.

The design is still in the early stages and can be considered the first steps in creating the necessary documentation for satisfying the assurance requirements ADV_FSP.3 Functional specification with complete summary and ADV_TDS.2 Architectural design, which are required by EAL3.

Chapter 5

CC discussion

The Common Criteria(CC) provides a comprehensive framework for the specification of security requirements of IT products and systems. Due to the extent of the CC it is a time consuming process to get familiarized with its concepts and contents. The Protection Profiles(PPs) and Security Targets(STs) which are available from the official CC website provide a good source for inspiration. Since the newest version of the CC 3.1 was just released to the public in September 2006 no certified PPs or STs are available at this point.

The most significant change from CC 2.x is that the possibility to state security functional requirements(SFRs) to be fulfilled by the IT environment has been removed. This emphasizes that only the Target of Evaluation is subject to evaluation. This subsequently means that the PP and especially the ST author is required to more thoroughly consider where to place the TOE boundary. This is particularly important when it is desired to develop a PP/ST for a software application such as a Secure Workflow System(SWFS). Typically a software application will be run on top of a general purpose operating system(OS) which then again relies on the underlying hardware.

Three approaches may be taken:

- the TOE is defined to be only the software application; or
- the underlying services are included in the TOE; or
- only specific parts which the software application specifically relies upon

are included

In the PP and ST developed in this thesis the first approach was taken. The advantage of this approach is that focus is kept on the functionality of the software application and the specification of its security functional requirements(SFRs). This is particularly desired when, as in this thesis, the CC is used to develop a secure software application. The problem of this approach is that since only the TOE is evaluated no assurance is given on the security of the system as a whole. To fully accomplish this a ST must be developed using the second approach.

The second approach of including the underlying services as a part of TOE requires that all of the functionality of e.g. the general purpose OS also must be taken into account. This includes functionality which is not used by the software application. The complexity of the TOE will be significantly increased and hereby the size of the ST.

The third approach tries to mitigate the problem by only including the specific parts which the software application directly relies upon. E.g. the ST for the Secure Workflow System states that it relies upon the OS to provide a cryptographic service provider(CSP) and a reliable clock for creating time stamps. These components should then be included in the ST. Nevertheless an assumption must be made on that the OS will protect its interfaces to the application.

As it is realized no easy solution exists. Basically it adds up to what one wishes to obtain assurance of and how much trust one has on that the environment fulfills the assumptions of the TOE. In the context of this thesis' goals the first approach provided a sufficient level of assurance.

Chapter 6

Future work

With the PP, ST and partial design specification provided in this thesis, the basis for the implementation of a concrete Secure Workflow System has been established.

The next step in the development process of a Secure Workflow System would be to complete the design specification such that the ADV: Development assurance requirements for EAL3 of CC Part 3 are fulfilled. In addition the remaining security assurance requirements must be fulfilled and a concrete implementation of the specified Secure Workflow System must be developed. When the Secure Workflow System has been developed it can be evaluated against the ST.

In the context of the Common Criteria the next step in the process is to have the PP and ST evaluated by one of the official CC evaluation labs. When the developed Secure Workflow System has been evaluated one might consider to prepare for a composite evaluation e.g. consisting of the developed Secure Workflow System and an evaluated operating system(OS). A composite evaluation will provide additional assurance that the Secure Workflow System in co-operation with the OS fulfills the stated security requirements.

Chapter 7

Conclusion

The aim of this project has been to design a Secure Workflow System using an approach based on the Common Criteria for Information Technology Security Evaluation (CC). The CC provides a comprehensive framework for the specification of security requirements for IT products and systems. Due to the extent of the CC it is however a time consuming process to get familiarized with its concepts and contents.

Given the limited timeframe for the project it has been important to scope the work in a way which does not create a full solution to the problem but at the other hand clearly illustrates how CC can be used for designing a Secure Workflow System. This has been done using the following steps:

A Protection Profile(PP) for Secure Workflow Systems has been developed on the basis of an analysis of the security requirements of secure workflow systems. The PP defines a high level model of a Secure Workflow System(SWFS), which addresses almost any type of workflow system where data protection and user accountability are priorities.

Based on the PP a conforming Security Target(ST) for a Secure Workflow System employing a centralised architecture has been developed. The ST refines upon the model of the PP to fit into a centralised architecture. To fulfill the information flow control requirements of the PP the Trusted Client Application has been added to the model. The ST TOE hereby consists of a Workflow System Application, which provides the functionality of the SWFS, and a Trusted Client Application which ensures that the ST information flow control require-

ments are enforced.

The ST has been used as a basis for deriving concrete specifications of how the centralised Secure Workflow System could be designed. The design specifies the external interfaces to the TOE security functionality and gives an concrete example of the ST TOE design by decomposing the TOE into subsystems. The design is still in the early stages and can be considered the first steps in creating the necessary documentation for satisfying the development assurance requirements required by EAL3.

The objectives of the project are hereby all accomplished with satisfactory results and the aim of the project is fulfilled.

Appendix A

Secure Workflow Systems Protection Profile

Version 1.0

February 2007

A.1 PP introduction

A.1.1 PP reference

Title:	Secure Workflow Systems Protection Profile
Version:	1.0
Author:	Rune Friis-Jensen, s011375, IMM, The Technical University of Denmark (DTU)
Publication date:	2007-02/05
CC Version:	3.1 Revision 1
Assurance Level:	EAL3+

A.1.2 TOE Overview

A.1.2.1 TOE type

This Protection Profile (PP) specifies the security requirements for Secure Workflow Systems (SWFS). A SWFS provides consumers with a system which is able to control the execution of business processes, workflows. Workflows consists of a combination of manual and automated activities. It is the objective of the SWFS to ensure that this is done in a secure manner

The SWFS interprets process definitions, which are computer processable definitions of business processes and creates instances of these, workflow instances. When a workflow instance has been created the SWFS will in accordance with the workflow instance's process definition automatically execute the defined business process by assigning tasks to worklists. These worklists can be accessed by authorised workflow clients which can then process the workitem of the task. At all times the SFWS ensures that the required information to support each step of the workflow is available.

A SWFS will have the capability to limit access to authorised users, enforce protection of assets both physically and logically and ensure that individual users are held accountable for their actions through the use of auditing.

The Secure Workflow Systems Protection Profile (SWFSPP) uses some of the standard workflow terms defined by the Workflow Management Coalition(WfMC), but does not have any requirements on WfMC conformance. The term workflow system and task are equivalent to the WfMC terms workflow enactment service and activity respectively.[20]

A.1.2.2 General TOE features

The TOE consists of one or more workflow engines which are software applications layered on an underlying system, e.g. a host OS. The TOE provides functionality to:

- control user access to the TOE, the assets and the TOE Security Functions (TSF)
- instantiate process definitions
- control workflow instances
- invoke trusted applications
- perform utility tasks like backup and recovery of assets
- generate audit data

The SWFSPP does not make any requirements on the amount of workflow engine(s) the TOE should consist of or whether a centralized or distributed architecture is used.

A.1.2.3 TOE assets

In order for something to be considered a TOE asset, its confidentiality, integrity and/or availability must be considered vital to the sound operation of the TOE. The primary TOE assets are:

Process definitions A process definition is a computer processable definition of business process. A process definition defines how information within a workflow is to be handled such as:

- starting and completion conditions
- which tasks the workflow consists of
- the rules for navigating between tasks
- references to applications, which may be invoked
- definitions of workflow relevant data which may need to be referenced

Control data Control data consists of data internally managed and maintained by the TOE such as:

- state information of workflow instances
- other internal status information
- checkpointing and recovery/restart information used by TOE to coordinate and recover from failure

Workflow relevant data Workflow relevant data, is used to determine transition conditions which influences the state transitions within the workflow instances. Workflow relevant data may be accessible to invoked applications, clients or other SWFSs, but only in a very limited way and highly constrained by the TOE.[20]

Application data Application data is application specific data and only relevant to the application and client tasks during the execution of a workflow instance.[20]

Worklists Worklists consists of workitems which each are associated with a task. workitems are assigned by the TOE and should be processed by clients during the execution of workflow instances.[20]

Audit data Audit data is generated by the TOE during operation. The purpose of the audit data is to provide a non-repudiable trace of the history of the workflow instantiations as well as being able to gather statistics.

A.1.2.4 TOE roles

In order for the TOE to operate in a secure manner at least 3 types of authorised user roles are to be supported:

Administrator A person who has privileges to install, configure and maintain the TOE and its security functions. This includes e.g. the ability to:

- manage the group of authorised users and the associated authentication data
- maintain and review the generated audit data
- manage the various Security Function Policies (SFP)

Manager A person who has privileges to create, modify and delete process definitions and manage workflow instances within the TOE. This includes e.g. the ability to:

- associate clients with workflow roles
- assignment and re-assignment of workitems
- monitoring the progress of task instances and workflow instances

Client A person or application which can participate in one or more workflows through the processing of tasks.

A.1.2.5 TOE communication

The TOE may interact with the following IT entities outside of the TOE:

- Client applications that allows clients to interface with the TOE in order to access worklists, workflow relevant data and application data which they are authorised for.
- Manager applications and tools that allow managers to interface with the TOE in order to manage process definitions and workflow instances.
- Administrator applications and tools that allow administrators to interface with the TOE in order to install, configure and manage the TOE and the TSF.
- Trusted applications which can be invoked by the TOE.
- Trusted SWFSs which the TOE exchanges information with.

The generic term user application is used for referring to any client, manager and administrator application.

Figure A.1 gives an overview of how the TOE is structured.

A.1.2.6 TOE security features

The TOE will provide the following security services completely or in co-operation with the IT environment:

Identification and authentication of all TOE roles, invoked applications and SWFSs.

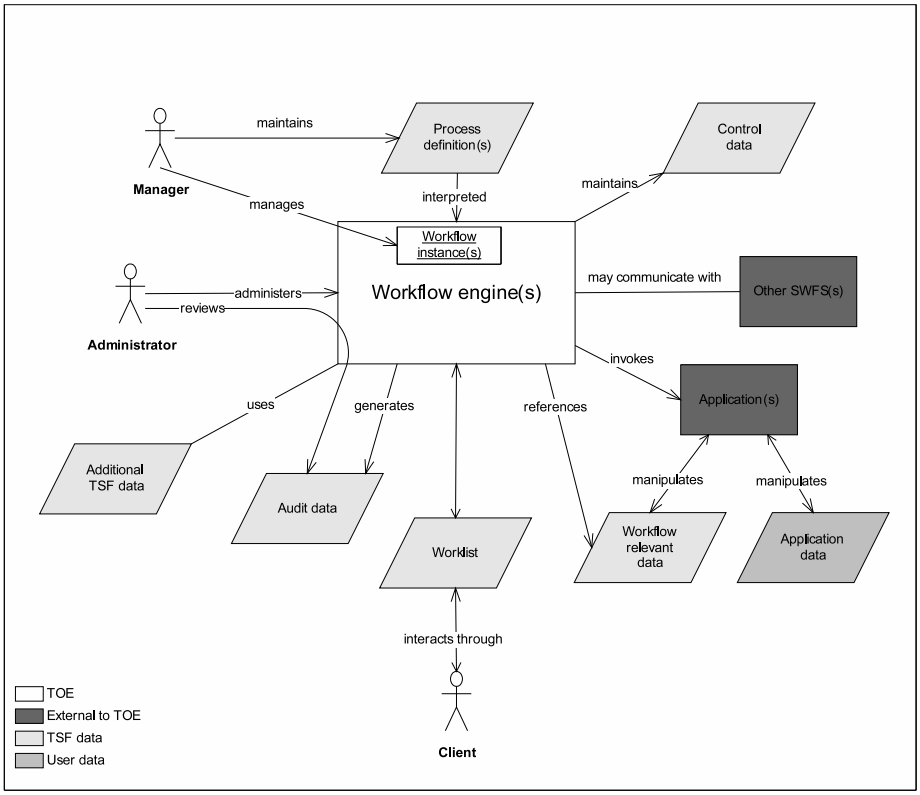

Figure A.1: Overview of the TOE structure

Access control to the TOE application data through the specification of access control SFPs.

Information flow control of TOE application data through the specification of information flow control SFPs.

Audit generation to capture all auditable events, thereby providing capability to hold users accountable for their actions and detect malicious behaviour.

Secure audit storage which stores all records for all security relevant operations performed on the TOE.

Secure audit review which allows administrators to review stored audit records and detect potential and actual security violations.

Authorised administration through the administrator role, which allows administrators to configure and manage the access control SFPs, information flow control SFPs, the identification and authentication of users and the auditing functions.

Backup of data such that corrupted or deleted data may be recovered.

A.1.2.7 User data protection

Application data is the only TOE user data. Due to the dynamic nature of workflows the security requirements for application data can become very complicated. Client privileges may depend on the state of the workflow, whether the client is assigned to a specific workflow role or whether the client has processed a specific task etc. To support these requirements the SFWSPP defines two types of access control SFPs which have to be implemented by the TSF; a SWFS access SFP and Workflow access SFP.

To enforce the two types of policies the SWFSPP uses the conventions shown in figure A.2. Each client is associated with one or more workflow groups, in each of which the client has zero or more workflow roles. Furthermore a client has a set of static privileges and a set of dynamic privileges. The static privileges are privileges which have been assigned to the client permanently or at least until they are revoked. Dynamic privileges are privileges which are assigned to the client as a result of the active binding of the client. I.e. privileges can be granted dynamically to a client when he activates a specific workflow role or specific task. The dynamic privileges are revoked when the binding is terminated. Finally each client is associated with a client history, which contains the relevant history of the client's interactions within the workflow instances. This could be consumed workflow groups, workflow roles, privileges etc.

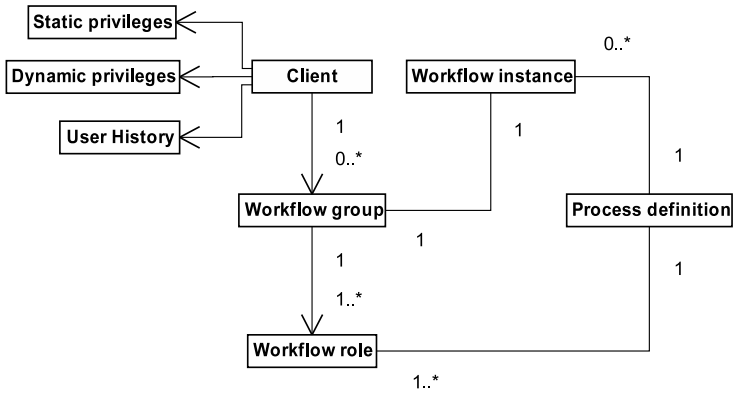

Figure A.2: Relations between SWFSPP conventions.

Since there may be constraints on what a client can do simultaneously a client is associated with a set of active privileges when a session is established. The set of active privileges is the subset of the client's static privileges and dynamic privileges which the client currently has activated.

The SWFS access SFP enforces the access control requirements, which is applicable to all workflow instances executed within the TOE. This could be requirements such as specific clients may not be members of the same workflow group or certain privileges may not be possessed by the same client.

The Workflow access SFP enforces the access control requirements of the workflow instance's access SFP. This SFP is an instantiation of the process access SFP defined at the process definition level. Figure A.3 shows the relation between the policies.

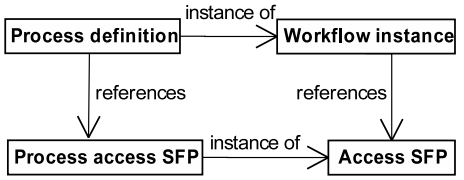

Figure A.3: Relation between process access SFP and the workflow instance's access SFP.

The process access SFP should specify the access control requirements within the process definition. This could e.g. be which workflow roles have access to a specific object or task and separation of duty constraints such as if client A has processed task 1 then he must not process task 5.

The specification of access control SFPs within a SWFS does however usually not provide sufficient protection of the application data. A SWFS will typically control multiple shared resources containing application data which often will have requirements upon how application data may flow from one resource to another. This may be between the applications which the SWFS interacts with, specific application data objects etc.

To control the flow of information the SWFSPP requires the TSF to implement two types of flow SFPs. Firstly an application flow SFP should be specified for each user application, invokable application and SWFS which the TOE interacts with. These policies should be used to enforce requirements such as certain types of information should only be handled by specific applications. Secondly a Workflow flow SFP shall be implemented which analogous to the Workflow access SFP shall enforce the information flow requirements of the workflow instance's flow SFP.

Figure A.4 shows the SWFSPP SFP framework. The assembly of the SWFS access SFP, the Workflow access SFP, the application flow SFP and the Workflow flow SFP are referred to as the TOE Security Policy (TSP).

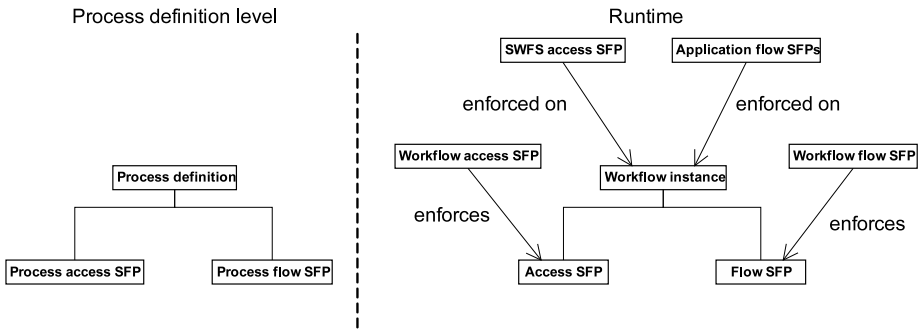

Figure A.4: SWFSPP policy framework

Since the policies very much the depend on the TOE, the PP only provides the basic policy requirements. It is the task of the ST author to decide on how fine grained the four types of policies are required to be in order to achieve a sufficient level of security.

A.1.2.8 Available non-TOE hardware/software/firmware

This section includes a list of non-TOE hardware/software which has to be available. The list should not be thought of as complete, but rather give the consumer a indication of what non-TOE hardware/software is required as a minimum by the TOE.

- Server(s)
- Operating system(s)
- Data storage i.e database(s) and/or file system(s)

A.2 Conformance claims

This PP conforms to the Common Criteria for Information Technology Security Evaluation(CC) version 3.1, revision 1. The PP is CC Part 2 conformant, CC Part 3 conformant and EAL3 Augmented.

PPs and STs wishing to claim conformance to this PP must claim strict conformance. [8]

A.3 Security problem definition

This section defines the security problem to be addressed. This is done in 4 steps.

- The threat agents are identified.
- The assumptions that are made on the operational environment, in order to provide security functionality are given.
- The threats to be countered by the TOE, its operational environment or a combination of these are identified.
- The organisational security policies(OSPs) to be enforced by the TOE are shown.

A.3.1 Threat agents

The threat agents can be categorized as shown below.

Authorized user	An authorized manager or client.
Unauthorized user	An entity which is **not** authorized to access the TOE.
External events	Interruption of TOE operation due to failure of hardware, storage, power supply, fire, water damage etc.

Note that administrators are not considered a threat agent which is due to the assumption AP.ADMIN. In the following the term attacker will be used to denote any of the threat agents.

A.3.2 Assumptions

In order for the TOE to be considered secure the operational environment has to meet the following assumptions on personnel and connectivity.

A.3.2.1 Personnel

AP.ADMIN *The administrators of the TOE are qualified in managing and maintaining the TOE and can be trusted not to abuse their privileges.*

This assumption is made to ensure that at least one user of the TOE can be trusted to be able to manage and maintain the TOE and the security functions and data it contains.

A.3.2.2 Connectivity

AC.RESOURCE *The TOE has sufficient resources available to function properly and securely.*

This assumption is made to ensure that the TOE and its security functions are able to operate reliably.

AC.OS *The underlying operating system and network services which the TOE relies upon are installed, configured and managed in a secure manner.*

Since the TOE is implemented in software it relies upon the underlying OS and hardware. This assumption therefore has to be made to guarantee that the TOE will operate in a secure manner.

AC.TIME *The underlying operating system shall provide the TOE with a clock which is synchronized with a reliable hardware clock.*

A.3.3 Threats

This section describes the threats that are to be countered by the TOE and its operational environment or a combination of these. All threats pose a threat to either primary assets as listed in section A.1.2 or secondary assets such as TSF security attributes. All the listed threats have been derived with the earlier described assumptions in mind.

T.ACCESS *Unauthorized access to the TOE.*

Besides the case where an attacker is able to bypass the access mechanisms of the TOE completely, the threat also includes the case where an attacker is able to access the TOE by impersonating an authorised user or an administrator.

T.DATA *Unauthorized access to application data.*

An attacker accesses data which it does not have permission to access.

T.DATAFLOW *The integrity of the information flowing from or to the TOE is compromised.*

An attacker may compromise the integrity of the data transmitted from and to the TOE deliberately or accidentally by changing its content.

T.MODIFY *Information protected by the TOE is modified maliciously by an attacker.*

As opposed to T.ACCESS this threat deals with the case where the attacker actually tries to make malicious changes to the data protected by the TOE.

T.UNATTENDED *An attacker gains access to the TOE by the use of an unattended session.*

If an authorised user leaves a session open without shutting it down an attacker could takeover the session and gain unauthorized access to the TOE and its assets.

T.PHYSICAL *The underlying OS/network services are physically damaged in a way that prevents the TOE from functioning properly or results in loss of data.*

T.MALFUNCTION *Malfunction in the TOE or underlying OS/network services prevents the TOE from functioning properly or results in loss of data.*

Malfunction comprises all software and hardware errors which are the cause of interruption of the operation of the TOE and may cause TOE assets to be lost or corrupted.

T.TRUSTED *The TOE invokes a trusted application or exchanges information with a SWFS which has been compromised or is being impersonated by an attacker.*

This threat deals with that an invokable application or SWFS may be compromised without detection by the TOE.

A.3.4 Organization security policies

This section lists the organizational security policies (OSPs) to be enforced by the TOE and its operational environment, or a combination of these.

P.ACCESS *Only authorized users and administrators may access the TOE.*

This policy exists to ensure that only administrators and authorised users may access or interact with the TOE. The policy hereby prevents anonymous access to and unauthenticated communication with the TOE.

P.TRAINING *Authorized users and administrators shall be continuously trained in using the TOE properly and securely.*

The purpose of this policy is to ensure that the authorised users and administrators of the TOE are capable of operating the TOE in a secure manner.

P.ACCOUNT *Authorized users shall be held accountable for their interactions with the TOE.*

The policy is to ensure that all authorized users can be held accountable for their actions and that fraud

and malicious intents can be acted upon by the administrators of the TOE.

P.APPLICATION *All applications which the TOE can invoke shall be run on trusted machines which configuration can only be changed by highly trusted persons who are authorised to do so and can be held accountable.*

P.WORKFLOW *Managers shall be able to manage the security mechanisms of the workflows which they are responsible for.*

A.4 Security objectives

A.4.1 Security objectives of the TOE

This section lists the security objectives of the TOE.

O.AUTH *The TOE shall provide means for identifying and authenticating users before allowing access to the TOE and its resources.*

O.ACCESS *A SWFS access SFP shall be specified which enforces the TOE access control requirements. Furthermore a Workflow access SFP shall be specified which shall enforce the access SFP of workflow instances.*

O.FLOW *Each user application, invokable application and SWFS the TOE interacts with must be covered by an application flow SFP. Furthermore a Workflow flow SFP shall be specified which shall enforce the flow SFP of a workflow instance.*

O.MANAGE *The TOE shall provide means of enabling administrators to manage the security mechanisms of the TOE and restrict these mechanisms from unauthorized use.*

O.WORKFLOW *The TOE shall provide means of enabling managers to manage the security mechanisms of the workflows which they are are responsible for.*

O.AUDIT *The TOE shall provide means of recording security relevant events in sufficient detail to help an administrator to detect attempted security violations and hold*

users accountable for any actions that are relevant to the security of the TOE.

O.DATAFLOW *The integrity of all data which is received and sent through the TOE interfaces must be protected.*

O.RECOVER *The TOE shall provide administrators with functionality which ensures the that the TOE can recover effectively after a system failure without compromising the security of the TOE. This includes providing functionality which ensures that backups of the TOE assets and TOE security functional data are made regularly and that the confidentiality, integrity and availability of these backups are adequately protected.*

O.SESSION *The TOE shall provide functionality that allows an authorised user or the TSF to invalidate or lock the user's current session after some reasonable period of inactivity. To unlock the session the user must re-authenticate.*

O.TRUSTED *The TOE shall provide means for additional assurance of the authenticity of trusted applications which are invoked and trusted SWFSs which the TOE exchanges information with.* Whether the session is invalidated or locked after a given time interval of inactivity or by the use of some kind of physical token the strategy and mechanisms to ensure this should be chosen based upon a threat analysis.

A.4.2 Security objectives of the operational environment

This section lists the security objectives of the operational environment.

OE.PHYSICAL *The operational environment shall ensure that the TOE and its underlying services are sufficiently protected from physical damage by an attacker.*

OE.ADMIN *The operational environment shall ensure that only highly qualified and trusted users are given administrative privileges.*

	The personnel with administrative privileges must be throughly vetted to ensure that they are competent and can be trusted not to abuse their privileges.
OE.BACKUP	*The operational environment shall ensure that backups of the TOE assets and TSF data are stored physically separate from TOE and are protected from physical damage.*
OE.TRAINING	*The operational environment shall ensure that all authorised users of the TOE and the administrators are continuously trained in the proper and secure use of the TOE.*
OE.RESOURCE	*The operational environment shall ensure that the TOE always has sufficient resources to operate properly and securely.*
OE.APPLICATION	*The operational environment shall ensure that all invokable applications and SWFSs which the TOE communicates with run on trusted machines whose configuration can only be changed by authorised personnel and who can be held accountable.*
OE.OS	*The operational environment shall ensure that the TOE, the underlying OS and hardware are installed, configured and operated in a way that maintains the security of the TOE. This includes that a security domain is provided which ensures that the TOE cannot be tampered with by other applications since the OS/hardware makes the interfaces through which the TOE can be accessed inaccessible to other applications. Furthermore it must be ensured that the OS and hardware will faithfully execute the commands of the TOE and will not tamper with the TOE in any manner.*
OE.TIME	*The operational environment shall ensure that the underlying OS provides the TOE with a reliable clock which is synchronized with a reliable hardware clock.*

A.4.3 Security objectives rationale

This sections provides the security objectives rationale which gives justifications which show that all assumptions, threats and OSPs are effectively addressed.

Furthermore a tracing which shows which threats, OSPs and assumptions are addressed by which security objectives. The tracing is shown in table A.1.

All argumentation based on the audit data assumes that it has not been compromised.

	AP.ADMIN	AC.RESOURCE	AC.OS	AC.TIME	T.ACCESS	T.DATA	T.DATAFLOW	T.MODIFY	T.UNATTENDED	T.PHYSICAL	T.MALFUNCTION	T.TRUSTED	P.ACCESS	P.TRAINING	P.ACCOUNT	P.APPLICATION	P.WORKFLOW
O.AUTH					x	x		x					x		x		
O.ACCESS						x		x									
O.FLOW						x											
O.MANAGE					x	x	x	x					x		x	x	
O.WORKFLOW																	x
O.AUDIT					x	x		x							x		
O.DATAFLOW							x										
O.RECOVER								x		x	x						
O.SESSION									x						x		
O.TRUSTED												x					
OE.PHYSICAL										x							
OE.ADMIN	x																
OE.BACKUP								x		x	x						
OE.TRAINING	x								x					x			
OE.RESOURCE		x															
OE.APPLICATION												x				x	
OE.OS			x														
OE.TIME				x													

Table A.1: Tracing of security objectives to assumptions, threats and OSPs.

AP.ADMIN The assumption is upheld by *OE.ADMIN and OE.TRAINING. OE.ADMIN directly upholds AP.ADMIN by requiring the operational environment to throughly vet the personnel, which are to be given administrative privileges, are qualified, competent and can be trusted not to abuse their privileges. OE.TRANING supports this by assuring that the administrators are continuously trained and thereby remain qualified.*

AC.RESOURCE *This assumption is upheld entirely by OE.RESOURCE by requiring the operational environment to ensure that the TOE has sufficient resources to operate securely and reliably.*

AC.OS *OE.OS solely upholds this assumption by requiring the operational environment to assure that the OS and underlying services are installed, configured and managed in a secure manner such that the security of the TOE is not compromised.*

AC.TIME *OE.TIME entirely upholds this assumption by requiring the operation environment to ensure that the underlying OS provides a reliable clock which is synchronized with a reliable hardware clock e.g. synchronized via GPS.*

T.ACCESS *This threat is primarily countered by O.AUTH which assures that the TOE provides means for authenticating users before allowing them access to the TOE. O.MANAGE and O.AUDIT both counter the threat indirectly. O.MANAGE assures that security mechanisms are provided for managing who has access to the TOE. O.AUDIT mitigates the situation where an attacker is able to compromise the authentication mechanism. It provides administrators with the means to react upon a security violation and track what the attacker has been doing. An administrator may hereby be able to reduce the damages.*

T.DATA *The treat is countered by O.AUTH, O.ACCESS, O.FLOW, O.MANAGE and O.AUDIT. The first four objectives counters the threat directly by providing authentication of users and mechanisms for protection of application data through the use of access control and information flow control. O.ACCESS ensures that an attacker cannot access application data, while O.FLOW ensures that an authorised user cannot make application data available to an attacker. O.AUDIT enables administrators to detect attempted violation of access rights. They can hereby prevent that a violation actually occurs and mitigate the situation where data has been maliciously modified by being able to track what the attacker has been doing.*

T.DATAFLOW *O.DATAFLOW and O.MANAGE counters the threat. O.DATAFLOW by requiring the TOE to protect the integrity of all data sent and verify the integrity of all data received. O.MANAGE assures that administrators have access to functionality to manage the secu-*

rity mechanisms of the TOE which are used to provide the integrity protection of the transmitted data.

T.MODIFY *This threat is mainly countered by O.AUTH, O.ACCESS and O.MANAGE by diminishing the likelihood of an attacker being able to access the TOE and access data. If an attacker is able to compromise the security of these objectives the treat is mitigated by O.AUDIT, O.RECOVER and OE.BACKUP.*

O.AUDIT makes it possible track an attackers malicious changes thereby improving the administrators chances of reducing the damage to the TOE data. O.RECOVER ensures that the TOE supports a backup mechanism such that malicious modified or deleted data may be possible to restore.

OE.BACKUP ensures that backups are kept physically separate from the TOE and that they are physically protected such that they are available.

T.UNATTENDED *The threat is directly countered by O.SESSION, which requires the TOE to provide functionality for automatic invalidation or locking of a inactive user session. The possibility of an attacker taking advantage of the unattended session is thereby decreased. OE.TRAINING assures that the authorized users are trained in the secure use of the TOE, which in relation to the threat could be learning users to log off or lock their session when they do not use it or leave it physically.*

T.PHYSICAL *The threat is countered by OE.PHYSICAL, O.RECOVER and OE.BACKUP. OE.PHYSICAL helps diminishing the threat by requiring that the operational environment makes sufficient precautions to prevent an attacker from physically damaging the TOE or any of its underlying services. If the TOE is physical damaged O.RECOVER may assist in restoring lost data and the effective recovery of the TOE. The loss of availability is hereby kept to a minimum without compromising the security of the TOE. OE.BACKUP ensures that backups are kept physically separate from the TOE such that they are available even when the TOE is physically damaged.*

T.MALFUNCTION *The threat is mitigated by O.RECOVER and OE.BACKUP for the same reasons as described for T.PHYSICAL.*

T.TRUSTED *The threat is mitigated by O.TRUSTED together with OE.APPLICATION. It is ensured that the TOE provides additional assurance of an invoked application's or a SWFS's authenticity. Additionally the operational environment is required to ensure that these are sufficiently protected against compromise.*

P.ACCESS *The OSP is enforced by O.AUTH and O.MANAGE, which ensures that only authorized users can access the TOE. Additionally administrators are able to control the security functions of the TOE, e.g. defining who has access and who does not.*

P.TRAINING *OE.TRAINING directly enforces this OSP by requiring the operational environment to arrange for training of all authorized users and administrators.*

P.ACCOUNT *O.AUDIT directly supports this OSP since it assures that the TOE provides functionality to log security relevant events. Administrators are hereby able to hold users responsible for their interactions with the TOE. How much is to be logged is entirely up to administrator and operational environment, but it should be sufficiently fine grained such that users can be held accountable, i.e. uniquely identified. O.AUTH, O.MANAGE, O.SESSION all support the OSP by providing functionality that makes it possible to identify a specific user. If any of these objectives are compromised it may not be possible to hold a user accountable because it would effect the contents of the audit log, which it may not be possible to rely upon in such an event.*

P.APPLICATION *The OSP is enforced by OE.APPLICATION which requires that the operational environment ensures that all the applications which the TOE communicates with runs on trusted machines with a trusted configuration. O.MANAGE provides the administrators with the ability to configure and manage the TOE such that this is fulfilled.*

P.WORKFLOW *The OSP is directly enforced by O.WORKFLOW which ensures that managers are able to manage the workflows executed within the TOE.*

A.5 Security requirements

A.5.1 Security functional requirements

This section describes the security functional requirements(SFRs) chosen from CC part 2 [9] which addresses the security objectives to be met by the TOE. An overview of the SFRs required by the TOE are shown in Table A.2. Assignments and selections performed have been marked in bold. For refinements, italics is used for additions and strikeout for deletions.

Class	SFR	Description
FAU	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
FDP	FDP_ACC.1(1)	Subset access control (SWFS access SFP)
	FDP_ACC.1(2)	Subset access control (Workflow access SFP)
	FDP_ACF.1(1)	Security attribute based access control (SWFS access SFP)
	FDP_ACF.1(2)	Security attribute based access control (Workflow access SFP)
	FDP_IFC.1(1)	Subset information flow control (Application flow SFP)
	FDP_IFC.1(2)	Subset information flow control (Workflow flow SFP)
	FDP_IFF.1(1)	Simple security attributes (Application flow SFP)
	FDP_IFF.1(2)	Simple security attributes (Workflow flow SFP)
	FDP_ETC.2	Export of user data with security attributes
	FDP_ITC.2	Import of user data with security attributes
	FDP_UIT.1	Data exchange integrity
FIA	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.6	Re-authenticating
	FIA_UAU.7	Protected authentication feedback

Table A.2: SFRs required by the TOE (continued on next page).

Class	SFR	Description
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Administrator attributes)
	FMT_MSA.1(2)	Management of security attributes (Workflow attributes)
	FMT_MSA.1(3)	Management of security attributes (Active privileges)
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (Audit logs)
	FMT_MTD.1(2)	Management of TSF data (Audited events)
	FMT_MTD.1(3)	Management of TSF data (System)
	FMT_MTD.1(4)	Management of TSF data (Workflow Management)
	FMT_MTD.1(5)	Management of TSF data (Workflow instances)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_RCV.1	Manual recovery
	FPT_RCV.4	Function recovery
	FPT_TDC.1	Inter-TSF basic TSF data consistency
FTA	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.2	User-initiated locking
FTP	FTP_ITC.1	Inter TSF trusted channel

Table A.2: SFRs required by the TOE.

A.5.1.1 FAU Security audit

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 [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and

- [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, 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].

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **administrators** with the capability to read **any** audit information from the audit records.

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

Application note: Information from the audit log which is relevant to managers or clients can be displayed to them by the use of a intermediary process, setup and controlled by an administrator. The process is to filter and process the audit log information in a secure manner such that only relevant information is displayed.

FAU_SAR.2 Restricted audit review

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

FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

A.5.1.2 FDP User data protection

FDP_ACC.1(1) Subset access control (SWFS access SFP)

FDP_ACC.1.1 The TSF shall enforce the **SWFS access SFP** on **all subjects, all SWFS controlled objects and all operations among them**.

FDP_ACC.1(2) Subset access control (Workflow access SFP)

FDP_ACC.1.1 The TSF shall enforce the **Workflow access SFP** on: **all subjects and objects referenced in a workflow instance's access SFP and all operations between these subjects and objects**

FDP_ACF.1(1) Security attribute based access control (SWFS access SFP)

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

- **user identity, user role, workflow groups, user history and [assignment: list of additional security attributes] associated with the subject**
- **the static privileges held by the subject to the object**
- **the dynamic privileges held by the subject to the object**
- **the set of active privileges held by the subject to the object**

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

- **the subject has the required privilege for the requested operation on the object in its set of static or dynamic privileges and the privilege can be added to the set of active privileges**
- **[assignment: additional 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:

- **the subject has the required privilege on the object in its set of active privileges**

- **[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].

FDP_ACF.1(2) Security attribute based access control (Workflow access SFP)

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

- **workflow groups, workflow roles, user history and [assignment: list of additional security attributes] associated with the subject**
- **the static privileges held by the subject to the object**
- **the dynamic privileges held by the subject to the object**
- **the set of active privileges held by the subject to the object**

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

- **the subject has the required privilege for the requested operation on the object in its set of static or dynamic privileges and the privilege can be added to the set of active privileges**
- **[assignment: additional 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:

- **the subject has the required privilege on the object in its set of active privileges**
- **[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].

FDP_IFC.1(1) Subset information flow control (Application flow SFP)

FDP_IFC.1.1 The TSF shall enforce the [assignment: application flow SFP] on [**assignment: list of subjects which cause information to flow to and from user application(s), invokable application(s) and/or SFWS(s)**].

***A*pplication note:** Any client application, invokable application or SWFS that the TOE communicates with must be covered by a application flow SFP. It may be necessary to iterate *FDP_IFC.1(1) in order to achieve this. For each iteration of FDP_IFC.1(1) a corresponding iteration of FDP_IFF.1(1) must be made.*

FDP_IFC.1(2) Subset information flow control (Workflow flow SFP)

FDP_IFC.1.1 The TSF shall enforce the **Workflow flow SFP** on **all subjects and objects referenced in a workflow instance's information flow control SFP and all operations among subjects and objects covered by the SFP.**

FDP_IFF.1(1) Simple security attributes (Application flow SFP)

FDP_IFF.1.1 The TSF shall enforce the [**assignment: application flow SFP**] based on the following types of subject and information security attributes: [assignment: list of 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]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities].

FDP_IFF.1.5 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.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

Application note: In environments with high security requirements the PP/ST author should also take *FDP_IFF.3 to FDP_IFF.6 which makes requirements on prevention of illicit information flows through covert channels into consideration.*

FDP_IFF.1(2) Simple security attributes (Workflow flow SFP)

FDP_IFF.1.1 The TSF shall enforce the **Workflow flow SFP** based on the following types of subject and information security attributes:

- **the workflow groups and the workflow roles associated with the subject**
- [**assignment: list of additional 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]

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities].

FDP_IFF.1.5 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.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

Application note: In environments with high security requirements the PP/ST author should also take *FDP_IFF.3 to FDP_IFF.6 which makes requirements on prevention of illicit information flows through covert channels into consideration.*

FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the **Workflow flow SFP and [assignment: application flow SFP(s)]** 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].

FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the **Workflow flow SFP and [assignment: application flow SFP(s)]** 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].

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **application flow SFP(s)** to be able to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: modification, deletion, insertion, replay] has occurred.

A.5.1.3 FIA Identification and authentication

FIA_ATD.1 User attribute definition

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

- **user authentication credentials**
- **user role**
- **user history**
- **workflow groups**
- **workflow roles**
- **static privileges**
- **dynamic privileges**
- [**assignment: list of additional security attributes**]

***A*pplication note:** Each workflow role which belongs to the user must be associated with a workflow group which the user belongs to.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions:

- **The session has been locked or terminated.**
- [**assignment: list of additional conditions under which re-authentication is required**]

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

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

FIA_USB.1 User-subject binding

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

- **user authentication credentials**
- **user role**
- **user history**
- **workflow groups**
- **workflow roles**
- **static privileges**
- **dynamic privileges**
- [**assignment: list of additional user security attributes**]

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

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

A.5.1.4 FMT Security Management

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

- **implementing the user identification and authentication mechanisms**
- **implementing the association between TOE roles and individual users**
- **controlling the behaviour of the audit generation**
- **implementing the SWFS access SFP**

- **implementing the Workflow access SFP**
- **implementing the application flow SFPs**
- **implementing the Workflow flow SFP**
- **implementing the TOE backup and recovery routines**
- **implementing the session locking methods**
- **[assignment: list of additional functions]**

to **administrators**.

FMT_MSA.1(1) Management of security attributes (Administrator attributes)

FMT_MSA.1.1 The TSF shall enforce the **SWFS access SFP** to restrict the ability to **modify** the security attributes **user identity, user role, user history, static privileges, [assignment: list of additional security attributes]** to **administrators**.

FMT_MSA.1(2) Management of security attributes (Workflow attributes)

FMT_MSA.1.1 The TSF shall enforce the **Workflow access SFP** to restrict the ability to **modify** the security attributes **workflow group, workflow role, [assignment: list of additional security attributes]** to **managers**.

FMT_MSA.1(3) Management of security attributes (Active privileges)

FMT_MSA.1.1 The TSF shall enforce the **SWFS access SFP and Workflow access SFP** to restrict the ability to **modify** the security attributes:

- **set of active privileges**
- **[assignment: list of additional security attributes]**

to **the client who owns the session**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **SWFS access SFP, Workflow access SFP, Workflow flow SFP,** [**assignment: application flow SFP(s)**] to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **administrators** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) Management of TSF data (Audit logs)

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, create, query, modify, delete, clear, [assignment: other operations]] the

- **audit logs**

to **administrators**.

Application note: It is left to the conforming PP/ST to specify which operations the administrator should be restricted to use on the audit data.

FMT_MTD.1(2) Management of TSF data (Audited events)

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

- **set of audited events**

to **administrators**.

FMT_MTD.1(3) Management of TSF data (System)

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the

- **SFWS access control SFP**
- **application flow SFP(s)**
- **Workflow access SFP**
- **Workflow flow SFP**
- **identification and authentication data**
- **mapping of authorised users to roles**
- [**assignment: list of additional TSF data**]

to **administrators**.

FMT_MTD.1(4) Management of TSF data (Workflow management)

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection: modify, delete, clear, create, [assignment: other operations]**] the

- **process definitions**
- **[assignment: list of workflow related TSF data, which managers need to have access to]**

to **managers**.

FMT_MTD.1(5) Management of TSF data (Workflow instances)

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection: create, suspend, terminate, delete, monitor, [assignment: other operations]**] the

- ***workflow instances***

to **managers, [assignment: other authorised identified roles]**

FMT_SMF.1 Specification of management functions

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

- **Functions to assign and maintain lists of authorised users**
- **Functions to manage object security attributes**
- **Functions to manage user security attributes**
- **Functions to manage and review the audit data.**
- **Functions to manage the SFWS access SFP**
- **Functions to manage the Workflow access SFP**
- **Functions to create and manage the application flow SFP(s)**
- **Functions to manage the Workflow flow SFP**
- **Functions to manage process definitions and workflow instances**
- **Functions to monitor workflow instances**
- **Function to create and recover backups.**
- **Functions to manage the session locking methods.**
- **[assignment: list of additional management functions to be provided by the TSF]**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Client**
- **Manager**
- **Administrator**
- [**assignment: additional authorised identified roles**]

Application note: ST authors may identify additional roles, i.e. roles which refines upon one of the existing ones in order to achieve a more detailed division of roles.

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

A.5.1.5 FPT Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF].

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 a remote trusted IT product within the following metric: [assignment: a defined modification metric].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: action to be taken] if modifications are detected.

FPT_RCV.1 Manual recovery

FPT_RCV.1.1 After [assignment: list of failures/service discontinuities] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that [assignment: list of functions and failure scenarios] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

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

A.5.1.6 FTA TOE access

FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by:

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

***A*pplication note:** The time interval of user inactivity should be defined with respect to the implementation of the user-initiated locking (FTA_SSL.2). E.g. if the user-initiated locking is activated by the removal of a physical token, e.g. a smart card or a USB key, the time interval of user inactivity may be set to a very high value.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: **Re-authentication of the user**.

FTA_SSL.2 User-initiated locking

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

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: **Re-authentication of the user**.

A.5.1.7 FTP Trusted path/channels

FTP_ITC.1 Inter TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote 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 [**selection: the TSF, [assignment:one or more SWFSs**]] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- **establishing a connection with a SWFS, which it wishes to exchange information with**
- **establishing a connection with a trusted applications which it wishes to invoke**
- [**assignment: list of additional functions for which a trusted channel is required**]

A.5.2 Security assurance requirements

This section gives the security assurance requirements which are to be fulfilled. A PP compliant TOE is to be evaluated at evaluation assurance level 3 augmented (EAL3+) from part 3 of CC[10]. EAL3 has been augmented with the assurance requirement ALC_CMS.4. The assurance requirements are listed in table A.3.

A.5.2.1 ADV_ARC.1 Security architecture description

Developer action elements

Assurance class	Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table A.3: Assurance Requirements

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.2 ADV_FSP.3 Functional specification with complete summary

Developer action elements

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the non-SFR-enforcing actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

A.5.2.3 ADV_TDS.2 Architectural design

Developer action elements

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the non-SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements

ADV_TDS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

A.5.2.4 AGD_OPE.1 Operational user guidance

Developer action elements

AGD_OPE.1.1D The developer shall provide the design of the TOE. available in the TOE design.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.5 AGD_PRE.1 Preparative procedures

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

A.5.2.6 ALC_CMC.3 Authorisation controls

Developer action elements

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

Content and presentation elements

ALC_CMC.3.1C The TOE shall be labeled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements

ALC_CMC.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.7 ALC_CMS.4 Problem tracking CM coverage

Developer action elements

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.8 ALC_DEL.1 Delivery procedures

Developer action elements

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.9 ALC_LCD.1 Developer defined life-cycle model

Developer action elements

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.10 ALC_DVS.1 Identification of security measures

Developer action elements

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

A.5.2.11 ATE_COV.2 Analysis of coverage

Developer action elements

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.12 ATE_DPT.1 Testing: basic design

Developer action elements

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.13 ATE_FUN.1 Functional testing

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

A.5.2.14 ATE_IND.2 Independent testing - sample

Developer action elements

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF interfaces to confirm that the TSF operates as specified.

A.5.2.15 AVA_VAN.2 Vulnerability analysis

Developer action elements

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

A.5.3 Security requirements rationale

This section gives the rationales to why the PP security objectives are satisfied by the TOE security requirements, which have been traced to them. Additionally it is shown that all dependencies have been fulfilled. Finally a rationale that explains why the evaluation assurance level EAL3 has been deemed appropriate is given.

A.5.3.1 SFR rationale

Table A.4 shows the tracing between security objectives and SFRs. Table A.5 gives all the dependencies on the SFRs and shows that they all are fulfilled.

O.AUTH The components FIA_UID.2 and FIA_UAU.2 ensures that users are required to authenticate themselves before any action in the TOE is allowed by the TSF. FIA_UAU.7 ensures that the feedback given to the user during authentication is limited such that the TSF authentication mechanism is more robust against attacks.

O.ACCESS The components FDP_ACC.1(1) and FDP_ACF.1(1) ensures that a SWFS access SFP is specified and enforced for all TOE application data.

FDP_ACC.1(2) and FDP_ACF.1(2) ensures that a Workflow access SFP is specified which enforces the workflow instances' access SFPs. FIA_ATD.1 provides the TSF with information about users needed to enforce the TSP. FIA_USB.1 supports the objective by binding the user security attributes to subjects acting on their behalf.

O.FLOW The components FDP_IFC.1(1) and FDP_IFF.1(1) ensures that a information flow control SFP is specified and enforced for all user applications, invokable applications and SFWSs which the TOE can interact with.

FDP_IFC.1(2) and FDP_IFF.1(2) ensures that a Workflow flow SFP is specified which enforces the workflow instances' flow SFPs. FIA_ATD.1 provides the TSF with information about users which is needed to enforce the TSP. FIA_USB.1 supports the objective by binding the user security attributes to subjects acting on their behalf.

O.MANAGE The components FMT_MOF.1, FMT_MSA.1(1-2), FMT_MSA.2, FMT_MTD.1(1-3) and FMT_SMR.1 ensures that administrators are able to manage the security functions, security attributes and relevant TSF data. FMT_SMF.1 provides the security functions required for the managing.

FMT_MSA.3 ensures that the TSF provides default values for the relevant security attributes.

O.WORKFLOW The components FMT_MSA.1(2), FMT_MTD.1(4-5) and FMT_SMR.1 ensures that managers are able to manage the security functions, security attributes and relevant TSF data of workflows. FMT_SMF.1 provides the security functions required for the managing.

FMT_MSA.2 and FMT_MSA.3 supports this by ensuring that the values for the security attributes are secure and ensures that the TSF provides default values for the relevant security attributes, respectively.

O.AUDIT The component FAU_GEN.1 ensures that auditable events are identified and audited. FAU_GEN.2 ensures that the audit records can be traced to individual users such that they are held accountable. FAU_SAR.1 and FAU_SAR.2 ensure that audit data can be reviewed only by administrators and users who have been granted explicit read access. FAU_STG.1 prevents unauthorised deletion and modification of the audit records.

O.DATAFLOW FDP_ITC.2 and FDP_ETC.2 ensures that when application data is imported from and exported to invoked applications and SWFSs outside of the TOE both the application flow control SFPs and the Workflow flow SFP are enforced. Furthermore the security attributes associated with the application data is used.
FPT_TDC.1 ensures that that a consistent interpretation of the security attributes exists between the TOE, the invoked applications and the SWFSs.

FDP_UIT.1 ensures that the integrity of all application data transmitted from the TOE can be checked and that the integrity of all application data upon TOE receipt is verified. FPT_ITI.1 ensures the same for all TSF data transmitted between the TOE and any trusted application.

O.RECOVER The component FPT_RCV.1 ensures that the TSF enters a maintenance mode in the event of a failure, from where it can return to a secure state. E.g. if data is corrupted or lost an administrator can by the use of a backup restore the data such that the TSF can return to its normal and secure operation. FPT_RCV.4 ensures that the TSF provides additional protection in the event of a failure by ensuring that certain functions either completes successfully or recovers to a consistent and secure state. FPT_FLS.1 ensures that the TSF in the event of a failure will preserve a secure state where all SFRs are enforced.

The components FMT_SMF.1 provides the functions for managing the backup and recovery mechanisms, while FMT_MOF.1 restricts their use to the administrators.

O.SESSION FTA_SSL.1 and FTA_SSL.2 ensures that the TSF allows TSF-initiated session locking after an administrator specified time of user inactivity and user-initiated session locking, respectively. FIA_UAU.6 ensures that the user is re-authenticated when the session has been locked before re-gaining access to the TOE.

O.TRUSTED FTP_ITC.1 ensures that the applications which the TOE can invoke and/or the SWFSs which the TOE can communicate with provide a communication channel which is logical distinct from other communication channels. It is hereby ensured that a assured identification of the channels end points exists and that the channel data is protected.

	O.AUTH	O.ACCESS	O.FLOW	O.MANAGE	O.WORKFLOW	O.AUDIT	O.DATAFLOW	O.RECOVER	O.SESSION	O.TRUSTED
FAU_GEN.1						x				
FAU_GEN.2						x				
FAU_SAR.1						x				
FAU_SAR.2						x				
FAU_STG.1						x				
FDP_ACC.1(1)		x								
FDP_ACC.1(2)		x								
FDP_ACF.1(1)		x								
FDP_ACF.1(2)		x								
FDP_IFC.1(1)			x							
FDP_IFC.1(2)			x							
FDP_IFF.1(1)			x							
FDP_IFF.1(2)			x							
FDP_ETC.2							x			
FDP_ITC.2							x			
FDP_UIT.1							x			
FIA_ATD.1		x	x							
FIA_UAU.2	x									
FIA_UAU.6									x	
FIA_UAU.7	x									
FIA_UID.2	x									
FIA_USB.1		x	x							
FMT_MOF.1				x				x		
FMT_MSA.1(1)				x						
FMT_MSA.1(2)				x	x					
FMT_MSA.1(3)										
FMT_MSA.2				x	x					
FMT_MSA.3				x	x					
FMT_MTD.1(1)				x						
FMT_MTD.1(2)				x						
FMT_MTD.1(3)				x						
FMT_MTD.1(4)				x	x					
FMT_MTD.1(5)				x	x					
FMT_SMF.1				x	x			x		

Table A.4: Tracing of TOE security objectives to SFRs (continued on next page).

	O.AUTH	O.ACCESS	O.FLOW	O.MANAGE	O.WORKFLOW	O.AUDIT	O.DATAFLOW	O.RECOVER	O.SESSION	O.TRUSTED
FMT_SMR.1				x	x					
FPT_FLS.1								x		
FPT_ITI.1							x			
FPT_RCV.1								x		
FPT_RCV.4								x		
FPT_TDC.1							x			
FTA_SSL.1									x	
FTA_SSL.2									x	
FTP_ITC.1										x

Table A.4: Tracing of TOE security objectives to SFRs.

SFR	**Dependency**	**Resolved**
FAU_GEN.1	FPT_STM.1	The dependency has not been fulfilled, since the underlying OS will provide the reliable clock as described in OE.TIME.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	 by FIA_UID.2 which is hierarchical
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	
FAU_STG.1	FAU_GEN.1	
FDP_ACC.1(1)	FDP_ACF.1	by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	by FDP_ACC.1(1)
FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	by FDP_ACC.1(2)
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	by FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1)

Table A.5: continued on next page

SFR	Dependency	Resolved
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1)
FDP_ETC.2	FDP_IFC.1	by FDP_IFC.1(1) and FDP_IFC.1(2)
FDP_ITC.2	FDP_IFC.1 FTP_ITC.1 FPT_TDC.1	by FDP_IFC.1(1) and FDP_IFC.1(2)
FDP_UIT.1	FDP_IFC.1 FTP_ITC.1	by FDP_IFC.1(1)
FIA_ATD.1	None	
FIA_UAU.2	FIA_UID.1	by FIA_UID.2 which is hierarchical
FIA_UAU.6	None	
FIA_UAU.7	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FIA_UID.2	None	
FIA_USB.1	FIA_ATD.1	
FMT_MOF.1	FMT_SMR.1	
	FMT_SMF.1	
FMT_MSA.1(1)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1) and FDP_ACC.1(2)
FMT_MSA.1(2)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1)
FMT_MSA.1(3)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1) and FDP_ACC.1(2)
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	by FDP_ACC.1(1-2) and FDP_IFC.1(1-2)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	by FMT_MSA.1(1-3)
FMT_MTD.1(1-5)	FMT_SMR.1 FMT_SMF.1	
FMT_SMF.1	None	

Table A.5: continued on next page

SFR	Dependency	Resolved
FMT_SMR.1	FIA_UID.1	by FIA_UID.2 which is hierarchical
FPT_FLS.1	None	
FPT_ITI.1	None	
FPT_RCV.1	AGD_OPE.1	
FPT_RCV.4	None	
FPT_TDC.1	None	
FTA_SSL.1	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FTA_SSL.2	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FTP_ITC.1	None	

Table A.5: Dependencies of SFRs. If the 'resolved' column is empty the dependency is directly fulfilled by the inclusion of the dependent SFR in the PP.

A.5.3.2 SAR Rationale

An evaluation assurance level of EAL3+ has been deemed appropriate, since EAL3 gives a moderate level of independently assured security. EAL3 has been chosen over EAL2 because it requires more complete testing coverage of the security functionality and mechanisms/procedures which ensure a higher level of security in the development environment. The augmented assurance required provides added assurance that flaws are tracked and resolved during development.

Appendix B

Centralised Secure Workflow System Security Target

Version 1.0

February 2007

Contents

B.1 ST introduction

B.1.1 ST reference

Title:	Centralised Secure Workflow System Security Target
Version:	1.0
Author:	Rune Friis-Jensen, s011375, IMM, The Technical University of Denmark (DTU)
Publication date:	2007-02/05
CC Version:	3.1 Revision 1
Assurance Level:	EAL3+

B.1.2 TOE Overview

B.1.2.1 TOE Type

This Security Target (ST) specifies the security requirements for a Secure Workflow System as defined in the Secure Workflow Systems Protection Profile 1.0[19].

> A SWFS provides consumers with a system which is able to control the execution of business processes, workflows. Workflows consists of a combination of manual and automated activities. It is the objective of the SWFS to ensure that this is done in a secure manner
>
> The SWFS interprets process definitions, which are computer processable definitions of business processes and creates instances of these, workflow instances. When a workflow instance has been created the SWFS will in accordance with the workflow instance's process definition automatically execute the defined business process by assigning tasks to worklists. These worklists can be accessed by authorised workflow clients which can then process the workitem of the task. At all times the SFWS ensures that the required information to support each step of the workflow is available.
>
> A SWFS will have the capability to limit access to authorised users, enforce protection of assets both physically and logically and ensure that individual users are held accountable for their actions through the use of auditing.
>
> The Secure Workflow Systems Protection Profile (SWFSPP) uses some of the standard workflow terms defined by the Workflow Management Coalition(WfMC), but does not have any requirements on

> WfMC conformance. The term workflow system and task are equivalent to the WfMC terms workflow enactment service and activity respectively.[20]

The TOE of this ST employs a centralised architecture where the core of the workflow system is deployed on a server. The TOE manages a single workflow engine which is entirely responsible for managing the execution of all workflows.

B.1.2.2 General TOE features

This ST conforms to the Secure Workflow Systems Protection Profile 1.0 (SWFSPP) [19]. This implies that the TOE provides functionality to:

- control user access to the TOE, the assets and the TOE Security Functions (TSF)
- instantiate process definitions
- control workflow instantiations
- invoke trusted applications
- perform utility tasks like backup and recovery of assets
- generate audit data

The TOE furthermore provides functionality to:

- modify workflow instances

B.1.2.3 TOE roles

The TOE provides the three authorised user roles as specified in the SWFSPP [19] with no additions. The authorised user roles are:

Administrator A person who has privileges to install, configure and maintain the TOE and its security functions. This includes e.g. the ability to:

- manage the group of authorised users and the associated authentication data
- maintain and review the generated audit data
- manage the various Security Function Policies (SFP)

Manager A person who has privileges to create, modify and delete process definitions and manage workflow instances within the TOE. This includes e.g. the ability to:

- associate clients with workflow roles
- assignment and re-assignment of workitems
- monitoring the progress of task instances and workflow instances

Client A person or application which can participate in one or more workflows through the processing of tasks.

B.1.2.4 TOE communication

As specified in the SWFSPP [19] the TOE may interact with the following IT entities outside of the TOE:

- Client applications that allows clients to interface with the TOE in order to access worklists, workflow relevant data and application data which they are authorised for.
- Manager applications and tools that allow managers to interface with the TOE in order to manage process definitions and workflow instances.
- Administrator applications and tools that allow administrators to interface with the TOE in order to install, configure and manage the TOE and the TSF.
- Trusted applications which can be invoked by the TOE.
- Trusted SWFSs which the TOE exchanges information with.

B.1.2.5 TOE security features

The TOE will provide the following security services completely:

Identification and authentication of all TOE roles, invokable applications and SWFSs.[19]

Access control to the TOE application data through the specification of access control SFPs.[19]

Information flow control of TOE application data through the specification of information flow control SFPs.[19]

Audit generation to capture all auditable events, thereby providing capability to hold users accountable for their actions and detect malicious behaviour.[19]

Secure audit review which allows administrators to review stored audit records and detect potential and actual security violations.[19]

Authorised administration through the administrator role, which allows administrators to configure and manage the access control SFPs, information flow control SFPs, the identification and authentication of users and the auditing functions.[19]

Adaptive recovery through editing of process definitions and workflow instances.

The TOE will provide the following security service in co-operation with the IT environment:

Secure audit storage which stores all records for all security relevant operations performed on the TOE.[19]

Cryptographic support for ensuring that sensitive information can be adequately protected when it is transferred from and to the TOE.

Backup of data such that corrupted or deleted data may be recovered.[19]

B.1.2.6 Available non-TOE hardware/software/firmware

This section includes a list of non-TOE hardware/software which has to be available. The list should not be thought of as complete, but rather give the consumer a indication of what non-TOE hardware/software is required as a minimum by the TOE.

- Server
- Operating system
- Data storage i.e database and/or file system

B.1.3 TOE Description

The TOE is a secure workflow system(SWFS) which consists of a Workflow System Application hosted on a server and a Trusted Client Application deployed on trusted machines. The TOE is implemented in software, which runs

on top of the host operating system(OS). Secure interfaces for administration, workflow management, invocation of trusted applications and SWFSs and client interaction are provided. Communication with users and applications is across an insecure network.

B.1.3.1 Physical scope of the TOE

The TOE consists of two components the Workflow System Application running on a server and the Trusted Client Application running on trusted client machines. Figure B.1 illustrates the physical scope of the TOE. The shaded components are the TOE, while the remaining ones are part of the IT environment.

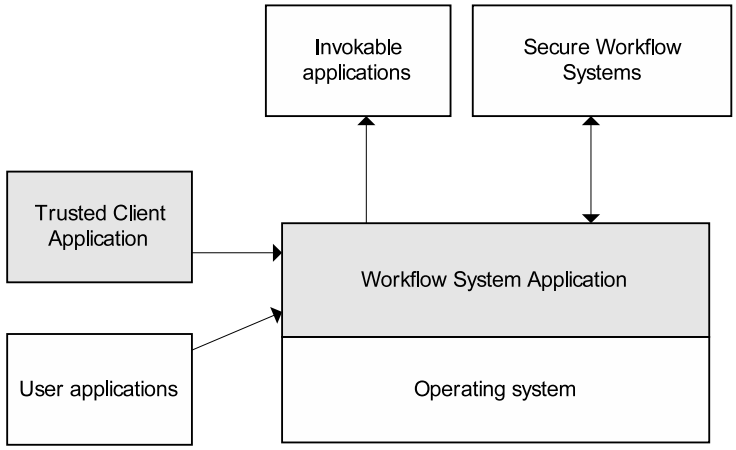

Figure B.1: The physical scope of the TOE. The shaded components are the TOE. The unshaded components is the IT environment. The direction of the arrows indicate which component initiates communication.

The Workflow System Application provides the main functionality of the TOE. It manages the execution of workflows and implements all of the security functions of the TOE. The Workflow System Application provides an interface for both the Trusted Client Application as well as other user applications. Furthermore interfaces are provided for invocation of applications and communication with other SWFSs.

The Trusted Client Application ensures that when the application is running it provides the only visible graphical user interface on the machine. Furthermore it is ensured that information flow policies of the TOE are enforced. E.g.

it should not be possible for a client to copy information from the Trusted Client Application to a local application using the OS window manager's cut/copy and paste functionality and vice versa. The Trusted Client Application is the only client application which may send and receive application data which has a sensitivity level above public (see Application data protection in section B.1.3.2).

B.1.3.2 Logical scope of the TOE

The logical scope of the TOE can be described in the terms of the TOE's security functions.

Identification and authentication

The Workflow System Application supports identification and authentication of all TOE roles, invokable applications and SWFSs. Identification and authentication must be accomplished before any actions can be made. Authentication data will be verified against the Workflow System Applications identification and authentication repository. If verification is successful access is granted.

Application data protection

The Workflow System Application provides protection of application data through the enforcement of both access control and information flow control.

The access control is enforced through the SWFS access SFP and the Workflow access SFP as described in the SWFSPP([19], A.1.2.6).

For enforcement of information flow control, the TOE supports the classification of data with a sensitivity label. The TOE supports two labels 'public' and 'private'. The 'private' label is associated with a set of workflow groups in which the data should be kept private. I.e. it should not be possible to make private data available outside of the specified workflow groups. Data which is classified as 'public' has no restriction and may flow from and to any TOE user. Figure B.2 illustrates the hierarchical structure of the sensitivity labels within a system with three workflow groups.

In order to control the information flow between the data with different sensitivity labels, the TOE specifies a Workflow flow SFP. The Workflow flow SFP specifies when data from one object may flow into another object.

The partial ordering of sensitivity labels is defined by the following rules:

- The sensitivity label of an object A is greater than that of object B if one of the following conditions exist:
  - The sensitivity label of A is private$\langle X \rangle$, where X is the set of workflow

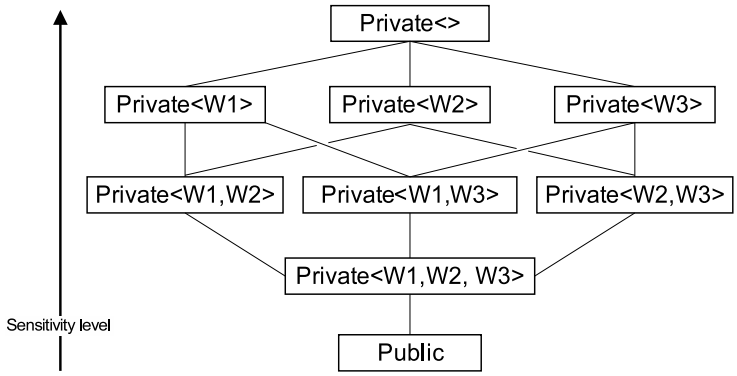

Figure B.2: Sensitivity levels which can be assigned to application data within a system with three workflow groups.

groups where the object is private and the sensitivity label of object B is public.

– The sensitivity label of A is private$\langle X \rangle$ and the sensitivity label of B is private$\langle Y \rangle$ and X is a proper subset of Y ($X \subset Y$).

- The sensitivity label of an object A is equal to that of object B if one of the following conditions exist:
  - The sensitivity label of A is public and the sensitivity label of B is public.
  - The sensitivity label of A is private$\langle X \rangle$ and the sensitivity label of B is private$\langle Y \rangle$ and the set X is equal to the set Y.
- The sensitivity label of an object A and object B is incomparable if they are not equal and neither has a greater sensitivity label than the other.

The classification of application data is specified within the process definitions flow SFP. The process definition flow SFP specifies how data which is created during the workflow is to be classified. Classification may be controlled entirely by the process flow SFP or it may specify that certain roles may classify data according to specified rules. Additionally it may be specified when and how data may be declassified that is lowering the sensitivity level of data.

A workflow example where declassification could be required is the publishing of a report. It may be required that the report should be kept private during its preparation while the published report should be public. To obtain this the flow SFP may specify that the executor of the final task of releasing the report may declassify the report from private to public.

To conform to the Secure Workflow Systems Protection Profile each user application, invokable application and SWFS, which the TOE may communicate with, has to be covered by an application flow SFP. The TOE of this ST fulfills this requirement by defining a limited, a basic and a Advanced application flow SFP. An application must be covered by one of these policies in order to able to interact with the TOE.

If an application is covered by the Limited application flow SFP the TOE may only send information of public sensitivity to it. All information received from the application shall by default be classified as public.

If an application is covered by the Basic application flow SFP the application must be CC certified at EAL3 or higher. The TOE may only send information of public sensitivity to the application. Information of any sensitivity level may be received from the application.

If an application is covered by the Advanced application flow SFP the application must be CC certified at EAL3 or higher and be capable of enforcing the Workflow flow SFP. Information of any sensitivity level may be sent from and received by the TOE.

The Trusted Client Application provides protection of application data by enforcing the Workflow flow SFP and the Advanced application flow SFP such that clients are prevented from bypassing the information flow control rules of the TOE.

Audit functions

All security relevant actions and events within the Workflow System Application are logged. For each such action or event an audit record is generated containing: date and time of the event, user, security attributes and success or failure. This ensures that users can be held accountable for their actions. The audit records are stored in a secure manner such that they can be reviewed by administrators in order to detect malicious behaviour or the extent of compromise.

Security management

The TOE allows for authorised administration by users assigned to the administrator role through a administration interface provided by the Workflow System Application. Administrators have the capability to manage the security-related functions and attributes. This includes management of:

- identification and authentication mechanisms
- users and their associated authentication data and TOE roles
- audit functions

- security functional policies (SFPs)
- backup and recovery functions
- session locking functions
- cryptographic functions used

Security related to the individual workflows are managed by users assigned to the manager role through the workflow management interface provided by the Workflow System Application. Managers have the capability to manage:

- process definitions and their associated access and flow SFPs.
- mapping of authorised users to workflow roles
- workflow instances

When process definitions are edited the manager has to decide whether the changes should be propagated to executing workflow instances of the process definition. If not then only future workflow instances will adhere to the new process definition. If changes should be propagated the manager shall decide upon which instances the changes should be propagated to. Changes may be propagated to one of the following:

- all instances
- specific instances
- instances which have surpassed the changes
- instances which have not reached the changes

If changes should be propagated to instances which has surpassed the changes the TOE will try to compensate or rollback the instance such that it fulfills the requirements of the process definition. If the propagation of changes fails the manager is consulted for further actions.

If an instance is edited a new branch of its process definition is created, which is used instead of the original one. When a instance has completed a manager may decide to propagate the changes to the original process definition.

The support for changing workflow instances does not only make the system more flexible but it also makes it more resistant to failures. Although the correctness of process definitions are verified before and when they are instantiated errors may still occur during the execution of workflow instances. This may for example be due to changes in the environment, such as inability to connect to

a resource or a failure in an invoked application. With no support for changes to workflow instances it may only be possible to rollback and retry or skip the faulty task in order to recover from the error. By supporting changes the TOE may additionally try to dynamically reconfigure the workflow instance or request a manger to get involved in changing the workflow instance such that it may recover from the error.

Cryptographic support

Cryptographic support is provided in co-operation with the host OS, which is a part of the IT environment. The OS shall provide a cryptographic service provider (CSP) which is FIPS140-2 certified. The Workflow System Application is required to ensure that FIPS140-2 compliant algorithms are used.

The TSF relies on cryptographic support to mutually authenticate TOE components, invokable applications, SWFSs and users. Furthermore all network communication is protected by cryptographic means to prevent loss of confidentiality and integrity.

Backup

The TOE provides a secure backup mechanism which is to be used to ensure that deleted or corrupted data may be restored. The administrator of the TOE may schedule when a backup of specific data should be made. The scheduling may either be based on time or according to specified system events. It is the job of the administrator to setup onto which storage media backups should be made and to ensure that backups are stored in a physical different location than the rest of the TOE. Furthermore the confidentiality, integrity and availability of backups must be ensured and regularly checked.

B.2 Conformance claims

This ST conforms to the Common Criteria for Information Technology Security Evaluation(CC) version 3.1, revision 1. The ST is CC Part 2 conformant, CC Part 3 conformant and EAL3 Augmented.

B.3 Security problem definition

This section defines the security problem to be addressed by listing:

- the threat agents of the TOE

- the assumptions on the operational environment
- the threats to be countered by the TOE
- the organisational security policies(OSPs) to be enforced by the TOE

B.3.1 Threat Agents

As of SWFSPP[19] the threat agents can be categorized as shown below.

Authorized user	An authorized manager or client.
Unauthorized user	An entity which is **not** authorized to access the TOE.
External events	Interruption of TOE operation due to failure of hardware, storage, power supply, fire, water damage etc.

Note that administrators are not considered a threat agent which is due to the assumption **AP.ADMIN**. In the following the term attacker will be used to denote any of the threat agents.

B.3.2 Assumptions

In order for the TOE to be considered secure the operational environment has to meet the following assumptions on personnel and connectivity.

B.3.2.1 Personnel

AP.ADMIN	*The administrators of the TOE are qualified in managing and maintaining the TOE and can be trusted not to abuse their privileges.* This assumption is made to ensure that at least one user of the TOE can be trusted to be able to manage and maintain the TOE and the security functions and data it contains.[19]

B.3.2.2 Connectivity

AC.RESOURCE	*The TOE has sufficient resources available to function properly and securely.*

This assumption is made to ensure that the TOE and its security functions are able to operate reliably.[19]

AC.OS *The underlying operating system and network services which the TOE relies upon are installed, configured and managed in a secure manner.*

Since the TOE is implemented in software it relies upon the underlying OS and hardware. This assumption therefore has to be made to guarantee that the TOE will operate in a secure manner.[19]

AC.TIME *The underlying operating system shall provide the TOE with a clock which is synchronized with a reliable hardware clock.*

B.3.3 Threats

This section describes the threats that are to be countered by the TOE and its operational environment or a combination of these. All threats pose a threat to either primary assets as listed in section B.1.2 or secondary assets such as TSF security attributes. All the listed threats have been derived with the earlier described assumptions in mind.

T.ACCESS *Unauthorized access to the TOE.*

Besides the case where an attacker is able to bypass the access mechanisms of the TOE completely, the threat also includes the case where an attacker is able to access the TOE by impersonating an authorised user or an administrator.[19]

T.DATA *Unauthorized access to application data.*

An attacker accesses data which it does not have permission to access.[19]

T.DATAFLOW *The integrity of the information flowing from or to the TOE is compromised.*

An attacker may compromise the integrity of the data transmitted from and to the TOE deliberately or accidentally by changing its content.[19]

T.MODIFY *Information protected by the TOE is modified maliciously by an attacker.*

As opposed to T.ACCESS this threat deals with the case where the attacker actually tries to make malicious changes to the data protected by the TOE.[19]

T.UNATTENDED *An attacker gains access to the TOE by the use of an unattended session.*

If an authorised user leaves a session open without shutting it down an attacker could takeover the session and gain unauthorized access to the TOE and its assets.[19]

T.PHYSICAL *The underlying OS/network services are physically damaged in a way that prevents the TOE from functioning properly or results in loss of data.*[19]

T.MALFUNCTION *Malfunction in the TOE or underlying OS/network services prevents the TOE from functioning properly or results in loss of data.*

Malfunction comprises all software and hardware errors which are the cause of interruption of the operation of the TOE and may cause TOE assets to be lost or corrupted.[19]

T.TRUSTED *The TOE invokes a trusted application or exchanges information with a SWFS which has been compromised or is being impersonated by an attacker.*

This threat deals with that an invokable application or SWFS may be compromised without detection by the TOE.[19]

T.TRUST_CLIENT *An attacker may impersonate the Trusted Client Application and thereby be able to disclose confidential information.*

T.TRUST_SERVER *An attacher may impersonate the Workflow System Application and gain access to user authentication information, which can be used to gain unauthorised access to the Workflow System Application.*

T.SECRET_FLOW *The confidentiality of information flowing across a network from and to the TOE is disclosed to an attacker.*

T.CRYPTO_KEYS *An attacker compromises the security of the TOE by disclosing cryptographic keys used for securing information flowing to and from the TOE.*

B.3.4 Organization security policies

This section lists the organizational security policies (OSPs) to be enforced by the TOE and its operational environment, or a combination of these.

P.ACCESS *Only authorized users and administrators may access the TOE.*

This policy exists to ensure that only administrators and authorised users may access or interact with the TOE. The policy hereby prevents anonymous access to and unauthenticated communication with the TOE.[19]

P.TRAINING *Authorized users and administrators shall be continuously trained in using the TOE properly and securely.*

The purpose of this policy is to ensure that the authorised users and administrators of the TOE are capable of operating the TOE in a secure manner.[19]

P.ACCOUNT *Authorized users shall be held accountable for their interactions with the TOE.*

The policy is to ensure that all authorized users can be held accountable for their actions and that fraud and malicious intents can be acted upon by the administrators of the TOE.[19]

P.APPLICATION *All applications which the TOE can invoke shall be run on trusted machines which configuration can only be changed by highly trusted persons who are authorised to do so and can be held accountable.*[19]

P.WORKFLOW *Managers shall be able to manage the security mechanisms of the workflows which they are responsible for.*[19]

P.FIPS140 *All cryptographic functions used by the TOE shall be FIPS PUB 140-2 compliant.*

P.TRUST_CLIENT *The Trusted Client Application shall be installed and configured in a manner that maintains the security of the TOE.*

P.USER_AUTH *Administrators and managers shall be required to authenticate using token and token PIN.*

B.4 Security objectives

B.4.1 Security objectives of the TOE

This section lists the security objectives of the TOE.

O.AUTH *The TOE shall provide means for identifying and authenticating users before allowing access to the TOE and its resources.*[19]

O.ACCESS *A SWFS access SFP shall be specified which enforces the TOE access control requirements. Furthermore a Workflow access SFP shall be specified which shall enforce the access SFP of workflow instances.*[19]

O.FLOW *Each user application, invokable application and SWFS the TOE interacts with must be covered by an application flow SFP. Furthermore a Workflow flow SFP shall be specified which shall enforce the flow SFP of a workflow instance.*[19]

O.MANAGE *The TOE shall provide means of enabling administrators to manage the security mechanisms of the TOE*

and restrict these mechanisms from unauthorized use. [19]

O.WORKFLOW *The TOE shall provide means of enabling managers to manage the security mechanisms of the workflows which they are are responsible for.*[19]

O.AUDIT *The TOE shall provide means of recording security relevant events in sufficient detail to help an administrator to detect attempted security violations and hold users accountable for any actions that are relevant to the security of the TOE.*[19]

O.DATAFLOW *The integrity of all data which is received and sent through the TOE interfaces must be protected.*[19]

O.RECOVER *The TOE shall provide administrators with functionality which ensures the that the TOE can recover effectively after a system failure without compromising the security of the TOE. This includes providing functionality which ensures that backups of the TOE assets and TOE security functional data are made regularly and that the confidentiality, integrity and availability of these backups are adequately protected.* [19]

O.SESSION *The TOE shall provide functionality that allows an authorised user or the TSF to invalidate or lock the user's current session after some reasonable period of inactivity. To unlock the session the user must reauthenticate.*[19]

O.TRUSTED *The TOE shall provide means for additional assurance of the authenticity of trusted applications which are invoked and trusted SWFSs which the TOE exchanges information with.*[19]

O.AUTHENTIC *The Workflow System Application shall authenticate itself to the user before allowing any communication.*

O.AUTH_CLIENT *The Trusted Client Application and the Workflow System Application shall mutually authenticate using a trusted channel before allowing any communication.*

O.FIPS140 *The cryptographic functions used by the TOE shall be FIPS140-2 compliant.*

O.SECRET_FLOW *The confidentiality of all data which is received and sent through the TOE interfaces must be protected.*

O.USER_AUTH *The TOE shall provide the following authentication mechanisms where the use of username and password is restricted to clients:*

- *token and token PIN*
- *username and password*

B.4.2 Security objectives of the operational environment

This section lists the security objectives of the operational environment.

OE.PHYSICAL *The operational environment shall ensure that the TOE and its underlying services are sufficiently protected from physical damage by an attacker.*[19]

OE.ADMIN *The operational environment shall ensure that only highly qualified and trusted users are given administrative privileges.* The personnel with administrative privileges must be throughly vetted to ensure that they are competent and can be trusted not to abuse their privileges.[19]

OE.BACKUP *The operational environment shall ensure that backups of the TOE assets and TSF data are stored physically separate from TOE and are protected from physical damage.*

OE.TRAINING *The operational environment shall ensure that all authorised users of the TOE and the administrators are continuously trained in the proper and secure use of the TOE.*[19]

OE.RESOURCE *The operational environment shall ensure that the TOE always has sufficient resources to operate properly and securely.*[19]

OE.APPLICATION *The operational environment shall ensure that all invokable applications and SWFSs which the TOE communicates with run on trusted machines whose configuration can only be changed by authorised personnel and who can be held accountable.*[19]

OE.OS *The operational environment shall ensure that the TOE, the underlying OS and hardware are installed, configured and operated in a way that maintains the security of the TOE. This includes that a security domain is provided which ensures that the TOE cannot be tampered with by other applications since the OS/hardware makes the interfaces through which the TOE can be accessed inaccessible to other applications. Furthermore it must be ensured that the OS and hardware will faithfully execute the commands of the TOE and will not tamper with the TOE in any manner.*[19]

OE.TIME *The operational environment shall ensure that the underlying OS provides the TOE with a reliable clock which is synchronized with a reliable hardware clock.*[19]

OE.CRYPTO_KEYS *Cryptographic keys must be securely administered and protected from disclosure.*

OE.FIPS140 *The operational environment shall ensure that the cryptographic service provider (CSP) provided to the TOE by the OS is FIPS140-2 compliant.*

This means that the operating system must be configured such that only FIPS140-2 implemented algorithms are used.

OE.TRUST_CLIENT *The operational environment shall ensure that the Trusted Client Application is installed and configured*

on client machines which are installed and configured by an administrator in a way that maintain the security of the TOE.

B.4.3 Security objectives rationale

This sections provides the security objectives rationale which gives justifies why all assumptions, threats and OSPs are effectively addressed. Furthermore a tracing which shows which threats, OSPs and assumptions are addressed by which security objectives. The tracing from the SWFSPP[19] is shown in table B.1 and the tracing of additional security objectives to threats and OSPs are shown in table B.2.

All argumentation based on the audit data assumes that it has not been compromised.

	AP.ADMIN	AC.RESOURCE	AC.OS	AC.TIME	T.ACCESS	T.DATA	T.DATAFLOW	T.MODIFY	T.UNATTENDED	T.PHYSICAL	T.MALFUNCTION	T.TRUSTED	P.ACCESS	P.TRAINING	P.ACCOUNT	P.APPLICATION	P.WORKFLOW
O.AUTH					x	x		x					x		x		
O.ACCESS						x		x									
O.FLOW						x											
O.MANAGE					x	x	x	x					x		x	x	
O.WORKFLOW																	x
O.AUDIT					x	x		x							x		
O.DATAFLOW							x										
O.RECOVER								x		x	x						
O.SESSION									x						x		
O.TRUSTED												x					
OE.PHYSICAL										x							
OE.ADMIN	x																
OE.BACKUP								x		x	x						
OE.TRAINING	x								x					x			
OE.RESOURCE		x															
OE.APPLICATION												x				x	
OE.OS			x														
OE.TIME				x													

Table B.1: Tracing of security objectives to assumptions, threats and OSPs as specified in the SWFSPP[19].

	T.ACCESS	T.DATA	T.DATAFLOW	T.TRUST_CLIENT	T.TRUST_SERVER	T.SECRET_FLOW	T.CRYPTO_KEYS	P.FIPS140	P.TRUST_CLIENT	P.USER_AUTH
O.AUTHENTIC	x				x		x			
O.AUTH_CLIENT		x		x			x			
O.FIPS140			x	x	x	x	x	x		
O.SECRET_FLOW						x				
O.USER_AUTH										x
OE.CRYPTO_KEYS							x			
OE.FIPS140			x	x	x	x	x	x		
OE.TRUST_CLIENT									x	

Table B.2: Tracing of additional security objectives to threats and OSPs.

AP.ADMIN The assumption is upheld by *OE.ADMIN and OE.TRAINING. OE.ADMIN directly upholds AP.ADMIN by requiring the operational environment to throughly vet the personnel, which are to be given administrative privileges, are qualified, competent and can be trusted not to abuse their privileges. OE.TRAINING supports this by assuring that the administrators are continuously trained and thereby remain qualified.*

AC.RESOURCE *This assumption is upheld entirely by OE.RESOURCE by requiring the operational environment to ensure that the TOE has sufficient resources to operate securely and reliably.[19]*

AC.OS *OE.OS solely upholds this assumption by requiring the operational environment to assure that the OS and underlying services are installed, configured and managed in a secure manner such that the security of the TOE is not compromised.[19]*

AC.TIME *OE.TIME entirely upholds this assumption by requiring the operation environment to ensure that the underlying OS provides a reliable clock which is synchronized with a reliable hardware clock e.g. synchronized via GPS.[19]*

T.ACCESS

This threat is primarily countered by O.AUTH which assures that the TOE provides means for authenticating users before allowing them access to the TOE. O.MANAGE and O.AUDIT both counter the threat indirectly. O.MANAGE assures that security mechanisms are provided for managing who has access to the TOE. O.AUDIT mitigates the situation where an attacker is able to compromise the authentication mechanism. It provides administrators with the means to react upon a security violation and track what the attacker has been doing. An administrator may hereby be able to reduce the damages.[19]

O.AUTHENTIC ensures that the user is connected to the authentic Workflow System Application. This prevents an attacker from impersonating the Workflow System Application and thereby gaining access to authentication data which may be used to gain access to the TOE.

T.DATA

The threat is countered by O.AUTH, O.ACCESS, O.FLOW, O.MANAGE, O.AUDIT and O.AUTH_CLIENT.

The first four objectives counters the threat directly by providing authentication of users and mechanisms for protection of application data through the use of access control and information flow control. O.ACCESS ensures that an attacker cannot access application data, while O.FLOW ensures that an authorised user cannot make application data available to an attacker. O.AUDIT enables administrators to detect attempted violation of access rights. They can hereby prevent that a violation actually occurs and mitigate the situation where data has been maliciously modified by being able to track what the attacker has been doing.[19]

O.AUTH_CLIENT ensures that an attacker cannot impersonate the Trusted Client Application and thereby get unauthorised access to data.

T.DATAFLOW

O.DATAFLOW and O.MANAGE counters the threat. O.DATAFLOW by requiring the TOE to protect the integrity of all data sent and verify the integrity of all data received. O.MANAGE assures that administrators have access to functionality to manage the secu-

rity mechanisms of the TOE which are used to provide the integrity protection of the transmitted data.[19]

O.FIPS140 and OE.FIPS140 ensure that the integrity of all data sent from and received by the TOE is protected by FIPS140-2 compliant algorithms.

T.MODIFY *This threat is mainly countered by O.AUTH, O.ACCESS and O.MANAGE by diminishing the likelihood of an attacker being able to access the TOE and access data. If an attacker is able to compromise the security of these objectives the treat is mitigated by O.AUDIT, O.RECOVER and OE.BACKUP.*

O.AUDIT makes it possible track an attackers malicious changes thereby improving the administrators chances of reducing the damage to the TOE data. O.RECOVER ensures that the TOE supports a backup mechanism such that malicious modified or deleted data may be possible to restore.

OE.BACKUP ensures that backups are kept physically separate from the TOE and that they are physically protected such that they are available. [19]

O.AUDIT makes it possible track an attackers malicious changes thereby improving the administrators chances of reducing the damage to the TOE data. O.RECOVER ensures that the TOE supports a backup mechanism such that malicious modified or deleted data may be possible to restore. Furthermore in cooperation with OE.BACKUP it is ensured that the TOE can recover effectively without compromising the security of the TOE.[19]

T.UNATTENDED *The threat is directly countered by O.SESSION, which requires the TOE to provide functionality for automatic invalidation or locking of a inactive user session. The possibility of an attacker taking advantage of the unattended session is thereby decreased. OE.TRAINING assures that the authorized users are trained in the secure use of the TOE, which in relation to the threat could be learning users to log off or lock their session when they do not use it or leave it physically.[19]*

T.PHYSICAL *The threat is countered by OE.PHYSICAL, O.RECOVER and OE.BACKUP. OE.PHYSICAL helps*

diminishing the threat by requiring that the operational environment makes sufficient precautions to prevent an attacker from physically damaging the TOE or any of its underlying services. If the TOE is physical damaged O.RECOVER may assist in restoring lost data and the effective recovery of the TOE. The loss of availability is hereby kept to a minimum without compromising the security of the TOE. OE.BACKUP ensures that backups are kept physically separate from the TOE such that they are available even when the TOE is physically damaged.[19]

T.MALFUNCTION *The threat is mitigated by O.RECOVER and OE.BACKUP for the same reasons as described for T.PHYSICAL.[19]*

T.TRUSTED *The threat is mitigated by O.TRUSTED together with OE.APPLICATION. It is ensured that the TOE provides additional assurance of an invoked application's or a SWFS's authenticity. Additionally the operational environment is required to ensure that these are sufficiently protected against compromise.[19]*

T.TRUST_CLIENT *Impersonation of the Trusted Client Application is countered by O.AUTH_CLIENT which ensures that the Workflow System Application and the Trusted Client Application must mutually authenticate before allowing any communication.*

O.FIPS140 and OE.FIPS140 ensures that FIPS140-2 compliant algorithms are used for the cryptographic functions.

T.TRUST_SERVER *Impersonation of the Workflow System Application is mitigated by O.AUTHENTIC which ensures that it will authenticate itself to the user before allowing any communication.*

O.FIPS140 and OE.FIPS140 ensures that FIPS140-2 compliant algorithms are used for the cryptographic functions.

T.SECRET_FLOW *The threat is countered by O.SECRET_FLOW which requires the TOE to encrypt all information flowing to and from the TOE. O.FIPS140 and OE.FIPS140 ensure that the encryption used is FIPS140-2 compliant.*

T.CRYPTO_KEYS *The threat is mainly countered by OE.CRYPTO_KEYS which ensures that the operational environment protects the cryptographic keys from disclosure. The threat is additionally countered by O.AUTHENTIC and O.AUTH_CLIENT which ensure that the Workflow System Application and the Trusted Client Application are communicating over a secure channel. The risk of disclosing the cryptographic keys is thereby minimized.*

O.FIPS140 and OE.FIPS140 ensures that the cryptographic functions are FIPS140-2 compliant.

P.ACCESS *The OSP is enforced by O.AUTH and O.MANAGE, which ensures that only authorized users can access the TOE. Additionally administrators are able to control the security functions of the TOE, i.e. defining who has access and who does not.[19]*

P.TRAINING *OE.TRAINING directly enforces this OSP by requiring the operational environment to arrange for training of all authorized users and administrators.[19]*

P.ACCOUNT *O.AUDIT directly supports this OSP since it assures that the TOE provides functionality to log security relevant events. Administrators are hereby able to hold users responsible for their interactions with the TOE. How much is to be logged is entirely up to administrator and operational environment, but it should be sufficiently fine grained such that users can be held accountable, i.e. uniquely identified. O.AUTH, O.MANAGE, O.SESSION all support the OSP by providing functionality that makes it possible to identify a specific user. If any of these objectives are compromised it may not be possible to hold a user accountable because it would effect the contents of the audit log, which it may not be possible to rely upon in such an event.[19]*

P.APPLICATION *The OSP is enforced by OE.APPLICATION which requires that the operational environment ensures that all the applications which the TOE communicates with runs on trusted machines with a trusted configuration. O.MANAGE provides the administrators with the ability to configure and manage the TOE such that this is fulfilled.[19]*

P.WORKFLOW *The OSP is directly enforced by O.WORKFLOW which ensures that managers are able to manage the workflows executed within the TOE.[19]*

P.FIPS140 *O.FIPS140 ensures in co-operation with OE.FIPS140 that the cryptographic functions used by the TOE are FIPS140-2 compliant.*

P.TRUST_CLIENT *The OSP is enforced by OE.TRUST_CLIENT which requires the operational environment to ensure that the Trusted Client Application is installed in a way that maintains the security of the TOE.*

P.USER_AUTH *The OSP is directly enforced by O.USER_AUTH.*

B.5 Security requirements

B.5.1 Security functional requirements

This section describes the security functional requirements(SFRs) chosen from CC part 2 [9] which addresses the security objectives to be met by the TOE. An overview of the SFRs required by the TOE are shown in Table B.3. Operations already performed in the SWFSPP have been marked bold. Assignments and selections performed in this ST have been marked in bold and italics. For refinements, italics is used for additions and strikeout for deletions.

Class	SFR	Description
FAU	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
FCS	**FCS_COP.1**	Cryptographic operation
FDP	FDP_ACC.1(1)	Subset access control (SWFS access SFP)
	FDP_ACC.1(2)	Subset access control (Workflow access SFP)
	FDP_ACF.1(1)	Security attribute based access control (SWFS access SFP)
	FDP_ACF.1(2)	Security attribute based access control (Workflow access SFP)
	FDP_IFC.1(1.1)	Subset information flow control (Limited application flow SFP)
	FDP_IFC.1(1.2)	Subset information flow control (Basic application flow SFP)

Table B.3: SFRs required by the TOE. SFRs in bold and italic are those which have been added compared to the SWFSPP (continued on next page).

Class	SFR	Description
	FDP_IFC.1(1.3)	Subset information flow control (Advanced application flow SFP)
	FDP_IFC.1(2)	Subset information flow control (Workflow flow SFP)
	FDP_IFF.1(1.1)	Simple security attributes (Limited application flow SFP)
	FDP_IFF.1(1.2)	Simple security attributes (Basic application flow SFP)
	FDP_IFF.1(1.3)	Simple security attributes (Advanced application flow SFP)
	FDP_IFF.2	Hierarchical security attributes (Workflow flow SFP)
	FDP_ETC.1	Export of user data without security attributes (Limited)
	FDP_ITC.1	Import of user data without security attributes (Limited)
	FDP_ETC.2	Export of user data with security attributes (Basic and Advanced)
	FDP_ITC.2	Import of user data with security attributes (Basic and Advanced)
	FDP_ITT.1	Basic internal transfer protection
	FDP_ITT.3	Integrity monitoring
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
FIA	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
FMT	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(1)	Management of security attributes (Administrator attributes)
	FMT_MSA.1(2)	Management of security attributes (Workflow attributes)
	FMT_MSA.1(3)	Management of security attributes (Active privileges)
	FMT_MSA.1(4)	Management of security attributes (Workflow flow SFP)
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (Audit logs)

Table B.3: SFRs required by the TOE. SFRs in bold and italic are those which have been added compared to the SWFSPP (continued on next page).

Class	SFR	Description
	FMT_MTD.1(2)	Management of TSF data (Audited events)
	FMT_MTD.1(3)	Management of TSF data (System)
	FMT_MTD.1(4)	Management of TSF data (Workflow Management)
	FMT_MTD.1(5)	Management of TSF data (Workflow instances)
	FMT_MTD.1(6)	Management of TSF data (Modification of instances)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FPT	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RCV.1	Manual recovery
	FPT_RCV.4	Function recovery
	FPT_TDC.1	Inter-TSF basic TSF data consistency
FTA	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.2	User-initiated locking
FTP	FTP_ITC.1	Inter TSF trusted channel
	FTP_ITC.1(2)	Inter TSF trusted channel (Client–Server)

Table B.3: SFRs required by the TOE. SFRs in bold and italic are those which have been added compared to the SWFSPP[19].

B.5.1.1 FAU Security audit

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 ***detailed*** level of audit; and
- ***no other 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, 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, ***no other audit relevant information***.

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **administrators** with the capability to read **any** audit information from the audit records.

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

***A*pplication note:** Information from the audit log which is relevant to managers or clients can be displayed to them by the use of a intermediary process, setup and controlled by an administrator. The process is to filter and process the audit log information in a secure manner such that only relevant information is displayed.

FAU_SAR.2 Restricted audit review

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

FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

B.5.1.2 FDP User data protection

FDP_ACC.1(1) Subset access control (SWFS access SFP)

FDP_ACC.1.1 The TSF shall enforce the **SWFS access SFP** on **all subjects, all SWFS controlled objects and all operations among them**.

FDP_ACC.1(2) Subset access control (Workflow access SFP)

FDP_ACC.1.1 The TSF shall enforce the **Workflow access SFP** on all subjects and objects referenced in a workflow instance's access SFP and all operations between these subjects and objects.

FDP_ACF.1(1) Security attribute based access control (SWFS access SFP)

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

- **user identity, user role, workflow groups, user history** and ***no additional security attributes*** associated with the subject
- **the static privileges held by the subject to the object**
- **the dynamic privileges held by the subject to the object**
- **the set of active privileges held by the subject to the object**

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

- **the subject has the required privilege for the requested operation on the object in its set of static or dynamic privileges and the privilege can be added to the set of active privileges**
- ***no additional rules***

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **the subject has the required privilege on the object in its set of active privileges**
- ***no additional rules***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on ~~the~~ ***no explicit denial rules***.

Application note: The refinement has been done for clarification.

FDP_ACF.1(2) Security attribute based access control (Workflow access SFP)

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

- **workflow groups, workflow roles, user history** and ***no additional security attributes*** associated with the subject
- **the static privileges held by the subject to the object**
- **the dynamic privileges held by the subject to the object**
- **the set of active privileges held by the subject to the object**

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

- **the subject has the required privilege for the requested operation on the object in its set of static or dynamic privileges and the privilege can be added to the set of active privileges**
- ***no additional rules***

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **the subject has the required privilege on the object in its set of active privileges**
- ***no additional rules***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on ~~the~~ ***no explicit denial rules***.

Application note: The refinement has been done for clarification.

FDP_IFC.1(1.1) Subset information flow control (Limited application flow SFP)

FDP_IFC.1.1 The TSF shall enforce the ***Limited application flow SFP*** on ***subjects which cause information to flow to and from user applications, invokable applications and SWFSs which are named in the SFP.***

FDP_IFC.1(1.2) Subset information flow control (Basic application flow SFP)

FDP_IFC.1.1 The TSF shall enforce the ***Basic application flow SFP*** on ***subjects which cause information to flow to and from user applications, invokable applications and SWFSs which are named in the SFP.***

FDP_IFC.1(1.3) Subset information flow control (Advanced application flow SFP)

FDP_IFC.1.1 The TSF shall enforce the ***Advanced application flow SFP*** on ***subjects which cause information to flow to and from user applications, invokable applications and SWFSs which are named in the SFP and the Trusted Client Application.***

FDP_IFC.1(2) Subset information flow control (Workflow flow SFP)

FDP_IFC.1.1 The TSF shall enforce the **Workflow flow SFP** on **all subjects and objects referenced in a workflow instance's information flow control SFP and all operations among subjects and objects covered by the SFP**.

FDP_IFF.1(1.1) Simple security attributes (Limited application flow SFP)

FDP_IFF.1.1 The TSF shall enforce the ***Limited application flow SFP*** based on the following types of subject and information security attributes:

- ***the applications named in the SFP***
- ***the applications authentication credentials***
- ***the sensitivity label of the object containing the information***

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:

- ***if the sensitivity label of the object containing the information is public***

FDP_IFF.1.3 The TSF shall enforce ~~the~~ ***no additional information flow control SFP rules***.

Application note: The refinement has been done for clarification.

FDP_IFF.1.4 The TSF shall provide the following ***list of additional SFP capabilities: none***.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***none***.

FDP_IFF.1(1.2) Simple security attributes (Basic application flow SFP)

FDP_IFF.1.1 The TSF shall enforce the ***Basic application flow SFP*** based on the following types of subject and information security attributes:

- ***the applications named in the SFP***
- ***the applications authentication credentials***
- ***the sensitivity label of the object containing the information***

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:

- all operations:
  - ***the application is CC certified or according to a comparable standard***
- ***operation: exporting information to an invoked application***.
  - ***if the sensitivity label of the object containing the information is public***

FDP_IFF.1.3 The TSF shall enforce ~~the~~ ***no additional information flow control SFP rules***.

Application note: The refinement has been done for clarification.

FDP_IFF.1.4 The TSF shall provide the following ***list of additional SFP capabilities: none***.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***none***.

FDP_IFF.1(1.2) Simple security attributes (Advanced application flow SFP)

FDP_IFF.1.1 The TSF shall enforce the ***Advanced application flow SFP*** based on the following types of subject and information security attributes:

- ***the applications named in the SFP***
- ***the applications authentication credentials***

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:

- ***all operations:***
  - ***the application is CC certified or certified according to a comparable standard***
  - ***the application is capable of enforcing the information flow rules of the Workflow flow SFP***

FDP_IFF.1.3 The TSF shall enforce ~~the~~ ***no additional information flow control SFP rules***.

Application note: The refinement has been done for clarification.

FDP_IFF.1.4 The TSF shall provide the following ***list of additional SFP capabilities: none***.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***none***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***none***.

FDP_IFF.2 Hierarchical security attributes (Workflow flow SFP)

FDP_IFF.2.1 The TSF shall enforce the **Workflow flow SFP** based on the following types of subject and information security attributes:

- **the workflow groups and the workflow roles associated with the subject**
- ***the sensitivity label of the object containing the information***

Application note: The sensitivity label shall specify whether the object has the hierarchical level of either private or public. If the level is private the set of one or more workflow groups must be specified in which the information contained in the object must be kept private.

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold:

- ***If information cannot flow from subject S to an object with less sensitivity than object O; then the flow of information from object O to subject S is permitted. (read operation)***
- ***If information cannot flow from an object with greater sensitivity than object O to subject S; then the flow of information from subject S to object O is permitted. (write operation)***

FDP_IFF.2.3 The TSF shall enforce ~~the~~ ***no additional information flow control SFP rules***.

Application note: The refinement has been done for clarification.

FDP_IFF.2.4 The TSF shall provide the following ***list of additional SFP capabilities: none***.

FDP_IFF.2.5 The TSF shall explicitly authorise an information flow based on the following rules: ***none***

FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: ***none***

FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes:

- There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
- There exists a 'least upper bound' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
- There exists a 'greatest lower bound' in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

Application note: The ordering of sensitivity labels is described in Application data protection in section B.1.3.2.

FDP_ITC.1 Import of user data without security attributes (Limited)

FDP_ITC.1.1 The TSF shall enforce the Workflow flow SFP and ***the limited application SFP*** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***the application must be covered by the SFP***.

FDP_ITC.2 Import of user data with security attributes (Basic and Advanced)

FDP_ITC.2.1 The TSF shall enforce the Workflow flow SFP and ***the basic or Advanced application flow 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: ***the application must be covered by the SFP***.

FDP_ETC.1 Export of user data without security attributes (Limited)

FDP_ETC.1.1 The TSF shall enforce the Workflow flow SFP and ***the Limited application flow SFP*** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

FDP_ETC.2 Export of user data with security attributes (Basic and Advanced)

FDP_ETC.2.1 The TSF shall enforce the Workflow flow SFP and ***the Basic application flow SFP or Advanced application flow SFP*** 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: ***the application must be covered by the SFP***.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the ***Advanced application flow SFP*** to prevent the ***disclosure, modification*** of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.3 Integrity monitoring

FDP_ITT.3.1 The TSF shall enforce the ***Advanced application flow SFP*** to monitor user data transmitted between physically-separated parts of the TOE for the following errors: ***cryptographic integrity errors***

FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall ***try to resend the data up to a configurable number of times and alert the administrator***.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the ***application flow SFPs*** to be able to ***transmit and receive*** objects in a manner protected from unauthorised disclosure.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **application flow SFP(s)** to be able to ***transmit and receive*** user data in a manner protected from **modification, insertion and replay errors**.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether **modification, insertion and replay** has occurred.

B.5.1.3 FIA Identification and authentication

FIA_ATD.1 User attribute definition

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

- **user authentication credentials**
- **user role**
- **user history**
- **workflow groups**
- **workflow roles**
- **static privileges**
- **dynamic privileges**
- ***no additional security attributes***

***A*pplication note:** Each workflow role which belongs to the user must be associated with a workflow group which the user belongs to.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ~~secrets~~ *passwords* meet ***the administrator defined password policy***.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide ***mutual authentication mechanisms*** to support user authentication.

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

- ***Workflow System Application authentication:***
  - ***verify X.509 certificate and proof of possession of corresponding private key***
- ***user authentication:***
  - ***verify username and password or alternatively verify token and token PIN for users which are assigned to the client role***
  - ***verify token and token PIN for users assigned to the administrator or manager role.***

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions:

- **The session has been locked or terminated.**
- ***no additional conditions.***

FIA_UAU.7 Protected authentication feedback

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

***A*pplication note:** Obscured feedback implies the TSF does not produce a visible display of any authentication data. It is acceptable though that some form of feedback is sent. E.g. when a user enters a password each character is replaced with a '*'.

FIA_UID.2 User identification before any action

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

FIA_USB.1 User-subject binding

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

- **user authentication credentials**
- **user role**
- **user history**
- **workflow groups**
- **workflow roles**
- **static privileges**
- **dynamic privileges**
- ***no additional security attributes***

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***none***.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***none***.

B.5.1.4 FMT Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***modify the behaviour of*** the functions

- **implementing the user identification and authentication mechanisms**
- **implementing the association between TOE roles and individual users**
- **controlling the behaviour of the audit generation**
- **implementing the SWFS access SFP**
- **implementing the Workflow access SFP**
- **implementing the application flow SFPs**
- **implementing the Workflow flow SFP**
- **implementing the TOE backup and recovery routines**
- **implementing the session locking methods**

- ***controlling the cryptographic functions used***
- ***defining the password policy***

to **administrators**.

FMT_MSA.1(1) Management of security attributes (Administrator attributes)

FMT_MSA.1.1 The TSF shall enforce the **SWFS access SFP** to restrict the ability to **modify** the security attributes **user identity, user role, user history, static privileges *and no additional attributes*** to **administrators**.

FMT_MSA.1(2) Management of security attributes (Workflow attributes)

FMT_MSA.1.1 The TSF shall enforce the **Workflow access SFP** to restrict the ability to **modify** the security attributes **workflow group, workflow role *and no additional attributes*** to **managers**.

FMT_MSA.1(3) Management of security attributes (Active privileges)

FMT_MSA.1.1 The TSF shall enforce the **SWFS access SFP and Workflow access SFP** to restrict the ability to **modify** the security attributes:

- **set of active privileges**
- ***and no additional attributes***

to **the client who owns the session**.

FMT_MSA.1(4) Management of security attributes (Workflow flow SFP)

FMT_MSA.1.1 The TSF shall enforce the ***Workflow flow SFP*** to restrict the ability to ***modify*** the security attributes:

- ***sensitivity label***

to ***those who are authorised by the workflow instance's flow SFP***.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **SWFS access SFP, Workflow access SFP, Workflow flow SFP,** ***limited, basic and Advanced application flow SFP*** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **administrators** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) Management of TSF data (Audit logs)

FMT_MTD.1.1 The TSF shall restrict the ability to ***create, move and delete*** the

- **audit logs**

to **administrators**.

FMT_MTD.1(2) Management of TSF data (Audited events)

FMT_MTD.1.1 The TSF shall restrict the ability to ***query and modify*** the

- **set of audited events**

to **administrators**.

FMT_MTD.1(3) Management of TSF data (System)

FMT_MTD.1.1 The TSF shall restrict the ability to ***initialize and modify*** the

- **SFWS access control SFP**
- **application flow SFP(s)**
- **Workflow access SFP**
- **Workflow flow SFP**

- **identification and authentication data**
- **mapping of authorised users to roles**
- ***password policy***

to **administrators**.

FMT_MTD.1(4) Management of TSF data (Workflow management)

FMT_MTD.1.1 The TSF shall restrict the ability to ***create, modify and delete*** the

- **process definitions**
- ***no additional workflow related TSF data***

to **managers**.

FMT_MTD.1(5) Management of TSF data (Workflow instances)

FMT_MTD.1.1 The TSF shall restrict the ability to ***create, suspend, terminate, monitor and delete*** the

- ***workflow instances***

to **managers** ***and users which have been explicitly authorised to do so for a specific set of workflow instances***.

FMT_MTD.1(6) Management of TSF data (Modification of instances)

FMT_MTD.1.1 The TSF shall restrict the ability to ***modify*** the

- ***workflow instances***

to ***managers***.

FMT_SMF.1 Specification of management functions

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

- **Functions to assign and maintain lists of authorised users**
- **Functions to manage object security attributes**
- **Functions to manage user security attributes**

- **Functions to manage and review the audit data.**
- **Functions to manage the SFWS access SFP**
- **Functions to manage the Workflow access SFP**
- **Functions to create and manage the application flow SFP(s)**
- **Functions to manage the Workflow flow SFP**
- **Functions to manage process definitions and workflow instances**
- **Functions to monitor workflow instances**
- **Function to create and recover backups.**
- **Functions to manage the session locking methods.**
- ***Functions to control the cryptographic functions used***
- ***Functions to manage the password policy***

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **Client**
- **Manager**
- **Administrator**
- ***and no additional roles***

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

B.5.1.5 FPT Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- ***system failures***
- ***semantic failures***

***A*pplication note:** System failures includes failures in the underlying infrastructure such as the OS or hardware and failures of TOE components. Semantic failures are failures which are associated with the execution of workflow tasks e.g. unavailability of resources or internal decisions.[14]

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

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 a remote trusted IT product within the following metric: ***the integrity is protected using digital signatures or MACs which are generated using FIPS140-2 compliant algorithms***.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform ***request of re-transmission and audit the failure*** if modifications are detected.

FPT_ITT.1 Basic internal TSF data transfer protection

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

FPT_RCV.1 Manual recovery

FPT_RCV.1.1 After ***system failure*** the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

***A*pplication note:** System failures includes failures in the underlying infrastructure such as the OS or hardware and failures of TOE components.

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that ***if a system failure occurs backup and recovery functions*** have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret ***the sensitivity label of an object*** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use ***the following interpretation rules*** when interpreting the TSF data from another trusted IT product*:*

- the sensitivity label shall be valid in relation to the partial ordering of sensitivity labels is described in section B.1.3.2 and;
- if the sensitivity label is invalid it shall be interpreted as being public and changed to public.

B.5.1.6 FTA TOE access

FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after ***an administrator specified time interval of user inactivity, which may be dependent on the authentication mechanism used*** by:

- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

Application note: The time interval of user inactivity should be defined with respect to the implementation of the user-initiated locking (FTA_SSL.2). E.g. if the user-initiated locking is activated by the removal of a physical token, e.g. a smart card or a USB key, the time interval of user inactivity may be set to a very high value.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: **Re-authentication of the user.**

FTA_SSL.2 User-initiated locking

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

- clearing or overwriting display devices, making the current contents unreadable;

- disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: **Re-authentication of the user**.

B.5.1.7 FTP Trusted path/channels

FTP_ITC.1 Inter TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote 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 and SWFSs*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- **establishing a connection with a SWFS, which it wishes to exchange information with**
- **establishing a connection with a trusted applications which it wishes to invoke**
- ***no additional functions***

FTP_ITC.1(2) Inter TSF trusted channel (Client–Server)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself ~~self~~ *the Trusted Client Application* and ~~a remote trusted IT product~~ *the Workflow System Application* 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 Trusted Client Application*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- ***performing mutual authentication between the Trusted Client Application and the Workflow System Application before any communication is allowed.***

B.5.1.8 FCS Cryptographic support

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform ***encryption of the TOE data flows and mutual authentication between the Trusted Client Application and the Workflow System Application*** in accordance with a ~~specified cryptographic algorithm~~ *one of the following TLS cipher suites:*

- ***TLS_RSA_WITH_AES_128_CBC_SHA, or***
- ***TLS_RSA_WITH_AES_256_CBC_SHA.***

and cryptographic key sizes ***128 or 256 bit for AES, and a minimum of 1024 bit for RSA*** that meet the following: ***FIPS140-2***.

***A*pplication note:** The refinement has been done for clarification. The TLS ciphersuites are described in [16] and [15].

B.5.2 Security assurance requirements

The security assurance requirements are those of the SWFSPP[19] with no augmentations. The assurance level to which the TOE of this ST is to be evaluated is evaluation level 3 augmented (EAL3+) from part 3 of CC[10]. EAL3 has been augmented with the assurance requirement ALC_CMS.4. The assurance requirements are listed in table B.4.

B.5.2.1 ADV_ARC.1 Security architecture description

Developer action elements

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements

Assurance class	Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table B.4: Assurance Requirements

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.2 ADV_FSP.3 Functional specification with complete summary

Developer action elements

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the non-SFR-enforcing actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

B.5.2.3 ADV_TDS.2 Architectural design

Developer action elements

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the non-SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements

ADV_TDS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

B.5.2.4 AGD_OPE.1 Operational user guidance

Developer action elements

AGD_OPE.1.1D The developer shall provide the design of the TOE. available in the TOE design.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.5 AGD_PRE.1 Preparative procedures

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

B.5.2.6 ALC_CMC.3 Authorisation controls

Developer action elements

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

Content and presentation elements

ALC_CMC.3.1C The TOE shall be labeled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements

ALC_CMC.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.7 ALC_CMS.4 Problem tracking CM coverage

Developer action elements

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.8 ALC_DEL.1 Delivery procedures

Developer action elements

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.9 ALC_LCD.1 Developer defined life-cycle model

Developer action elements

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.10 ALC_DVS.1 Identification of security measures

Developer action elements

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

B.5.2.11 ATE_COV.2 Analysis of coverage

Developer action elements

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.12 ATE_DPT.1 Testing: basic design

Developer action elements

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.13 ATE_FUN.1 Functional testing

Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

B.5.2.14 ATE_IND.2 Independent testing - sample

Developer action elements

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF interfaces to confirm that the TSF operates as specified.

B.5.2.15 AVA_VAN.2 Vulnerability analysis

Developer action elements

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

B.5.3 Security requirements rationale

This section gives the rationales to why the ST security objectives are satisfied by the TOE security requirements, which have been traced to them and that all dependencies have been fulfilled.

B.5.3.1 SFR rationale

Table B.5 shows the tracing between security objectives and SFRs. Table B.6 gives all the dependencies on the SFRs and shows that they all are fulfilled.

O.AUTH The components FIA_UID.2 and FIA_UAU.2 ensures that users are required to authenticate themselves before any action in the TOE is allowed by the TSF. FIA_UAU.7 ensures that the feedback given to the user during authentication is limited such that the TSF authentication mechanism is more robust against attacks.[19]

O.ACCESS The components FDP_ACC.1(1) and FDP_ACF.1(1) ensures that a SWFS access SFP is specified and enforced for all TOE application data. FDP_ACC.1(2) and FDP_ACF.1(2) ensures that a Workflow access SFP is specified which enforces the workflow instances' access SFPs. FIA_ATD.1 provides the TSF with information about users needed to enforce the TSP. FIA_USB.1 supports the objective by binding the user security attributes to subjects acting on their behalf.[19]

O.FLOW The components FDP_IFC.1(1-3) and FDP_IFF.1(1-3) ensures that a information flow control SFP is specified and enforced for all user applications, invokable applications and SFWSs which the TOE can interact with.[19]

FDP_IFC.1(2) and FDP_IFF.1(2) ensures that a Workflow flow SFP is specified which enforces the workflow instances' flow SFPs. FIA_ATD.1 provides the TSF

with information about users which is needed to enforce the TSP. FIA_USB.1 supports the objective by binding the user security attributes to subjects acting on their behalf.[19]

O.MANAGE The components FMT_MOF.1, FMT_MSA.1(1-2), FMT_MSA.2, FMT_MTD.1(1-3) and FMT_SMR.1 ensures that administrators are able to manage the security functions, security attributes and relevant TSF data. FMT_SMF.1 provides the security functions required for the managing.[19]

FMT_MSA.3 ensures that the TSF provides default values for the relevant security attributes.[19]

O.WORKFLOW The components FMT_MSA.1(2), FMT_MTD.1(4-6) and FMT_SMR.1 ensures that managers are able to manage the security functions, security attributes and relevant TSF data of workflows. FMT_SMF.1 provides the security functions required for the managing.[19]

FMT_MSA.2 and FMT_MSA.3 supports this by ensuring that the values for the security attributes are secure and ensures that the TSF provides default values for the relevant security attributes, respectively.[19]

O.AUDIT The component FAU_GEN.1 ensures that auditable events are identified and audited. FAU_GEN.2 ensure that the audit records can be traced to individual users such that they are held accountable. FAU_SAR.1 and FAU_SAR.2 ensure that audit data can be reviewed only by administrators and users who have been granted explicit read access. FAU_STG.1 prevents unauthorised deletion and modification of the audit records.[19]

O.DATAFLOW FDP_ITC.2 and FDP_ETC.2 ensures that when application data is imported from and exported to invoked applications and SWFS outside of the TOE both the application flow control SFPs and the Workflow flow SFP are enforced. Furthermore the security attributes associated with the application data is used.
FPT_TDC.1 ensures that that a consistent interpretation of the sensitivity labels exists between the TOE, the invoked applications and the SWFSs.[19]

FDP_UIT.1 ensures that the integrity of all application data transmitted from the TOE can be checked and that the integrity of all application data upon TOE receipt is verified. FPT_ITI.1 ensures the same for all TSF data transmitted between the TOE and any trusted application.[19]

FDP_ITT.1 and FTP_ITT.1 ensures that the integrity of application data (user

data) and TSF data transmitted between the Workflow System Application and the Trusted Client Application is protected. FTP_ITT.3 ensures monitoring of integrity and actions in case of detection of errors.

O.RECOVER The component FPT_RCV.1 ensures that the TSF enters a maintenance mode in the event of a failure, from where it can return to a secure state. E.g. if data is corrupted or lost an administrator can by the use of a backup restore the data such that the TSF can return to its normal and secure operation. FPT_RCV.4 ensures that the TSF provides additional protection in the event of a failure by ensuring that certain functions either completes successfully or recovers to a consistent and secure state. FPT_FLS.1 ensures that the TSF in the event of a failure will preserve a secure state where all SFRs are enforced.

The components FMT_SMF.1 provides the functions for managing the backup and recovery mechanisms, while FMT_MOF.1 restricts their use to the administrators.

O.SESSION FTA_SSL.1 and FTA_SSL.2 ensures that the TSF allows TSF-initiated session locking after an administrator specified time of user inactivity and user-initiated session locking, respectively. FIA_UAU.6 ensures that the user is re-authenticated when the session has been locked before re-gaining access to the TOE.

O.TRUSTED FTP_ITC.1 ensures that the applications which the TOE can invoke and/or the SWFSs which the TOE can communicate with provide a communication channel which is logical distinct from other communication channels. It is hereby ensured that a assured identification of the channels end points exists and that the channel data is protected. [19]

O.AUTH_CLIENT The component FTP_ITC.1(2) ensures that the Workflow System Application and the Trusted Client Application mutually authenticate using a trusted channel before allowing any communication. FCS_COP.1 ensures that cryptographic functions which are FIPS140-2 compliant are used for the authentication.

O.AUTHENTIC This objective is met by FIA_UAU.5 which requires that during user authentication the Workflow System Application must authenticate itself to the user.

O.FIPS140 FCS_COP.1 ensures that the cryptographic functions used are FIPS140-2 compliant.

O.SECRET_FLOW FDP_UCT.1 and FPT_ITC.1 ensures that both application data and TSF data sent to and received from user applications, invokable applications and SWFSs is protected from unauthorised disclosure. FPT_ITI.1 ensures the same for all TSF data transmitted between the TOE and trusted SWFSs. Finally FDP_ITT.1 ensures that information sent to and received from the Trusted Client Application is protected from unauthorised disclosure.

FCS_COP.1 ensures that the cryptographic functions used for protecting the information are FIPS140-2 compliant.

O.USER_AUTH The component FIA_UAU.5 ensures that the required authentication mechanisms are provided and that username and password authentication is restricted to users in the client role.

FIA_SOS.1 ensures that when passwords are used for authentication they comply to the password policy rules, which ensures that 'strong' passwords are used.

	O.AUTH	O.ACCESS	O.FLOW	O.MANAGE	O.WORKFLOW	O.AUDIT	O.DATAFLOW	O.RECOVER	O.SESSION	O.TRUSTED	O.AUTH_CLIENT	O.AUTHENTIC	O.FIPS140	O.SECRET_FLOW	O.USER_AUTH
FAU_GEN.1						x									
FAU_GEN.2						x									
FAU_SAR.1						x									
FAU_SAR.2						x									
FAU_STG.1						x									
FCS_COP.1											x		x	x	
FDP_ACC.1(1)		x													
FDP_ACC.1(2)		x													
FDP_ACF.1(1)		x													
FDP_ACF.1(2)		x													
FDP_IFC.1(1.1)			x												
FDP_IFC.1(1.2)			x												
FDP_IFC.1(1.3)			x												
FDP_IFC.1(2)			x												
FDP_IFF.1(1.1)			x												

Table B.5: Tracing of TOE security objectives to SFRs. SFRs in bold and italic are those which have been added compared to the SWFSPP[19] (continued on next page).

	O.AUTH	O.ACCESS	O.FLOW	O.MANAGE	O.WORKFLOW	O.AUDIT	O.DATAFLOW	O.RECOVER	O.SESSION	O.TRUSTED	O.AUTH_CLIENT	O.AUTHENTIC	O.FIPS140	O.SECRET_FLOW	O.USER_AUTH
FDP_IFF.1(1.2)			x												
FDP_IFF.1(1.3)			x												
FDP_IFF.2			x												
FDP_ETC.1							x								
FDP_ETC.2							x								
FDP_ITC.1							x								
FDP_ITC.2							x								
FDP_ITT.1							x							x	
FDP_ITT.3							x								
FDP_UCT.1														x	
FDP_UIT.1							x								
FIA_ATD.1		x	x												
FIA_SOS.1															x
FIA_UAU.2	x														
FIA_UAU.5												x			x
FIA_UAU.6									x						
FIA_UAU.7	x														
FIA_UID.2	x														
FIA_USB.1		x	x												
FMT_MOF.1				x				x							
FMT_MSA.1(1)				x											
FMT_MSA.1(2)				x	x										
FMT_MSA.1(3)															
FMT_MSA.1(4)					x										
FMT_MSA.2				x	x										
FMT_MSA.3				x	x										
FMT_MTD.1(1)				x											
FMT_MTD.1(2)				x											
FMT_MTD.1(3)				x											
FMT_MTD.1(4)					x										
FMT_MTD.1(5)					x										
FMT_MTD.1(6)					x										
FMT_SMF.1				x	x			x							
FMT_SMR.1				x	x										

Table B.5: Tracing of TOE security objectives to SFRs. SFRs in bold and italic are those which have been added compared to the SWFSPP[19] (continued on next page).

	O.AUTH	O.ACCESS	O.FLOW	O.MANAGE	O.WORKFLOW	O.AUDIT	O.DATAFLOW	O.RECOVER	O.SESSION	O.TRUSTED	O.AUTH_CLIENT	O.AUTHENTIC	O.FIPS140	O.SECRET_FLOW	O.USER_AUTH
FPT_FLS.1								x							
FPT_ITC.1														x	
FPT_ITI.1							x								
FPT_ITT.1							x								
FPT_RCV.1								x							
FPT_RCV.4								x							
FPT_TDC.1							x								
FTA_SSL.1									x						
FTA_SSL.2									x						
FTP_ITC.1										x					
FTP_ITC.1(2)											x				

Table B.5: Tracing of TOE security objectives to SFRs. SFRs in bold and italic are those which have been added compared to the SWFSPP[19]

SFR	**Dependency**	**Resolved**
FAU_GEN.1	FPT_STM.1	The dependency has not been resolved, since the underlying OS will provide the reliable clock as described in OE.TIME.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	 by FIA_UID.2 which is hierarchical
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	
FAU_STG.1	FAU_GEN.1	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 FCS_CKM.4	by FDP_ITC.1 and FDP_ITC.2 The dependency has not been resolved, since the underlying OS provides the cryptographic service provider.

Table B.6: continued on next page

SFR	Dependency	Resolved
	FMT_MSA.2	
FDP_ACC.1(1)	FDP_ACF.1	by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	by FDP_ACC.1(1)
FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	by FDP_ACC.1(2)
FDP_IFC.1(1.1)	FDP_IFF.1	FDP_IFF.1(1.1)
FDP_IFC.1(1.2)	FDP_IFF.1	FDP_IFF.1(1.2)
FDP_IFC.1(1.3)	FDP_IFF.1	FDP_IFF.1(1.3)
FDP_IFC.1(2)	FDP_IFF.1	by FDP_IFF.1(2)
FDP_IFF.1(1.1)	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1.1)
FDP_IFF.1(1.2)	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1.2)
FDP_IFF.1(1.3)	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1.3)
FDP_IFF.2	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1)
FDP_ETC.1	FDP_IFC.1	by FDP_IFC.1(1.1) and FDP_IFC.1(2)
FDP_ETC.2	FDP_IFC.1	by FDP_IFC.1(1.2-3) and FDP_IFC.1(2)
FDP_ITC.1	FDP_IFC.1 FMT_MSA.3	by FDP_IFC.1(1.1-2) and FDP_IFC.1(2)
FDP_ITC.2	FDP_IFC.1 FTP_ITC.1 FPT_TDC.1	by FDP_IFC.1(1.3) and FDP_IFC.1(2)
FDP_ITT.1	FDP_IFC.1 FTP_ITC.1	by FDP_IFC(1.3)
FDP_ITT.3	FDP_IFC.1 FDP_ITT.1	by FDP_IFC(1.3)
FDP_UCT.1	FDP_IFC.1 FTP_ITC.1	by FDP_IFC(1.1-3)
FDP_UIT.1	FDP_IFC.1 FTP_ITC.1	by FDP_IFC(1.1-3)
FIA_ATD.1	None	
FIA_SOS.1	None	

Table B.6: continued on next page

SFR	Dependency	Resolved
FIA_UAU.2	FIA_UID.1	by FIA_UID.2 which is hierarchical
FIA_UAU.5	None	
FIA_UAU.6	None	
FIA_UAU.7	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FIA_UID.2	None	
FIA_USB.1	FIA_ATD.1	
FMT_MOF.1	FMT_SMR.1	
	FMT_SMF.1	
FMT_MSA.1(1)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1) and FDP_ACC.1(2)
FMT_MSA.1(2)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1)
FMT_MSA.1(3)	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	by FDP_ACC.1(1) and FDP_ACC.1(2)
FMT_MSA.1(4)	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	by FDP_IFC.1(2)
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	by FDP_ACC.1(1-2) and FDP_IFC.1(1-2)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	by FMT_MSA.1(1-3)
FMT_MTD.1(1-6)	FMT_SMR.1 FMT_SMF.1	
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	by FIA_UID.2 which is hierarchical
FPT_ITC.1	None	
FPT_ITT.1	None	
FPT_FLS.1	None	
FPT_ITC.1	None	
FPT_ITI.1	None	
FPT_RCV.1	AGD_OPE.1	

Table B.6: continued on next page

SFR	Dependency	Resolved
FPT_RCV.4	None	
FPT_TDC.1	None	
FTA_SSL.1	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FTA_SSL.2	FIA_UAU.1	by FIA_UAU.2 which is hierarchical
FTP_ITC.1	None	
FTP_ITC.1(2)	None	

Table B.6: Dependencies of SFRs. If the 'resolved' column is empty the dependency is directly fulfilled by the inclusion of the dependent SFR in the ST.

B.5.3.2 SAR Rationale

The evaluation assurance level of EAL3+ is unchanged compared to the SWFSPP [19]. As described in the SWFSPP[19]:

> ...EAL3 gives a moderate level of independently assured security. EAL3 has been chosen over EAL2 because it requires more complete testing coverage of the security functionality and mechanisms/procedures which ensure a higher level of security in the development environment. The augmented assurance required provides added assurance that flaws are tracked and resolved during development.

B.6 TOE summary specification

This section describes the general mechanisms that the TOE uses for satisfying the SFRs. Table B.7 shows the SFRs which are satisfied by the different TOE security functions.

Security functions	SFRs
Security audit	
Audit generation and recording	FAU_GEN.1, FAU_GEN.2
Audit review	FAU_SAR.1, FAU_SAR.2
Audit protection	FAU_STG.1
Cryptographic support	FCS_COP.1
Protection of data	

Table B.7: Mapping of the security functions to SFRs (continued on next page).

Security functions	**SFRs**
Access control	FDP_ACC.1(1), FDP_ACC.1(2) FDP_ACF.1(1), FDP_ACF.1(2)
Information flow control	FDP_IFC.1(1.1), FDP_IFC.1(1.2) FDP_IFC.1(1.3), FDP_IFC.1(2) FDP_IFF.1(1.1), FDP_IFF.1(1.2) FDP_IFF.1(1.3), FDP_IFF.1(2)
Backup and recovery	FPT_FLS.1, FPT_RCV.1 FPT_RCV.4
Identification and authentication	
User attributes	FIA_ATD.1, FIA_USB.1
Mutual authentication	FIA_SOS.1, FIA_UID.2 FIA_UAU.2, FIA_UAU.5
Session locking and re-authentication	FIA_UAU.6, FTA_SSL.1 FTA_SSL.2
Protected authentication feedback	FIA_UAU.7
Security Management	
Security Roles	FMT_SMR.1
Administrative interface	FMT_MOF.1, FMT_MSA.1(1) FMT_SMF.1, FMT_MSA.2 FMT_MSA.3, FMT_MTD.1(1) FMT_MTD.1(2), FMT_MTD.1(3)
Workflow management interface	FMT_MSA.1(2), FMT_MSA.1(4) FMT_MTD.1(4), FMT_MTD.1(5) FMT_MTD.1(6)
Client interface	FMT_MSA.1(3)
Secure communication	
User applications	FDP_UCT.1, FDP_UIT.1
Trusted external applications	FCS_COP.1, FPT_ITI.1 FPT_ITC.1
Trusted Client Application	FCS_COP.1, FDP_ITT.1 FDP_ITT.3, FPT_ITT.1 FTP_ITC.1(2)
Importation and exportation	FDP_ETC.1, FDP_ITC.1 FDP_ETC.2, FDP_ITC.2 FPT_TDC.1

Table B.7: Mapping of the security functions to SFRs.

B.6.1 Security audit

B.6.1.1 Audit generation and recording

The audit functions records all security relevant events and stores them in an audit log. For each audited event the following information is recorded:

- Date and time of the event
- Type of event
- Subject identity
- Outcome (success or failure)
- Identity of the user that caused the event

The date and time of an event is provided by the underlying OS which provides a reliable clock, which is synchronized with a hardware clock which keeps a reliable time.

The audit functions shall record the events of the detailed level of audit as specified in CC Part 2[9]. This includes, but is not limited to:

- use of the identification and authentication mechanisms
- use of data exchange mechanisms such as invocation of an application
- locking or unlocking of a user session
- failures or service discontinues

In relation to management the use of administrative management functions as well as workflow management functions shall be recorded.

B.6.1.2 Audit review

The Workflow System Application provides audit review for authorised administrators though the administrative interface. The audit functions ensure that the TSF is capable of providing the audit records from the audit log in a suitable manner which allows administrators to easily interpret and process the information.

The audit functions prohibit all users as default to read audit records. Administrators may however grant users read-access to audit records.

B.6.1.3 Audit protection

Through cryptographic protection the audit functions ensure that the audit log is protected from unauthorised modifications. The audit log is stored in easily identifiable files on the OS file system.

B.6.2 Cryptographic support

The cryptographic support is provided in co-operation with the underlying OS. The TSF is configured to make use of encryption services that meet the FIPS140-2 standard and ensures that such services are used.

B.6.3 Protection of data

B.6.3.1 Access control

Access control is provided by the access control function which consists of a decision function and an enforcement function. The decision function decides upon whether an operation should be allowed or rejected based upon the access control SFPs of the Workflow System Application. The enforcement function enforces the decisions of the decision function.

The Workflow System Application implements two access control SFPs; the SWFS access SFP(FDP_ACC.1(1)) and the Workflow access SFP(FDP_ACC.1(2)). Both SFPs are applicable to the entire system and manged by administrators. The SWFS access SFP contains rules which are to be enforced globally across all workflow instances. Each workflow instance has an associated access SFP which specifies the access control rules within the instance. The workflow instance's access SFP is an instantiation of the process access SFP which is defined and manged by a manager [19]. The Workflow access SFP ensures that the workflow instance access SFPs are enforced.

Besides defining the assignment of access control privileges to clients the SFPs can be used to define constraints e.g. separation of duty or binding of duty.

Access privileges are divided into two types as defined in SWFSPP; static privileges and dynamic privileges. Static privileges are privileges which are directly assigned to the client. Dynamic privileges are acquired by a client as a result of an active binding e.g. when a user accepts to execute a workitem from the user's worklist the privileges required for executing the associated task are acquired by the client. Dynamic privileges may be associated with workflow roles, groups or tasks and may be acquired as a result of the following actions:

- a client activates workflow role

- a client activates workflow group by activating workflow role
- a client accepts to execute a workitem from the client's worklist

A client cannot use an acquired privilege before it has been activated by being added to the client's set of active privileges. The rules of the access control SFPs control whether activation is granted or denied. An activation function automatically controls the activation and deactivation of client privileges.

B.6.3.2 Information flow control

The two types of information flow control supported by the TOE are object to object and between the Workflow System Application and external applications. The information flow rules between objects are defined in the Workflow flow SFP(FDP_IFC.1(2)). To enforce the object to object information flow control objects are associated with a sensitivity label as described in the Application data protection paragraph of section B.1.3.2.

The information flow rules between the Workflow System Application and external applications are defined in the application flow SFPs. The Workflow System Application supports three application flow policies, a Basic(FDP_IFC.1(1.1)), a Limited(FDP_IFC.1(1.2)) and an Advanced(FDP_IFC.1(1.3)) application flow SFP. Each increases the level of trust in the application. All applications which the Workflow System Application communicates must be covered by an application flow SFP.

B.6.3.3 Backup and recovery

The TOE provides backup and recovery functions to ensure that it can recover to a secure state after system failures which cause the TSF to enter an insecure state. A secure state is a state where all SFPs are enforced, TSF and user data is consistent and the TOE is fully operational.

B.6.4 Identification and authentication

B.6.4.1 User attributes

Each user is associated with the following set of user security attributes:

- user authentication credentials
- user role

- user history
- workflow groups
- workflow roles
- static privileges
- dynamic privileges

Each workflow role which belongs to the user must be associated with a workflow group which the user belongs to. The user authentication credentials, user role and user history attributes are applicable to users in any role. The workflow groups attribute is only applicable to managers and clients. With respect to managers it denotes which workflow groups and thereby workflow instances a manager is responsible for and may manage. With respect to clients it denotes that a client is assigned to one or more workflow roles which are part of the workflow group. The remaining attributes are only applicable to clients. The workflow roles attribute describes the set of workflow roles the client possess. The static and dynamic privileges attributes constitute the privileges the client may activate (see B.6.3.1).

Subjects which act on the behalf of a user are associated with the user's user security attributes.

B.6.4.2 Mutual authentication

Users must be identified and perform mutual authentication with the Workflow System Application before they are allowed to perform any security-relevant actions. The TSF supports authentication using one of the following mechanisms:

- workflow system authentication
  - X.509 certificate and proof of possession of corresponding private key
- user authentication
  - verify username and password or alternatively verify token and token PIN for users which are assigned to the client role
  - verify token and token PIN for users assigned to the administrator or manager role

If the authentication data can be verified the user is permitted access to the TOE. Once authenticated the TOE associates the user identity and the corresponding user attributes.

Passwords must be stored hashed and not in clear-text. The hash algorithm used should by FIPS 180-2[4] compliant. The administrator may specify the following restrictions on passwords in a password policy:

- Permitted characters
- Password structure (e.g. requirement upon a minimum of special characters)
- Minimum length
- Maximum lifetime
- Number passwords from the user password history, which are disallowed as a new password

B.6.4.3 Session locking and re-authentication

A session may be locked on the request of the user or automatically by the TSF. The TSF shall lock the session after an administrator specified time-interval of user inactivity, which may be dependent on the authentication mechanism used.

To unlock a locked session the user is required to re-authenticate.

B.6.4.4 Protected authentication feedback

The TSF shall not produce a visible display of passwords or PINs when used. To provide the user with some feedback the TOE shall however obscure authentication information. E.g. when a user enters a password each character is replaced with a '*'.

B.6.5 Security management

B.6.5.1 Security roles

The TOE supports the following TOE user roles:

- Administrator
- Manager
- Client

The Workflow System Application provides administrators with an administrative interface for managing the overall security of the TOE. An workflow management interface provides managers with capability to manage the process definitions and the execution of workflow instances. The client interface provides clients with a interface for accessing the Workflow System Application. Through this interface clients may interact with the system with respect to the privileges they may activate.

B.6.5.2 Administrative interface

The administrative interface allows administrators to:

- Start-up and shutdown the TOE
- Manage the set of authorised users and their security attributes e.g. associate users with TOE roles
- Manage the behaviour of the identification and authentication mechanisms and which mechanisms are to used(see B.6.4.2).
- Manage the access control and information flow control functions which are used to enforce all SFPs of the TOE and decide whether a operation should be allowed or disallowed.
- Manage and define the SFPs which are to be enforced within the entire system; the SWFS access SFP, Workflow flow SFP and application flow SFPs.
- Manage the session locking functions (see B.6.4.3).
- Manage the audit functions (see B.6.1).
- Manage the cryptographic functions (see B.6.2).
- Specify when and how backups of TSF data, security functional policies and audit log data shall be made and to revert to previous revisions of these files. The administrator may specify different backup schemes for backup data e.g. frequency of backup and backup mode. Recovery operations may be performed when the TSF is in the maintenance mode.

B.6.5.3 Workflow management interface

The workflow management interface allows managers to:

- Create, modify and delete process definitions and workflow instances and their associated workflow access and flow SFPs.

- Monitor created workflow instances.
- Manage the workflow user security attributes, workflow group and workflow role, in order for clients to participate in workflow instances.
- Assign and revoke static privileges related to workflow instances or to enable clients to create new workflow instances of specified process definitions.

B.6.5.4 Client interface

The client interface allows clients to:

- Manage the set of active privileges.

Management of the set of active privileges may be performed automatically as the client indirectly activates privileges by performing available tasks.

B.6.6 Secure communication

B.6.6.1 User applications

To ensure that information received from and sent to user applications is not modified or disclosed the TLS protocol[16] shall be used between the user application and the Workflow System Application. The following cipher suites may be used:

- TLS_RSA_WITH_AES_128_CBC_SHA, or
- TLS_RSA_WITH_AES_256_CBC_SHA.

The cryptographic keys are required to be of 128 or 256 bits for AES and be of a minimum of 1024 bits for RSA. The cryptographic service provider used by the TOE shall be FIPS140-2 compliant and be provided by the host OS of the Workflow System Application.

B.6.6.2 Trusted external applications

The functions responsible for invoking trusted applications and communicating with trusted SWFSs establishes trusted channels using the TLS protocol[16] with the cipher suites described in B.6.6.1. To ensure the authenticity of both endpoints TLS is used in mutual authentication mode using X.509 certificates. When the trusted channel has been established the confidentiality and integrity of all data sent and received is protected.

B.6.6.3 Trusted Client Application

The communication between the Trusted Client Application and the Workflow System Application is protected by TLS as well. The Trusted Client Application and the Workflow System Application mutually authenticate using X.509 certificates. For all user data transmitted the Advanced application flow SFP is enforced and data is monitored for integrity errors.

B.6.6.4 Importation and exportation

The importation and exportation functions of the TOE ensure that data is imported and exported according the application flow SFPs. Depending on what SFP the application is covered by the security attributes of the data is either ignored or used. The functions ensure that the sensitivity label of objects sent and received are interpreted consistently.

Appendix C

Design

Table C.1 lists the commands of the 4 TSFIs of group A identified in section 4.2. All commands prefixed with 'WM' are part of the WAPI. An activity corresponds to a task and a process instance to a workflow instance. All TSFI containing the word 'Open' has two additional commands 'Fetch' and 'Close'. This means that e.g. that the command WMOpenProcessDefinitionsList also has a WMFetchProcessDefinition and WMCloseProcessDefinitionsList. The 'Fetch' command returns the next item in the list obtained using the 'Open' command, while the 'Close' command closes the list.

Common Interface Commands
WMConnect *Purpose: Enables a user to establish a connection to the Workflow System Application.*
WMDisconnect *Purpose: Disconnect user from Workflow System Application.*
ReAuthenticate *Re-authenticate user of a specified session.*
LockSession Lock and save specified session.

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

UnlockSession Unlock and load specified session.
Administrative Interface Commands
Startup *Purpose: Startup the Workflow System Application.*
Shutdown *Purpose: Shutdown the Workflow System Application.*
ReturnFromMaintenance *Purpose: Return the Workflow System Application from maintenance mode to operational mode.*
OpenUserList *Purpose: Get list of user accounts matching a filter criterion.*
OpenUserAttributeList *Purpose: Get list of attributes associated with a specified user.*
GetUserAttributeValue *Purpose: Returns the value of a specified user attribute.*
ChangeUserAttribute *Purpose: Assign an attribute, remove an attribute or change the value of an attribute for a specified user.*
AddUser *Purpose: Add user account.*
DeleteUser *Purpose: Delete user account.*
OpenRoleList *Purpose: Get list of security roles.*
OpenSFPList *Purpose: Get list of security functional policies(SFP).*
ModifySFP *Purpose: Modify a specified SFP.*
GetCryptoConf *Purpose: Get the configuration of the cryptographic functions used.*
ChangeCryptoConf *Purpose: Change the configuration of the cryptographic functions used.*
CreateBackup *Purpose: Create a new backup using the specified filter criterion.*
GetBackupConf *Purpose: Get the backup configuration.*
ChangeBackupConf *Purpose: Change the backup configuration.*
OpenBackupList *Purpose: Get list of created backups matching the filter criterion.*

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

GetBackupInfo *Purpose: Get information about specified backup.*
RecoverBackup *Purpose: Recovers data using the specified backup.*
GetPasswdPolicy *Purpose: Get the client password policy.*
ChangePasswdPolicy *Purpose: Change the client password policy.*
AuditConf *Purpose: Get audit configuration.*
GetAudit *Purpose: Get audit log.*
OpenApplicationObjectList *Purpose: Get a list of application data objects that matches a filter criterion.*
OpenLabelList *Purpose: Get a list of sensitivity labels that matches a filter criterion.*
ChangeObjectLabel *Purpose: Change the label of a specified object.*
AddApplication *Purpose: Add new invokable application.*
DeleteApplication *Purpose: Delete application.*
OpenApplicationList *Purpose: Get list of invokable applications.*
OpenApplicationAttributeList *Purpose: Get list of attributes of a specified application.*
GetApplicationAttributeValue *Purpose: Get value of attribute for specified application.*
AssignApplicationAttribute *Purpose: Assign an attribute, change an attribute or change the value of an attribute of a specified application.*
OpenApplicationMap *Purpose: Get the map containing the mapping between applications and application agents matching a filter criterion for a specified process definition.*
ChangeApplicationMapping *Purpose: Change the mapping between an application and an application agent.*
Workflow management Interface Commands

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

OpenWFRoleList *Purpose: Get list of workflow roles matching a filter criterion for a specified process definition.*
OpenWFRoleMap *Purpose: Get the map containing the mapping between workflow roles and users matching a filter criterion for a specified process definition.*
ChangeWFRoleMapping *Purpose: Change the mapping between a workflow role and a user.*
WMOpenProcessDefinitionsList *Purpose: Get list of process definitions that matches a filter criterion.*
DeleteProcessDefinition *Purpose: Delete specified process definition.*
ExportProcessDefinition *Purpose: Exports a specified process definition to outside of the TOE.*
ImportProcessDefinition *Purpose: Imports a process definition from outside of the TOE.*
WMOpenProcessDefinitionStatesList *Purpose: Get list of states that are available and match a filter criterion for a specified process definition.*
WMChangeProcessDefinitionState *Purpose: Change the state of the process definition.*
WMCreateProcessInstance *Purpose: Create new workflow instance of a specified process definition.*
WMStartProcess *Purpose: Start the execution of a specified workflow instance.*
WMTerminateProcessInstance *Purpose: Terminate a specified workflow instance gracefully. Stops the workflow instance when the currently running tasks are complete.*
WMOpenProcessInstanceStatesList *Purpose: Get list of states that are available and match a filter criterion for a specified workflow instance.*
WMChangeProcessInstanceState *Purpose: Change the state of the workflow instance.*
WMOpenProcessInstanceAttributesList *Purpose: Get list of attributes for a specified workflow instance.*
WMGetProcessInstanceAttributeValue *Purpose: Returns the value of a specified workflow instance attribute.*
WMAssignProcessInstanceAttribute *Purpose: Assign an attribute, change an attribute or change the value of an attribute of a specified workflow instance.*

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

WMOpenActivityInstanceStatesList *Purpose: Get list of states that are available and match a filter criterion for a task instance.*
WMChangeActivityInstanceState *Purpose: Change the state of a specified task instance.*
WMOpenActivityInstanceAttributesList *Purpose: Get list of attributes for a specified task instance.*
WMGetActivityInstanceAttributeValue *Purpose: Returns the value, type and length of a specified task instance attribute.*
WMAssignActivityInstanceAttribute *Purpose: Assign an attribute, change an attribute or change the value of an attribute of a specified task instance.*
WMOpenProcessInstancesList *Purpose: Get list of workflow instances that matches a filter criterion.*
WMGetProcessInstance *Purpose: Provides information about what work has been done within a workflow instance and what is the current work being done within the workflow instance.*
WMOpenActivityInstancesList *Purpose: Get list of task instances that matches a filter criterion.*
WMGetActivityInstance *Purpose: Provides status information about a task within a workflow instance.*
WMChangeProcessInstancesState *Purpose: Change the state of the workflow instances of a specified process definition matching a filter criterion..*
WMChangeActivityInstancesState *Purpose: Change the state of the task instances of a specified process definition matching a filter criterion.*
WMTerminateProcessInstances *Purpose: Terminate the workflow instances of a specified process definition matching a filter criterion.*
WMAssignProcessInstancesAttribute *Purpose: Assign an attribute to a set of workflow instances within a process definition matching a filter criterion.*
WMAssignActivityInstancesAttribute *Purpose: Assign an attribute to a set of task instances within a process definition matching a filter criterion.*

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

WMAbortProcessInstances *Purpose: Abort the set of workflow instances that correspond to a specified process definition, that match the specific filter criterion, regardless of its state. The workflow instances will be terminated when possible.*
WMAbortProcessInstance *Purpose: Abort a specified workflow instance regardless of its state. The workflow instance will be terminated when possible.*
WMOpenWorkitemStatesList *Purpose: Get the list of states that are available for a specified workitem matching a filter criterion.*
WMChangeWorkitemState *Purpose: Change the state of a specified workitem.*
WMReassignWorkItem *Purpose: Re-assign a specified workitem from one client worklist to another client worklist.*
WMAssignWorkItemAttribute *Purpose: Assign an attribute, change an attribute or change the value of an attribute of a specified workitem.*
Client Interface Commands
WMOpenWorkList *Purpose: Returns a list of workitems assigned to a specified client or assigned within a specified workflow group.*
WMGetWorkItem *Purpose: Retrieves a workitem. The workitem is not necessarily locked or retracted from other users worklists, but it may be.* *Note: Any dynamic privileges associated with this workitem will be assigned to the client.*
WMCompleteWorkItem *Purpose: Tell the system that this workitem has been completed.* *Note: Any dynamic privileges associated are revoked and the workitem is retracted from all worklists.*
WMOpenWorkItemAttributesList *Purpose: Returns a list of attributes for a workitem.*
WMGetWorkItemAttributeValue *Purpose: Returns the value, type and length of a specified workitem attribute.*
WMTAInvokeApplication *Purpose: Invokes a specified application*
ExportAppData *Purpose: Exports application data or part of some application data to the outside of the TOE.*

Table C.1: List of identified commands for each of the 4 TSFIs (continued on next page).

ImportAppData *Purpose: Imports application data or part of some application data into the TOE.*

Table C.1: List of identified commands for each of the 4 TSFIs.

Bibliography

[1] Workflow Management Application Programming Interface (Interface 2&3) Specification. (ver. 2.0), July 1998.

[2] Labeled Security Protection Profile. (Version 1.b), October 1999. Available from http://www.commoncriteriaportal.org.

[3] Workflow Management Facility Specification, v1.2. Technical report, The Object Management Group, April 2000. Available from http://www.omg.org/docs/formal/00-05-02.pdf.

[4] Fips 180–2, Secure Hash Standard (SHS). August 2002.

[5] Security Target for Citrix MetaFrame XP Presentation Server For Windows with Feature Release 3. (Version 1.6), March 2004. Used for evaluation of Citrix MetaFrame XP Presentation Server with Feature Release 3. The ST is available from http://www.commoncriteriaportal.org.

[6] Security Target for IBM z/VM Version 5 Release 1 with Required System Update (RSU) 1. (Version 1.6), May 2005. Used for evaluation of IBM z/VM Version 5, Release 1 with RSU1. The ST is available from http://www.commoncriteriaportal.org.

[7] webMethods Fabric 6.5 EAL2 Common Criteria Evaluation Security Target V1.0. December 2005. Used for evaluation of webMethods Fabric 6.5. The ST is available from http://www.commoncriteriaportal.org.

[8] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2006. Version 3.1, Revision 1. Available from http://www.commoncriteriaportal.org.

[9] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2006. Version 3.1, Revision 1. Available from http://www.commoncriteriaportal.org.

[10] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2006. Version 3.1, Revision 1. Available from http://www.commoncriteriaportal.org.

[11] Microsoft Windows 2003/XP Security Target. (Version 1.0), September 2006. Used for evaluation of Microsoft Windows Server 2003 and Microsoft Windows XP. The ST is available from http://www.commoncriteriaportal.org.

[12] WebSphere MQ EAL4 Security Target. (Version 1.0), July 2006. Used for evaluation of IBM WebSphere MQ 6.0.1.1. The ST is available from http://www.commoncriteriaportal.org.

[13] Gido A.J.F. Brouns. Featuring Workflow Management – An overview of the distinctive features of workflow processes and their consequences for workflow management. March 15 2000. Available from http://www.win.tue.nl/~ace/publications/wfm.pdf.

[14] Xuemin Lin Chengfei Liu, Maria Orlowska and Xiaofang Zhou. Task Failures, Infrastructure Failures and WFMS Failures. pages 276–283, April 2001.

[15] P. Chown. Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS). June 2002. Available from http://tools.ietf.org/html/rfc3268.

[16] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. April 2006. Available from http://tools.ietf.org/html/rfc4346.

[17] Gordon Docherty. Workflow from a Business Perspective: Organizational and Management Considerations. Technical report, Enterprise Workflow National Project, March 2005. Website: http://www.workflownp.org.uk/.

[18] Christian Stüble Dr. Steffen Lange, Dr. Andreas Nonnengart and Roland Vogt. Discretionary Information Flow Control (MU) Protection Profile. (Version 2.01), September 2002. Available from http://www.commoncriteriaportal.org.

[19] Rune Friis-Jensen. Secure Workflow Systems Protection Profile 1.0. 2007. Part of the Master Thesis, A CC Approach to Secure Workflow Systems by the same author.

[20] David Hollingsworth. Workflow Management Coalition The Workflow Reference Model. Technical report, Workflow Management Coalition, January 1995.

[21] Allan Pedersen and Anders Hedegaard. Security in POS Systems. Master's thesis, The Technical University of Denmark (DTU), August 2005.

[22] Charles Plesums. *The Workflow Handbook 2002*, pages 19–38. 2002. Chapter is available from http://www.wfmc.org/information/introduction_to_workflow02.pdf.

[23] Jim Reynolds and Ramaswamy Chandramouli. Role–Based Access Control Protection Profile. (Version 1.0), July 1998. Available from http://www.commoncriteriaportal.org.

[24] Howard Smith. Database Management System Protection Profile. (Issue 2.1), May 2000. Available from http://www.commoncriteriaportal.org.