Tivoli software

IBM

Identity Management Protection Profile

IMPP

BSI-PP-0024

Version Number 1.17

Date: January 12, 2006

Status: Final

Author: David Ochel

Owner: Brian Matthiesen

Note: This document will become a public document at the end of the evaluation

Table of Contents

1. PROTECTION PROFILE (PP) INTRODUCTION 5

1.1. PP IDENTIFICATION 5
1.2. PP OVERVIEW 5
1.3. PP EVALUATION STATUS 5
1.4. CC CONFORMANCE CLAIM 5
1.5. STRENGTH OF FUNCTION 6

2. TOE DESCRIPTION 7

2.1. INTRODUCTION 7
2.2. TOE STRUCTURE 8
2.3. SECURITY FUNCTIONALITY 8
2.4. SECURITY POLICY MODELING 9
2.4.1 Entitlement and Provisioning 9
2.4.2 Supportive Security Functionality 9
2.4.3 IT Environment 11

3. TOE SECURITY ENVIRONMENT 12

3.1. ASSUMPTIONS 12
3.1.1 Environment of use of the TOE 12
3.2. THREATS 12
3.3. ORGANIZATIONAL SECURITY POLICIES 13

4. SECURITY OBJECTIVES 15

4.1. SECURITY OBJECTIVES FOR THE TOE 15
4.2. SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 16
4.3. NON-IT SECURITY OBJECTIVES FOR THE ENVIRONMENT 17

5. IT SECURITY REQUIREMENTS 18

5.1. TOE SECURITY REQUIREMENTS 18
5.1.1 TOE Security Functional Requirements 18
5.1.2 TOE Security Assurance Requirements 25
5.2. SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT 25
5.2.1 Managed Resources 25
5.2.2 Repository 26
5.2.3 Secure Network Sessions 27
5.2.4 Runtime Environment of the TOE 28

6. PP APPLICATION NOTES 29

7. RATIONALE 30

7.1. SECURITY OBJECTIVES RATIONALE 30
7.1.1 Security Objectives Coverage 30
7.1.2 Security Objectives Sufficiency 31
7.2. SECURITY REQUIREMENTS RATIONALE 32
7.2.1 Security Requirements Coverage 32
7.2.2 Security Requirements Sufficiency 34
7.2.3 Security Requirements Dependencies 35
7.2.4 Internal Consistency and Mutual Support 37
7.2.5 Evaluation Assurance Level and Strength of Function 38

A. APPENDIX 39

A.1 DEFINITION OF TERMS 39

Figures

Figure 1: Structural view of TOE (white) and IT Environment (grey) 8
Figure 2: A provisioning workflow and the scope of the TSP 10

Tables

Table 1: security objectives traced back to threats and organizational security policies 30
Table 2: security objectives for the IT environment traced back to threats, organizational security policies and assumptions 30
Table 3: security objectives for the non-IT environment traced back to threats, organizational security policies and assumptions 31
Table 4: sufficiency of objectives countering threats 31
Table 5: sufficiency of objectives implementing OSPs 32
Table 6: sufficiency of objectives covering assumptions 32
Table 7: SFRs for the TOE traced back to objectives for the TOE 33
Table 8: SFRs for the environment traced back to objectives for the environment 34
Table 9: Dependency Analysis for TOE SFRs 36
Table 10: Dependency Analysis for the Managed Resources in the IT environment 37
Table 11: Dependency Analysis for the Repository in the IT environment 37
Table 12: Dependency Analysis for Transaction Security in the IT environment 37
Table 13: Dependency Analysis for the Runtime Environment of the TOE in the IT environment 37

Document Control Information

Required Reviewers

Area	Reviewer Name	Date Reviewed
IBM Tivoli	Bob Blakley	
Product Testing	Brian Matthiesen	
Product Architecture	Tony Gullotta	
Product Development	Weber (Weibo) Yuan	
Product Marketing	Steve Henning	

Approval

Changes not related to content (e.g., spelling, grammar, organizational title changes, etc.) do not require approval. The approvers of this document are:

Area	Approver Name	Date Approved
Quality Assurance	Brian Matthiesen	

Approval is by formal review.

History

Version	Date	Summary of Changes
1.00	February 13, 2004	First release submitted for evaluation.
1.10	April 21, 2004	Evaluation results and comments incorporated.
1.11	May 11, 2004	Updated due to comments from Quality Assurance.
1.12	June 06, 2004	Editorial changes.
1.13	July 23, 2005	Changed conformance claim to CC 2.2.
1.14	August 11, 2005	Clarified T.AUTHORIZED
1.15	January 03, 2006	Addressed certifier comments
1.16	January 04, 2006	Corrected typographical error.
1.17	January 12, 2006	Clarification on threats.

1. Protection Profile (PP) Introduction

This document represents a Protection Profile (PP) for products offering identity management, i.e. a solution to manage accounts on multiple resources for persons within large organizations.

1.1. PP Identification

Title: Identity Management Protection Profile Version 1.17 Status: Final

Keywords: Identity Management, Protection Profile, IMPP

This document is a Protection Profile expressing Common Criteria requirements for identity management solutions, offered to the security community by IBM.

1.2. PP Overview

The target of evaluation (TOE) is a product providing an identity management solution. This Protection Profile describes the TOE, its boundary, IT environment and IT security requirements.

Identity Management solutions provide the software and services needed for deploying policy-based provisioning solutions. They help companies automating the process of provisioning employees, contractors and business partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise.

The TOE provides the following Identity Management security functionality:

- entitlement decisions and export of user account information to management resources
- export and management of person and account data

The TOE provides the following security functionality to support the Identity Management functionality:

- identification and authentication of users
- authorization of user-initiated transactions
- auditing of transactions
- TSF protection

1.3. PP Evaluation Status

Registration of IMPP has been applied for.

1.4. CC Conformance Claim

The Protection Profile is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.2, Revision 256, CCIMB-2004-01-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.2, CCIMB-2004-01-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.2, Revision 256, CCIMB-2004-01-003

referenced hereafter as [CC].

For its evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation

Methodology, Version 2.2, Revision 256, CCIMB-2004-01-004 [CEM]

This Protection Profile claims the following CC conformance:

- part 2 conformant
- part 3 conformant
- evaluation assurance level (EAL) 3 augmented by ALC_FLR.1

1.5. Strength of Function

The claimed strength of function (SOF) for this TOE is: **SOF-medium**.

2. TOE Description

The following sections provide a description of the structure of the TOE and the TOE boundary, and an overview of the minimum security functionality provided by the TOE.

2.1. Introduction

Identity management is a commonly used term for the central management of user identities that need to be available throughout a number of systems in a distributed operating environment. The TOE is an identity management product.

The TOE's main purpose is organization-wide account management for a large number of systems that are known as managed resources. For this purpose the TOE maintains a repository containing information about all persons (or, identities) that belong to the organization and might need access to an arbitrary number of managed resources.

While the managed resources itself are not part of the TOE (examples for managed resources would be a file server or a data base system), each managed resource is represented within the TOE as a 'service' object. By applying administrator-defined rules that are targeting attributes assigned to a person (for example, a certain role assigned to a person) the TOE is able to decide whether the person is allowed to possess an account on selected services or not. The positive result of such a decision is called 'entitlement': the person is entitled to an account on a service. The administrator-defined rules are therefore called 'entitlement rules'. An entitlement may not only comprise the pure fact that an account is granted to a person, but may also contain certain attributes for such an account (e.g. group memberships on the managed resource).

The TOE initiates the actual enforcement of an entitlement, i.e. the creation of an account for a person on the service the person is entitled to, by interfacing the managed resource and invoking its proprietary account management functions. This is called the 'provisioning'. Provisioning of accounts is not restricted to the creation of accounts, but includes also the modification or deletion of accounts if the entitlement of a person changes or is no longer existent.

The term identity management implies a solution that may provide advanced features of person and account management, e.g. the management of passwords for accounts, the position of a person in an organizational hierarchy, the definition of supervisors for persons, etc. – Such features would likely be based on additional attributes maintained for persons in the TOE's repository.

A TOE providing sufficient automation for the provisioning of user accounts will be able to support an organization in its account management – users in certain organizational roles can automatically be entitled to and provisioned with accounts on the systems they will need to use. The involvement of potentially several system administrators to generate and maintain such accounts is reduced to a minimum. Having a central repository for the management of persons belonging to the organization and, at the same time, the accounts provisioned for them on the managed resources that are distributed throughout an organization will result in a timely, high consistency between a person's status within the organization and the person's authorization to access actual systems and data associated with this status.

2.2. TOE Structure

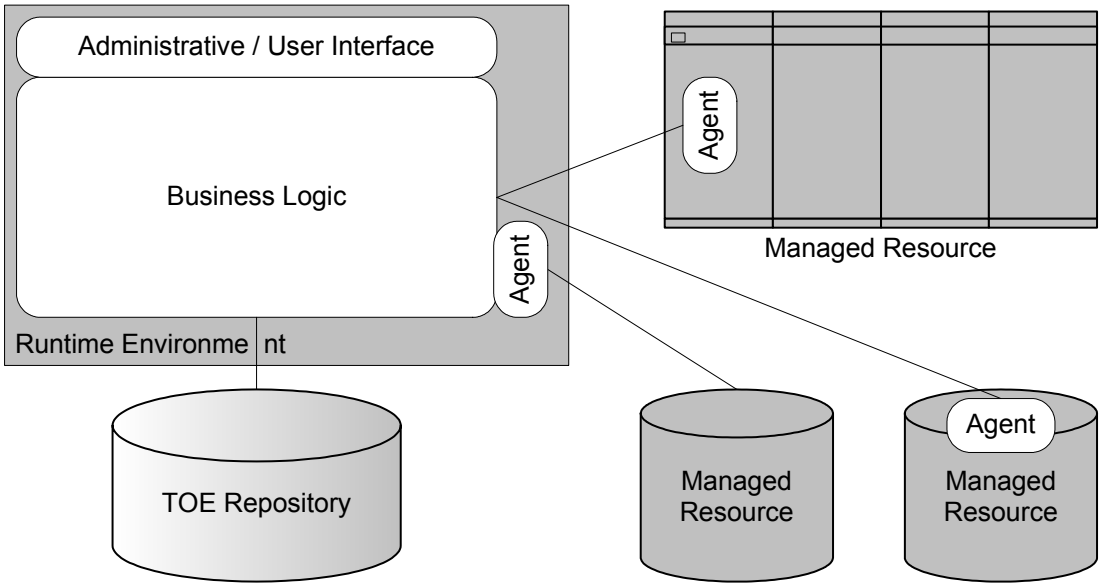

Figure 1: Structural view of TOE (white) and IT Environment (grey)

The TOE comprises a central element that implements its business logic and provides an interface to allow interaction with TOE users (e.g. management of entitlement rules). The central element of the TOE is likely to be implemented as an application that runs on a runtime environment provided by the IT environment.

The managed resources in the IT environment are interfaced by 'agents'. Agents transport account management requests generated by the TOE's business logic during provisioning to the managed resources that are expected to enforce these requests. For the purpose of this overview, IMPP envisions two different types of agents (without the intention to limit an actual TOE to the implementation of those types): agents that reside on the central runtime environment for the TOE and invoke account managements interfaces that are exported by managed resources, and agents that are installed on the managed resource itself (e.g. as a plug-in, service or daemon) and interface account management resources directly (e.g. the /etc/passwd file on a Linux system).

TSF data and user data is stored in a TOE Repository. Note that – since the storage of data is no core functionality of the TOE – IMPP does not stipulate whether the repository is implemented as part of the TOE or in the IT environment.

2.3. Security Functionality

The security functionality involved in the business logic of service entitlements and account provisioning can be characterized as follows:

- provide entitlement decisions – such decisions are the result of evaluating entitlement rules that define the entitlement of persons with certain attribute values to a service
- export account data – account data exported to a managed resource in the environment must represent the actual entitlement status of the person that is associated with the account; such data may also contain security attributes (e.g. passwords)

In addition, supportive security functionality is required for a TOE. This is inevitable in order to protect the TSF itself as well as the TSF data and user data:

- user authentication and the authorization of user-initiated actions – e.g. the management of user data such as person information and entitlement rules, as well as the triggering of account

provisioning, must be restricted to authorized individuals represented by TOE users

- auditing – the generation of audit data is considered a valuable contribution to the secure management and operation of the TOE by providing accountability for security-relevant events
- TSF protection – the TOE must prevent bypassing of the TSF

2.4. Security Policy Modeling

This section shall enable the reader to understand and comprehend the selection of security functional requirements in chapter 5 that define the minimum security functionality required from an identity management solution.

2.4.1 Entitlement and Provisioning

The concept of account entitlement and provisioning introduced in IMPP actually shows a strong resemblance to the concept of discretionary access control. In traditional access control models a user (the subject) requests access to certain resources (the objects) – an access control decision is made based on user-defined rules (the access control information). Positive decision is enforced by granting the subject access to the objects. In an identity management solution, a person (the subject) demands accounts on services (the objects) – an entitlement decision is made based on user-defined rules (the entitlement rules). Positive decision is enforced by provisioning user accounts for the subject on the managed resources, or objects.

Small deviations seem to exist between discretionary access control and account provisioning. An access control model has subjects that are actively requesting access to an object – in identity management, the request to provision an account on a managed resource is not issued by the person that is demanding the account, but by an entity that is not necessarily linked to the person. Such an entity is typically a TOE user that is able to access the TSF in order to initiate the account provisioning. Managed objects are not under control of the TOE, but only represented by services in the TOE's data model. However, the actual entitlement decision is an access control decision. IMPP adapts the security functional requirements provided by CC Part 2 for the definition and enforcement of discretionary access control policies to define a **provisioning policy** which implements the entitlement decision. Note that the entitlement rules are considered self-contained objects managed by the TOE, rather than attributes associated with the service representations in the TOE.

The provisioning itself is consequently modelled as export of data to the IT environment. The PP demands that such export is the actual enforcement of an entitlement decision, i.e. the provisioning policy must be invoked when account data is exported. As an optional part of the data export, IMPP also allows for the implementation of additional, administrator-specified rules that can be defined for the export of account data: workflows are considered self-contained objects maintained by the TOE representing functionality that may be invoked as part of the provisioning process before or after the actual export of the account data. Note that IMPP does not further endorse the definition or employment of workflows – this is left to the ST author.

2.4.2 Supportive Security Functionality

TOE users are required to provide administration of the TSF and management of the objects maintained by the TOE. Depending on the TOE implementation, they may be required to initiate the actual account provisioning and to participate in administrator-specified workflows. Accountability for the actions of TOE users is required and implemented by appropriate auditing requirements.

In order to ensure that only authorized TOE users can perform these activities, including the modification of security-relevant user data, the TOE has to control the access to the TOE security functions as well as to TSF data and user data. While this (and the requirement for auditing) requires successful identification and authentication of TOE users, IMPP imposes in addition the implementation of a discretionary access control policy to mandate access to the TOE: it is

considered necessary to allow the separation of administrative actions related to the TOE itself, such as audit configuration and review, from the administrative actions related to the policies that the TOE enforces, such as user data and entitlement rule management. For this reason, the concept of the **TOE access control policy** and a TOE administrator role is introduced. However, in most cases it is left to the ST author to restrict the access to certain functionality to the administrator role or to another class of authorized users.

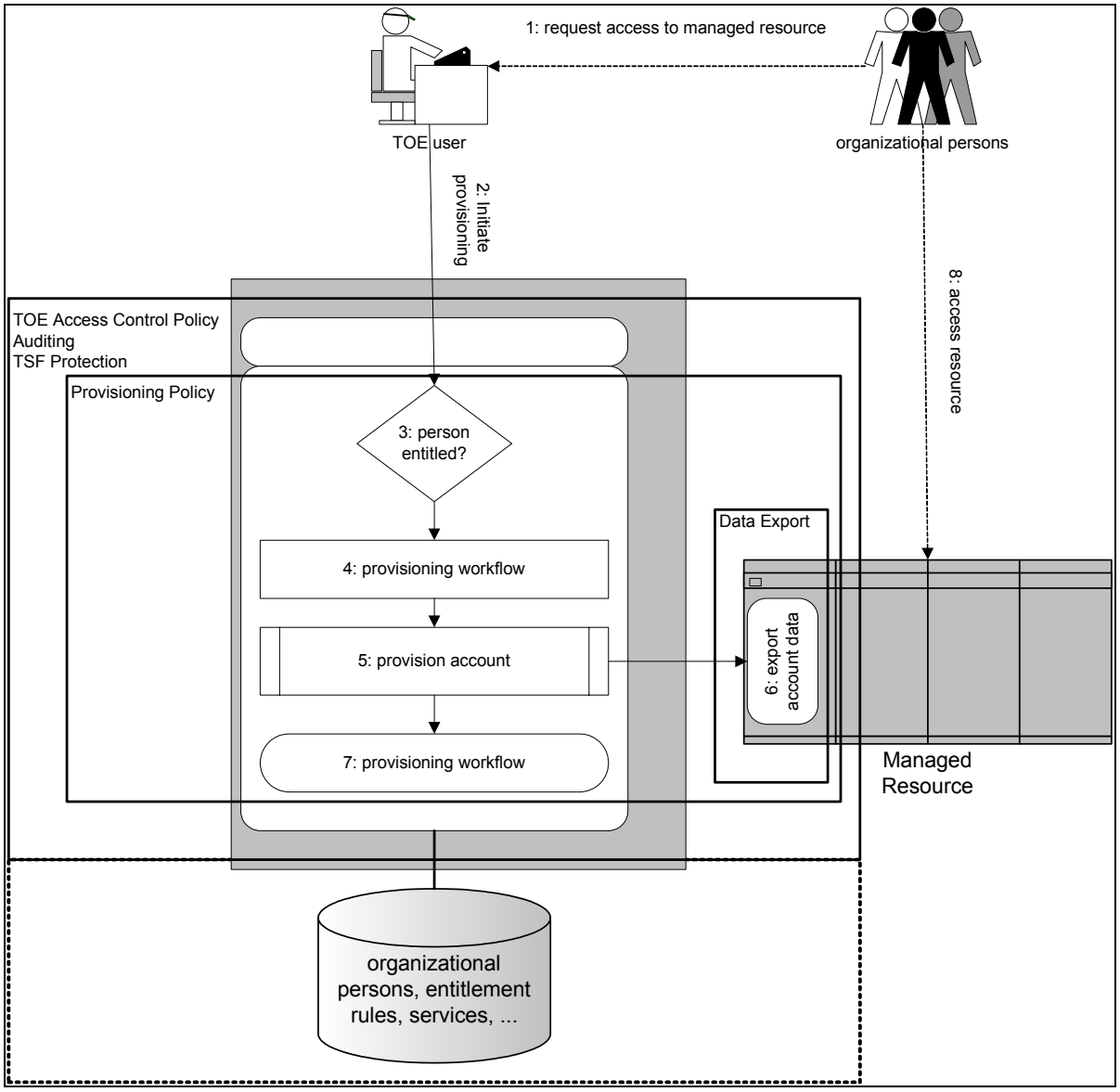

Figure 2: A provisioning workflow and the scope of the TSP

It is therefore appropriate to require the maintenance of, and restriction of access to, the following objects of the TOE access control policy:

- persons, also known as organizational persons, having organizational and account data attributes (subjects of the provisioning policy)
- services (objects of the provisioning policy)
- entitlement rules
- workflows

- TOE users, having role and authentication credential attributes (subjects of the TOE access control policy)
- access control information
- audit data

It is conceivable that the TOE will not be an organization's main repository for person data (for example, an organization might already operate a solution for human resources management). In such cases, the import of person data from trusted products in the IT environment needs to be supported to allow the automated handling of large numbers of persons – this has been reflected by an appropriate requirement. Another conceivable architecture, which is not further addressed by IMPP, is a TOE that applies provisioning policies directly to persons managed in an external person repository (such as an X.500 directory serving as an organization's primary corporate directory for multiple applications) without importing the person data from the external repository into the dedicated TOE Repository first.

In addition, reference mediation is required to protect the TSF from circumvention.

2.4.3 IT Environment

In order to provide flexibility IMPP allows for the implementation of aspects that are not considered the TOE's core functionality in the IT environment. It is the choice of the ST author to pull the corresponding requirements into the TOE instead:

The utilization of a repository in the IT environment to actually store TSF data and user data is expected by IMPP. Also, assuming that the TOE due to its nature has to be a distributed product, protection of network sessions is required to be implemented by the IT environment. In addition, the runtime environment of the TOE is required to provide support in areas that typically cannot be implemented by a software application on its own, namely in providing for domain separation and a reliable time source.

3. TOE Security Environment

3.1. Assumptions

The description of assumptions illustrates the security aspects of the environment in which the TOE will be used or is intended to be used. This includes information about the environment of use of the TOE, including physical, personnel, and connectivity aspects.

3.1.1 Environment of use of the TOE

Physical aspects:

A.PHYS_PROT The machine(s) providing the runtime environment for the TOE need to be protected against unauthorized physical access and modification.

Personnel aspects:

A.ADMIN The administrators for the TOE and the underlying systems of the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator guidance. They are well trained to securely and trustworthy administer all aspects of TOE operation in accordance with the TOE's Security Target.

They will protect their credentials used for authentication against the TOE. Credentials must not be disclosed to any other individual.

A.USER Users of the TOE originate from a well managed user community as described in section 3.2.

They will protect their credentials used for authentication against the TOE. Credentials must not be disclosed to any other individual.

Connectivity aspects:

A.AGENT It is assumed that the runtime environment for an agent operates as specified with respect to the interfaces exposed to the TOE for exchange of account information and provides adequate protection measures against tampering with the agent and its interfaces.

A.REPOSITORY The repository in the IT environment used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in them.

Application Note: This assumption only applies if the TOE relies on an external repository for TSF or user data storage.

A.SERVER The machine(s) providing the runtime environment for all parts of the TOE are configured in such a way that no unauthorized access to the TOE is possible either locally or via any network connection.

3.2. Threats

The security threats that need to be countered by the TOE or by the TOE environment are listed

below.

The **assets** to be protected by the TOE comprise the information processed and transmitted by the TOE. The term "information" is used here to refer to all data held within the TOE or parts of the TOE. The TOE counters the general threat of unauthorized access to information, where "access" includes disclosure, modification and destruction.

The assets to be protected are therefore:

- information related to persons and accounts (including e.g. organizational structures, users, roles and groups)
- policies, service definitions, workflows, entitlement rules and access control information maintained by the TOE
- authentication and transaction security credentials

The **threat agents** can be categorized as either

- unauthenticated individuals, i.e. entities not known to the TOE but having network-based access to the communications interfaces exposed by the TOE, or
- authorized users of the TOE, i.e. individuals who have successfully authenticated themselves to the TOE and may access resources as defined by the access control information via the user and administrative interface.

The threat agents are assumed to originate from a well managed user community in a non-hostile working environment, and hence the product protects against threats of inadvertent or casual attempts to breach the system security. The TOE is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. An example of an intended environment is a corporate network well protected from external attacks and with an overall user community (including unauthenticated users) that can be assumed to be non-hostile. System administrators of the TOE as well as those for the underlying systems and external data repositories supportive to the TSF are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility.

T.BYPASS	An attacker accesses protected resources of the TOE in a way that bypasses the TSF, exploiting non-TSF portions of the TOE.
T.COM_ATT	An attacker intercepts communication between the TOE and an external entity or between different parts of the TOE in order to get access to confidential information, to impersonate as an authorized user or as part of the TOE or to manipulate the data transmitted between the TOE and an external or internal entity.
T.UNAUTHORIZED	An attacker (possibly, but not necessarily, a person allowed to use the TOE) gains access to TSF data or user data that he is not authorized to have access to.

3.3. Organizational Security Policies

The following organizational security policies are deemed appropriate in a security environment for the TOE:

P.ACCOUNTABILITY	The users of the TOE shall be held accountable for security-relevant transactions they have requested.

P.FEED	Account and person data imported into the TOE must be properly associated with the corresponding data already existent in the TOE data store. Person information stored in an external data store and subject to import into the TOE is managed in a way that allows proper association with the person information and organizational structure as defined within the TOE.
P.PROVISION	The provisioning of accounts on a remote service shall only be entitled to persons that are subject to a corresponding provisioning policy and entitlement rules resp.. Account data provided to managed resources must be interpreted consistently and managed as requested by the TOE.

4. Security Objectives

This section defines the security objectives for the TSF and its supporting environment. Security objectives are categorized as IT security objectives for the TOE or the IT environment as well as non-IT security objectives to be met by organizational means in the TOE environment.

4.1. Security Objectives for the TOE

O.ACI	The TSF must ensure that only authorized users gain access to the TOE and the resources it protects. Access control shall be governed by access control information that may authorize access for single users or groups of users to single resources or groups of resources. Administrators shall not be restricted in accessing arbitrary resources.
O.AUDIT	The TSF must generate information about the status of security relevant transactions for recording. The TSF must present this information to authorized users.
O.FEED	The TSF must ensure that account and person data imported into the TOE are properly associated with the corresponding data already existent in the TOE data store.
O.I&A	The TSF must authenticate users and administrators which request access to the TOE and its resources.
O.PROVISION	The TSF must ensure that account generation on a managed resource is only initiated for persons that are entitled to possess an account on this managed resource.

4.2. Security Objectives for the IT Environment

OE.AUDIT The runtime environment for the audit mechanism of the TOE must provide a reliable time source for audit record generation.

Application Note: If the TOE itself provides a secure time source, the ST author shall merge this objective with O.AUDIT.

OE.COM_PROT Communication of TOE external entities with the TOE as well as communication between physically distributed parts of the TOE must be protected to ensure the integrity and confidentiality of the communication.

Application Note: In case the TOE implements functions for transaction security, the ST author may transform this objective into an objective for the TOE.

OE.ENFORCEMENT The runtime environment for the TOE must provide a dedicated execution domain for the TOE to protect it from untrusted subjects.

OE.MANAGED Each managed resource exchanging account data with the TOE must interpret this data in a consistent way and perform the account management actions requested by the TOE.

OE.REPOSITORY The repository in the IT environment used by the TOE to store TSF or user data must protect such data against unauthorized access.

Application Note: In case the TOE implements storage of TSF data and user data, the ST author may transform this objective into an objective for the TOE.

4.3. Non-IT Security Objectives for the Environment

OE.ADMIN	Those responsible for the TOE shall ensure that the administrative personnel for the TOE and its underlying systems – as well as administrators for the repositories and data feed in the environment – are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator guidance. They must be well trained to securely administer all aspects of TOE installation, configuration and operation in accordance with its Security Target and initiate administrative actions from a secure environment using terminals and / or workstations they trust via secured connections to the TOE. They do not disclose their authentication credentials to others and securely transmit passwords they have generated for users to those users.
OE.AGENT	Those responsible for the TOE shall seek confidence that the runtime environment for an agent operates as specified and provides adequate protection measures against tampering with the agent and its interfaces.
OE.FEED	Those responsible for the TOE must ensure that the information provided by the IT environment that will be used for data import into the TOE allows proper association with the persons and their position in the organizational hierarchy as managed by the TOE.
OE.SERVER	Those responsible for the TOE must ensure that the TOE is protected against physical attack which might compromise IT security objectives. The underlying systems must be configured in a way that prevents unauthorized access to the TOE.
OE.USER	Those responsible for the TOE shall control the user community that can request access to resources protected by the TOE. This includes a configuration where the client systems allowed to submit requests to the TOE are controlled (e. g. a company internal network with a known and controlled user community protected against unauthorized access from external networks). Users must not disclose their authentication credentials to others.

5. IT Security Requirements

This chapter defines the security requirements for the TOE as well as for the IT environment.

Chapter 5.1 defines the security requirements for the TOE itself, separated into security functional requirements and security assurance requirements. Those requirements use the appropriate Common Criteria functional and assurance components. Operations have been performed where necessary to make sure that Security Targets derived from this PP meet the objectives of this PP. Selections and assignments performed have been marked in bold and italics. Iterations of security functional requirements have been marked by applying an additional identifier to the appropriate component names. Refinements have been marked in bold, italics and underlined. Operations to be performed by Security Target authors are enclosed in square brackets.

Chapter 5.2 defines the security requirements for the IT environment, separate for each component within the environment. The security functional requirements defined in this section try to identify a minimum set of requirements needed to provide for an IT environment that is able to support the TSF.

Application Notes have been applied where necessary to guide the ST author through the intention of the selected requirements.

5.1. TOE Security Requirements

5.1.1 TOE Security Functional Requirements

5.1.1.1 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:

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

b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and

c) ***the following auditable events:***

- ***person management***
- ***account management***
- ***policy administration***
- [assignment: *other specifically defined auditable events**, if any***].

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Application Note: The PP does not specify a detailed list of audit records that need to be generated by an Identity Management product. It is left to the ST author to determine security relevant actions within TOE operation and to refine the existing auditable events as deemed appropriate.

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,*** [assignment: ***other*** *authorized users****, if any***] with the capability to read ***all 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: It is permissible that a TOE allows other TOE users than those in the administrator role to view (subsets of) audit records, e.g. to establish the role of an auditor or to allow single TOE users to view audit records that relate to the person or account data of certain identities.

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.

5.1.1.2 User data protection

FDP_ACC.1 (ETC) Subset access control

FDP_ACC.1.1 (ETC) The TSF shall enforce the ***Provisioning Policy*** on

- ***persons as subjects,***
- ***services (representing managed resources) as objects and***
- ***the provisioning of accounts for a person on managed resources due to positive entitlement decision.***

Application Note: This SFR defines the subjects and objects mandated by the Provisioning Policy for the TOE. While this SFR has not been iterated in IMPP, an additional identifier has been added to the component name to allow better comprehension of SFR dependencies – all SFRs contributing to the Provisioning Policy are identified by (ETC).

FDP_ACC.2 (ACF) Complete access control

FDP_ACC.2.1 (ACF) The TSF shall enforce the ***TOE Access Control Policy*** on

- ***TOE users as subjects,***
- ***persons, services, entitlement rules, workflows, TOE users, access control information and audit data as objects***

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (ACF) The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Application Note: This SFR defines the subjects and objects mandated by the TOE Access Control Policy for the TOE. While this component has not been iterated in IMPP, an additional identifier has been added to the component name to allow better comprehension of SFR dependencies – all SFRs contributing to the TOE Access Control Policy are identified by (ACF).

FDP_ACF.1 (ACF) Security attribute based access control

FDP_ACF.1.1 (ACF) The TSF shall enforce the ***TOE Access Control Policy*** to objects based on ***administrator-specified access control information, user names and roles***.

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

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

FDP_ACF.1.4 (ACF) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application Note: This SFR defines the rules for the TOE Access Control Policy. The ST author shall specify TOE-specific access control rules. IMPP expects a discretionary access control in place but does not further mandate the explicit rules to be enforced.

FDP_ACF.1 (ETC) Security attribute based access control

FDP_ACF.1.1 (ETC) The TSF shall enforce the ***Provisioning Policy*** to objects based on ***entitlement rules, persons and person attributes indicating organizational relationships***.

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

- ***For each account provisioning initiated on a managed resource the corresponding person must be entitled to such an account on the corresponding service.***
- [assignment: ***additional*** *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects****, if any***].

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

FDP_ACF.1.4 (ETC) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application Note: This SFR defines the rules for the Provisioning Policy. The ST author may specify additional, TOE-specific rules for account provisioning.

FDP_ETC.2 (ETC) Export of user data with security attributes

FDP_ETC.2.1 (ETC) The TSF shall enforce the ***Provisioning Policy*** when exporting user data, controlled under the SFP(s), outside of the TSC.

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

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

FDP_ETC.2.4 (ETC) The TSF shall enforce the following rules when user data is exported from the TSC: ***user-defined provisioning workflows associated with an entitlement and the managed resource respectively;*** [assignment: *additional exportation control rules*].

Application Note: The provisioning of accounts on managed resources is considered export of user data: the Provisioning Policy invoked for the export of account data provides an entitlement decision – if a person is entitled to an account on the managed resource, the TOE exports the corresponding account data toe the managed resource via an agent. As outlined in chpt. 2 IMPP envisions additional workflows that can be specified by a TOE user or administrator and processed by the TOE as part of the provisioning (data export) function. The ST author may further specify such exportation control rules in addition to the entitlement rules implemented by FDP_ACF.1 (ETC).

5.1.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***an administrator configurable number of*** unsuccessful authentication attempts occur related to ***user authentication***.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of* ***restrictive*** *actions* ***to prevent successful brute force attacks***].

Application Note: As part of the required authentication mechanism, actions due to unsuccessful authentication attempts must be specified in the ST in order to avoid password guessing attacks. The number of unsuccessful authentication attempts may be refined to specify an exact amount of attempts.

FIA_ATD.1 (ACF) User attribute definition

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

- ***user name***
- ***authentication credentials***
- ***role memberships***
- [assignment: *list of **additional** security attributes**, if any***].

Application Note: This SFR fulfills a dependency introduced by FIA_USB.1 for the implementation of the TOE Access Control Policy. In addition to the security attributes that are used in the access control information, it is required that the TOE maintains authentication credentials to enforce authentication of users. The ST author may add additional security attributes that need to be maintained to support the TSP.

FIA_ATD.1 (ETC) User attribute definition

FIA_ATD.1.1 (ETC) The TSF shall maintain the following list of security attributes belonging to individual ***persons***:

- ***unique identifier***
- ***organizational relationships***
- ***account data***
- [assignment: *list of **additional** security attributes**, if any***].

Application Note: Using a DAC model for the implementation of the Provisioning Policy, IMPP consequently defines the security attributes related to the **persons** that are the subject of the entitlement decisions provided by this policy.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

Application Note: IMPP requires the ST author to define a quality metric for authentication credentials (e.g., passwords) to provide for a sufficient Strength of Function (SOF) of the mechanisms used to implement the authentication functionality.

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.

Application Note: This SFR implements the authentication functionality that is deemed necessary to support the enforcement of the TOE Access Control Policy and to provide for accountability of user actions.

FIA_UID.2 User identification before any action

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

Application Note: This SFR contributes to authentication of the TOE users.

FIA_USB.1 User-subject binding

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

Application Note: This SFR has been introduced to support the TOE Access Control Policy by ensuring that the subject created during login of a TOE user will be associated with the user names and roles that are used in the access control information to decide on access to objects mandated by the TOE Access Control Policy.

5.1.1.4 Security management

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***TOE Access Control Policy*** to restrict the ability to ***create, query, modify, delete*** [assignment: *other operations**, if any***] the security attributes ***related to persons, users, access control information, entitlement rules, services and workflows*** to ***administrators*** [assignment: ***additional*** *authorized identified roles**, if any**]*.

Application Note: This SFR requires the TOE Access Control Policy to be enforced to protect the management of security relevant data maintained by the TOE. The ST author may augment the list of relevant security attributes, e.g. if auditing is configurable in a TOE, and the list of authorized roles.

FMT_MSA.3 (ACF) Static attribute initialisation

FMT_MSA.3.1 (ACF) The TSF shall enforce the ***TOE Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (ACF) The TSF shall allow the [assignment: *the authorized identified roles]* to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TOE must not offer access to objects by default (an exception are administrators, who might not be subject to access control). Access has to be granted explicitly by specifying appropriate access control information. The ST author must specify the roles that are allowed to specify alternative initial values for access control information, if any.

FMT_MSA.3 (ETC) Static attribute initialisation

FMT_MSA.3.1 (ETC) The TSF shall enforce the ***Provisioning Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (ETC) The TSF shall allow the [assignment: *the authorized identified roles]* to specify alternative initial values to override the default values when an object or information is created.

Application Note: This SFR mandates restrictive default values for the application of the Provisioning Policy, in other words: entitlement rules must be specified explicitly and shall not by default entitle all persons managed by the TOE to accounts on all services. While the restriction to the authorized roles specified by the ST author for the management of alternative default values is enforced by the TOE Access Control Policy, the CC expect the policy to be specified in

FMT_MSA.3.1 for which the security attributes are applicable, i.e. the Provisioning Policy.

FMT_SMF.1 Specification of Management Functions

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

- ***management of access control information***
- ***management of entitlement rules***
- ***management of workflows, or additional exportation rules***
- ***management of persons***
- ***management of users***
- ***management of services (representing managed resources)***
- [assignment: *list of **additional** security management functions to be provided by the TSF**, if any***]

Application Note: Management of the TSF, subjects and objects maintained by the TOE and their security attributes must be provided by the TOE. The ST author may specify additional security management functions in accordance with TSP and TOE functional requirements, e.g. the configuration of auditing, if applicable.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***user, administrator*** [assignment: ***other*** *authorized identified roles**, if any***].

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

Application Note: All persons having an account on the TOE are actually considered users. An administrator role has been introduced by IMPP to provide for the potential of separation of TOE administration and other user-interaction with the TOE. The definition of roles in the ST shall not prevent the administrator-specified definition of further groups to ease maintenance of multiple users with the same access rights. The ST author may specify additional roles that need to be supported by the TOE.

5.1.1.5 Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Note: The TOE needs to protect the TSF from circumvention.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret ***person and account data*** 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:

- ***person data import:***
  If a person is already existent in the TOE data store, the imported person data must be associated with the matching person; otherwise it must be treated as data for a new person.
- ***account data import:***
  The TSF shall not associate imported account data with persons in the TOE data store if that account data cannot unambiguously be linked to a person.
- [assignment: *list of* ***additional*** *interpretation rules to be applied by the TSF****, if any***].

Application Note: While the PP does mandate interpretation rules in order to avoid misinterpretation of person and account data imported via external trusted sources, (e.g. a person already existent in the TOE data store is created twice due to a missing unambiguous link to the imported data, such as a Distinguished Name) it is not the intention of the PP to define how the imported data is handled by the TOE, and to what extent the import of data from trusted sources is supported by a TOE. This should be specified by the ST author. (E.g. data representing a new person could automatically be added to an organization or could be subject to prior approval functionality before being added to an organization.)

5.1.2 TOE Security Assurance Requirements

The target evaluation assurance level for the product is EAL3 augmented by ALC_FLR.1.

5.2. Security Functional Requirements for the IT Environment

This section contains two kinds of functional requirements:

a) Security functional requirements that must be fulfilled by the IT environment, namely the managed resources, to support the security functionality of the TOE.

b) Security functional requirements that are supportive to TSF and can be fulfilled by the IT environment or the TOE itself – since IMPP does not want to impose unnecessary restrictions on the implementation of an identity management solution, such requirements have been defined for the IT environment and may be moved by ST authors into the TSF domain.

Note: the security functional requirements have been refined according to [CC] Part 1 B.2.6 (modified by Interpretation 058) to indicate that the IT environment, not the TOE, must meet the requirements. Those refinements are identified by bold typesetting and not subject to the assessment requirements associated with modified CC components.

5.2.1 Managed Resources

The TOE provides account data to managed resources in concordance with the provisioning policies that apply for persons managed by the TOE.

This section will identify a SFR for

- ensuring that account data provided to managed resources is interpreted by the managed resource as intended by the TOE.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The **IT environment** shall provide the capability to consistently interpret ***account data*** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The **IT environment** shall use ***the following interpretation rules*** when interpreting the TSF data from **the TOE**:

- **The managed resource shall associate the data provided by the TOE by user name with the account data already existent on the managed resource.**
- **User name and other account data must be utilized by the managed resource without undetected modification.**
- **Account management requests issued by the TOE (e.g. create, modify, delete user) must be performed as requested.**
- [assignment: *list of **additional** interpretation rules to be applied by the TSF, **if any***].

Application Note: This SFR is intended to ensure that account data exported to a managed resource during provisioning is interpreted by the managed resource as expected – it is anticipated that the TOE in general has neither the possibility nor the responsibility to provide for the correct implementation on the managed resource in the IT environment. The ST author may specify additional interpretation rules for managed resources. These may be different for different managed resources, in which case the component should be iterated for each managed resource.

5.2.2 Repository

It is the assumption of this Protection Profile that the TOE uses a repository in the IT environment for storing TSF data and user data (e.g. audit data, persons, roles, policies, and accounts).

This section will identify SFRs for

- protecting the integrity of the stored data by requiring that the TOE, when accessing such data, needs to be authenticated

Please note that these functional requirements could also be fulfilled by the TOE itself, in which case the corresponding Security Target should list them as security functional requirements for the TOE instead of the IT environment.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The **IT environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The **IT environment** shall be able to ***prevent unauthorized*** modifications to the audit records.

Application-Note: This SFR contributes to the protection of audit data generated by the TOE. This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author needs to move it to the section listing the SFRs for the TOE and to reverse the applied refinement.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The **IT environment** shall allow ***actions that do not mediate access to or modification of TSF data and user data*** on behalf of the user to be performed before the user is authenticated.

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

Application-Note: This SFR requires authentication for users accessing the repository holding the TSF data and user data. It is expected that access to TSF data and user data of the TOE will not be granted to other entities than the TOE – if the repository in the IT environment serves multiple users and not only the TOE, an effective access control policy will have to be implemented in addition. This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author may delete it in favor of the requirement FIA_UAU.2 that has been selected for the TOE.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The **IT environment** shall allow ***actions that do not mediate access to or modification of TSF data and user data*** on behalf of the user to be performed before the user is identified.

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

Application-Note: Identification supports the authentication requirement for the repository in the IT environment. This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author may delete it in favor of the requirement FIA_UID.2 that has been selected for the TOE.

5.2.3 Secure Network Sessions

The TOE internal TSF data transfer, as well as the data transfer between the TOE and other trusted IT products (such as clients and external repositories), needs to be protected against unauthorized disclosure and modification of the transferred data. This may be done by implementation of an SSL / TLS layer in the IT environment or by otherwise appropriate protection of the network that is used to transfer TSF data and user data.

This section will identify SFRs for

- protecting the integrity and confidentiality of data transferred via network communication between TOE subsystems itself and between TOE subsystems and entities in the IT environment

Please note that these functional requirements could also be fulfilled by the TOE itself, in which case the corresponding Security Target should list them as security functional requirements for the TOE instead of the IT environment.

FPT_ITT.1 Basic internal TSF data transfer protection

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

Application-Note: This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author needs to move it to the section listing the SFRs for the TOE and to reverse the applied refinement.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The **IT environment** shall provide a communication channel between **the TOE** 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 **IT environment** shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The **IT environment** shall initiate communication via the trusted channel for ***transaction of all TSF data and user data***.

Application-Note: This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author needs to move it to the section listing the SFRs for the TOE and to reverse the applied refinement.

5.2.4 Runtime Environment of the TOE

The runtime environment for the TOE's audit record generation mechanism needs to provide a reliable time source in order to generate audit records. Also, in order to support the enforcement of TSF in the TOE, the runtime environment shall provide domain separation functionalities for the TOE's usage.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The **IT environment** shall maintain a security domain for **the TOE's** execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The **IT environment** shall enforce separation between the security domains of subjects in the **IT environment's scope of control**.

Application Note: This SFR is intended to support the reference mediation implemented by the TOE. If it is unclear whether the underlying abstract machine can provide a dedicated execution domain for the TOE, this requirement can be satisfied by operating the TOE on a dedicated and physically protected machine.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The **IT environment** shall be able to provide reliable time stamps for **the TOE's** use.

Application-Note: This security functional requirement may be fulfilled by the TOE instead of the IT environment. In this case, the ST author needs to move it to the section listing the SFRs for the TOE and to reverse the applied refinement.

6. PP Application Notes

The PP authors have added application notes to security functional requirements that

a) require further operations left to the ST author. In cases where this Protection Profile does not benefit from restricting the implementation of the TOE by performing SFR operations, it has been left to the ST author to perform those operations as he sees fit for the concrete TOE.

b) can be fulfilled by the TOE, although the PP states that the requirement is for the IT environment. In cases where experience has shown that it is not necessarily meaningful to provide certain supporting functionality within the TOE itself, appropriate requirements have been postulated for the IT environment. However, this should not prevent the ST author from including these requirements in the TOE instead.

The intended audience of the application notes throughout IMPP is the ST author. It is not required to reproduce the application notes that assist the ST author in interpreting the IMPP intention and performing operations on security functional requirements in an ST.

7. Rationale

This chapter provides the rationale for the selection of security objectives and requirements within this Protection Profile.

7.1. Security Objectives Rationale

7.1.1 Security Objectives Coverage

The mapping in Table 1 indicates how each security objective for the TOE is traced back to at least one threat or organizational security policy.

Objective	**Threat / OSP**
O.ACI	T.UNAUTHORIZED T.BYPASS
O.AUDIT	P.ACCOUNTABILITY T.BYPASS
O.FEED	P.FEED
O.I&A	P.ACCOUNTABILITY T.UNAUTHORIZED
O.PROVISION	P.PROVISION

Table 1: security objectives traced back to threats and organizational security policies

The mappings in Table 2 and Table 3 indicate how each security objective for the environment is traced back to at least one assumption, threat or organizational security policy.

Objective (IT Environment)	**Threat / OSP / Assumption**
OE.AUDIT	P.ACCOUNTABILITY
OE.COM_PROT	T.COM_ATT
OE.ENFORCEMENT	T.BYPASS
OE.MANAGED	P.PROVISION
OE.REPOSITORY	A.REPOSITORY P.ACCOUNTABILITY

Table 2: security objectives for the IT environment traced back to threats, organizational security policies and assumptions

Objective (non-IT Environment)	**Threat / OSP / Assumption**
OE.ADMIN	A.ADMIN
OE.AGENT	A.AGENT
OE.FEED	P.FEED
OE.SERVER	A.PHYS_PROT A.SERVER

Objective (non-IT Environment)	Threat / OSP / Assumption
OE.USER	A.USER

Table 3: security objectives for the non-IT environment traced back to threats, organizational security policies and assumptions

7.1.2 Security Objectives Sufficiency

The following arguments provide justification that the security objectives are suitable to counter each single threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

T.BYPASS	O.ACI requires that all client requests be subject to authorization before they are performed, therefore contributing to the sufficient mitigating the threat of bypassing security functions. O.AUDIT provides additional mitigation by providing a mechanism to administrators for reviewing security-relevant activities executed by the system, allowing them to detect the unauthorized execution of functions. This is supported by requiring a trusted execution domain for the TOE in the IT environment in OE.ENFORCEMENT.
T.COM_ATT	OE.COM_PROT requires the protection of communication in order to remove the threat of disclosure of or tampering with TSF data and user data.
T.UNAUTHORIZED	O.ACI required the implementation of an authorization mechanism in order to control access to resources protected by the TOE on a need-to-know basis. This is supported by requiring authentication of users in O.I&A.

Table 4: sufficiency of objectives countering threats

The following arguments provide justification that the security objectives are suitable to cover each single organization security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

P.ACCOUNTABILITY	O.I&A provides the means of uniquely identifying (and authenticating) users in a way that makes audit records traceable to single users. O.AUDIT establishes accountability of requested transactions by requiring the generation of appropriate audit records for such transactions and the functionality to make these audit records available to authorized users. OE.REPOSITORY supports the protection of audit records stored in repositories in the IT environment. OE.AUDIT supports the generation of audit records by providing a reliable time source.
P.FEED	O.FEED requires that the TOE offers a consistent way of relating imported user data to data already present in the TOE data store. OE.FEED covers the assumption on proper management of data

	in external data feeds that are used as sources for the TOE by requiring that such data is managed in a way that can be used for data import.
P.PROVISION	O.PROVISION requires the establishment of entitlements for persons in order to be subject to account provisioning on managed resources. OE.MANAGED requests consistent interpretation of account data provided to managed resources.

Table 5: sufficiency of objectives implementing OSPs

The following arguments provide justification that the security objectives for the environment are suitable to cover each single assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

A.ADMIN	OE.ADMIN covers the assumption on administrators that are non-hostile and abide by the instructions provided, by requiring that administrators for the TOE show such qualities. They will also protect passwords as assumed.
A.AGENT	OE.AGENT covers the assumption that the managed resources interact as specified with the TOE's agents and protect the agent against tampering by requiring that this is ensured in the IT environment.
A.PHYS_PROT	OE.SERVER requires that the TOE is physically protected, thus covering the corresponding assumption.
A.REPOSITORY	OE.REPOSITORY covers the assumption on TSF data and user data protection by the repository in the IT environment by requiring identification and authentication for the repository.
A.SERVER	OE.SERVER requires a configuration and operation of the TOE that protects the TOE from unauthorized access.
A.USER	OE.USER covers the assumption on non-hostile users which protect their passwords by requiring a controlled user community having access to the TOE.

Table 6: sufficiency of objectives covering assumptions

7.2. Security Requirements Rationale

This chapter provides the rationale for the selection of security requirements. In addition to this rationale, chapter 5 includes application notes for several security functional requirements to further improve the interpretation of those requirements with respect to a PP-conformant implementation of the TOE.

7.2.1 Security Requirements Coverage

The following tables illustrate which security objectives are implemented by which security functional requirements. Table 7 indicates how each TOE security functional requirement can be traced back to at least one security objective for the TOE, Table 8 indicates how each functional security requirement for the IT environment can be traced back to at least one security objective for

the environment.

SFR	Objective
FAU_GEN.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FAU_SAR.1	O.AUDIT
FAU_SAR.2	O.AUDIT
FDP_ACC.1 (ETC)	O.PROVISION
FDP_ACC.2 (ACF)	O.ACI
FDP_ACF.1 (ACF)	O.ACI
FDP_ACF.1 (ETC)	O.PROVISION
FDP_ETC.2 (ETC)	O.PROVISION
FIA_AFL.1	O.I&A
FIA_ATD.1 (ACF)	O.ACI O.I&A
FIA_ATD.1 (ETC)	O.PROVISION
FIA_SOS.1	O.I&A
FIA_UAU.2	O.I&A
FIA_UID.2	O.I&A
FIA_USB.1	O.AUDIT O.I&A
FMT_MSA.1	O.ACI O.PROVISION
FMT_MSA.3 (ACF)	O.ACI
FMT_MSA.3 (ETC)	O.PROVISION
FMT_SMF.1	O.ACI O.I&A O.PROVISION
FMT_SMR.1	O.ACI O.PROVISION
FPT_RVM.1	O.ACI O.AUDIT
FPT_TDC.1	O.FEED O.PROVISION

Table 7: SFRs for the TOE traced back to objectives for the TOE

SFR (environment)	Objective (environment)
Managed Resources	
FPT_TDC.1	OE.MANAGED
Repository	
FAU_STG.1	OE.REPOSITORY
FIA_UAU.1	OE.REPOSITORY
FIA_UID.1	OE.REPOSITORY
Secure Network Sessions	
FPT_ITT.1	OE.COM_PROT
FTP_ITC.1	OE.COM_PROT
Runtime Environment of the TOE	
FPT_SEP.1	OE.ENFORCEMENT
FPT_STM.1	OE.AUDIT

Table 8: SFRs for the environment traced back to objectives for the environment

7.2.2 Security Requirements Sufficiency

The following arguments provide justification for each security objective for the TOE, showing that the TOE security functional requirements are suitable to meet and achieve the security objectives.

O.ACI requires that only authorized users gain access to TOE resources, and that access can be controlled based on access control information. This objective is achieved by imposing the TOE Access Control Policy in *FDP_ACC.2 (ACF)*, which is specified in *FDP_ACF.1 (ACF)*. This SFP covers, according to *FMT_MSA.1*, access to the management of security attributes. Security attributes required to enforce access control are defined in *FIA_ATD.1 (ACF)*. Restrictive default values for the SFP are defined in *FMT_MSA.3 (ACF)*, while the management of the SFP is ensured by *FMT_SMF.1*. The administrator role defined in *FMT_SMR.1* supports the definition of the SFP, which in turn states that administrators are not subject to access control (i.e. they are granted access to all objects). The authorization functionality modeled in these SFRs contributes to the implementation of TSP enforcement required in *FPT_RVM.1*.

O.AUDIT requires that the status of security relevant transactions is recorded by means of audit records. This is achieved by implementing the generation of audit records and the specification of auditable events in *FAU_GEN.1*. The generation of audit records is supported by *FAU_GEN.2* and *FIA_USB.1*, allowing a proper association of audit records with users. *FAU_SAR.1* contributes to O.AUDIT by implementing functionality for reviewing audit records, which can be restricted by means of access control (*FAU_SAR.2*). The audit functionality modeled in these SFRs contributes to the implementation of TSP enforcement required in *FPT_RVM.1*.

O.FEED requires that person data imported via external data feed or from remote resources is properly associated with data already existing in the TOE. This objective is achieved by *FPT_TDC.1* requiring consistent interpretation of data shared between the TOE and other trusted IT products.

O.I&A requires users to be authenticated by the TOE. This objective is achieved by requiring authentication in *FIA_UAU.2*, which in turn is enabled by means to identify single users (*FIA_UID.2*). The quality of the credentials used for authentication is ensured by *FIA_SOS.1*. To allow a proper relationship between authenticated users and their representation in the TOE, *FIA_USB.1* establishes a user-subject binding. Authentication credentials are security attributes in

terms of the TSF according to *FIA_ATD.1 (ACF)*, management is provided by *FMT_SMF.1*. *FIA_AFL.1* provides means to prevent the authentication mechanism from misuse through brute force attacks.

O.PROVISION requires that accounts are provisioned only to persons that are entitled to the corresponding service, and that account information is properly associated with these persons. This is achieved by implementing the Provisioning Policy defined in *FDP_ACC.1 (ETC)*, which is applied to the export of account data (Provisioning) in *FDP_ETC.2 (ETC)* and specified in *FDP_ACF.1 (ETC)*. Management of this SFP (*FMT_SMF.1*) is restricted to authorized users by the TOE Access Control Policy as in *FMT_MSA.1*. Security attributes for the enforcement of the Provisioning Policy are defined in *FIA_ATD.1 (ETC)*. Restrictive default values for the definition of the Provisioning Policy are provided in *FMT_MSA.3 (ETC)*. Consistent interpretation of the data provisioned to managed resources, as far as the TOE is concerned, is provided by *FPT_TDC.1*.

The following arguments provide justification for each security objective for the IT environment, showing that the security functional requirements for the IT environment are suitable to meet and achieve the security objectives:

OE.AUDIT requires the provision of a reliable time source for audit generation. This is achieved by requiring a reliable time source in *FPT_STM.1*.

OE.COM_PROT requires the protection of communication between TOE parts and between TOE parts and external entities in order to ensure the integrity and confidentiality of transferred data. This is achieved for TOE internal transfer by *FPT_ITT.1* and by requiring a trusted channel in *FTP_ITC.1* for inter-TSF communication.

OE.ENFORCEMENT requires a dedicated execution domain for the TOE, which is satisfied by *FPT_SEP.1* introducing domain separation for the runtime environment of the TOE in order to protect the TOE from untrusted subjects.

OE.MANAGED requires interpreting data on managed resources that is provided by the TOE during account provisioning in a consistent fashion. This is implemented by defining appropriate interpretation rules in *FPT_TDC.1*.

OE.REPOSITORY requires the repositories used for TSF data and user data storage to protect such data. This is achieved by implementing authentication as in *FIA_UAU.1* and identification as in *FIA_UID.1*. The explicit objective to protect audit records against unauthorized deletion is implemented by *FAU_STG.1*.

7.2.3 Security Requirements Dependencies

The following tables show the fulfillment of dependencies imposed on security functional requirements by Part 2 of the Common Criteria (the left column identifies the CC Part 2 component, the middle column identifies the dependencies on that component drawn from CC Part 2, and the right column illustrates how the dependency is fulfilled in IMPP). No additional dependencies exist for the security functional requirements in IMPP.

Dependencies within the EAL3 “package” selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed again here. The included component on flaw remediation, ALC_FLR.1, has no dependencies on other requirements.

The security functional requirements in IMPP do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in IMPP introduce dependencies on any security functional requirement.

SFR	Dependencies	Fulfillment of dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1 (Environment)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1 (ETC)	FDP_ACF.1	FDP_ACF.1 (ETC)
FDP_ACC.2 (ACF)	FDP_ACF.1	FDP_ACF.1 (ACF)
FDP_ACF.1 (ACF)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 (ACF) FMT_MSA.3 (ACF)
FDP_ACF.1 (ETC)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 (ETC) FMT_MSA.3 (ETC)
FDP_ETC.2 (ETC)	[FDP_ACC.1 FDP_IFC.1]	FDP_ACC.1 (ETC)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1 (ACF)	%	%
FIA_ATD.1 (ETC)	%	%
FIA_SOS.1	%	%
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	%	%
FIA_USB.1	FIA_ATD.1	FIA_ATD.1 (ACF)
FMT_MSA.1	[FDP_ACC.1 FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 (ACF) FMT_SMR.1 FMT_SMF.1
FMT_MSA.3 (ACF)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MSA.3 (ETC)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	%	%
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RVM.1	%	%
FPT_TDC.1	%	%

Table 9: Dependency Analysis for TOE SFRs

SFR	Dependencies	Fulfillment of dependencies
FPT_TDC.1	%	%

Table 10: Dependency Analysis for the Managed Resources in the IT environment

SFR	Dependencies	Fulfillment of dependencies
FAU_STG.1	FAU_GEN.1	FAU_GEN.1 (TOE)
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	%	%

Table 11: Dependency Analysis for the Repository in the IT environment

SFR	Dependencies	Fulfillment of dependencies
FPT_ITT.1	%	%
FTP_ITC.1	%	%

Table 12: Dependency Analysis for Transaction Security in the IT environment

SFR	Dependencies	Fulfillment of dependencies
FPT_SEP.1	%	%
FPT_STM.1	%	%

Table 13: Dependency Analysis for the Runtime Environment of the TOE in the IT environment

7.2.4 Internal Consistency and Mutual Support

Chapter 7.2.2 has already shown how the IT security requirements work together to implement the single objectives for the TOE and the IT environment. This chapter will elaborate on the internal consistency and mutual support of the IT security requirements. Further information can as well be found in the application notes to the security requirements in chapter 5.

Internal Consistency and Mutual Support of Security Functional Requirements for the TOE

The TOE's main purpose is Identity Management, i.e. managing a large base of person information and provisioning accounts on services to persons that are entitled to use them.

Management of the user (and TSF) data is restricted by the **TOE Access Control Policy** implemented by *FDP_ACC.2 (ACF)* and defined in *FDP_ACF.1 (ACF)*. *FMT_SMR.1* introduces the role of an administrator, whose access is – according to *FDP_ACF.1 (ACF)* – not further restricted by the access control SFP.

In order to enforce access control for the TOE, users are required to **identify and authenticate** themselves in *FIA_UID.2* and *FIA_UAU.2*. The credentials used for authentication are subject to quality requirements that can be defined in *FIA_SOS.1*. Brute force attacks against the authentication mechanism are prevented by *FIA_AFL.1* Actions of users within the system are tied to specific users by user-subject binding as in *FIA_USB.1*.

Actions requested by users are subject to **auditing** as defined in *FAU_GEN.1*. Audit records are associated with users as in *FAU_GEN.2* and *FIA_USB.1*. The TOE offers functionality to review audit records (*FAU_SAR.1*) for authorized users (*FAU_SAR.2)*.

Person data that is derived from external sources is subject to consistent interpretation of the data in

accordance with the interpretation rules specified in *FPT_TDC.1*.

The Provisioning itself, i.e. the export of user data to the managed resources based on the decision whether a person is entitled to an account on the managed resource, is subject to a **Provisioning Policy** as implemented by *FDP_ACC.1 (ETC)* and described in *FDP_ACF.1 (ETC)*. It is applied to the export of user data by *FDP_ETC.2 (ETC)*. In addition, FPT_TDC.1 supports the consistent interpretation of account data exchanged with managed resources during provisioning.

The **management of security attributes** for the Security Functional Policies described above – as part of the security management functions defined in *FMT_SMF.1* – is itself subject to the TOE Access Control Policy, as required by *FMT_MSA.1*. Restrictive default values for all policies are required in *FMT_MSA.3 (ACF)* and *FMT_MSA.3 (ETC)*. The security attributes maintained by the TOE for users and persons are defined in *FIA_ATD.1 (ACF)* and *FIA_ATD.1 (ETC)*.

Bypass prevention for the TSF is offered by *FPT_RVM.1*.

Internal Consistency and Mutual Support of Security Functional Requirements for the IT Environment

The IT environment for the TOE offers supportive mechanisms for the security functionality of the TOE.

It must be ensured that the data presented to **managed resources** by the TOE as part of the provisioning functionality will be consistently interpreted by the managed resources. FPT_TDC.1 specifies appropriate interpretation rules.

The generation of audit records by the TOE requires a reliable time source – such is provided by the **Runtime Environment** as required in *FPT_STM.1*. In addition, the underlying machine provides protection of the TOE by offering a dedicated execution domain for it in *FPT_SEP.1*.

TSF data and user data is stored in **external repositories**, which are required to implement identification (*FIA_UID.1*) and authentication (*FIA_UAU.1*) for their users in order to make sure that only the TOE is able to access its data. In addition, audit records stored in the repositories have to be protected against unauthorized modification (*FAU_STG.1*).

Network communication between the TOE subsystems, as well as between the TOE and external entities, requires protection against disclosure and modification of TSF data and user data – this is required for TOE internal transfer by *FPT_ITT.1* and for external communication by *FTP_ITC.1*.

7.2.5 Evaluation Assurance Level and Strength of Function

The evaluation assurance level (EAL) 3 was chosen as a medium level of assurance reflecting the expected assurance requirements of commercial customers using the target of evaluation (TOE) for the protection of data with a low or medium level of sensitivity. The TOE is intended to provide a reasonable level of protection for this data comparable to the protection provided by most commercial-off-the-shelf operating system products. This is reflected as well in the definition of the TOE environment in chpt. 2 and the security objectives for the TOE in chpt. 4 of IMPP.

The assurance level EAL3 was augmented with ALC_FLR.1 to address the flaw remediation process that is part of the Mutual Recognition Arrangement. Since the evaluation methodology for ALC_FLR.1 has been harmonized, this was considered a useful augmentation for the assurance level chosen.

The PP claims for the functions provided by the TOE that are subject to probabilistic or permutational analysis a medium strength (SOF-medium) as a minimum. This allows resistance against attackers with a moderate attack potential.

A. Appendix

A.1 Definition of Terms

Access Control Information	Controls user access by defining the access privileges of a user or group. An ACI grants or denies the ability to initiate user and management functions.
Account	Object that represents the information defined for a user, or identity, within the context of a managed resource. This information may be security and/or profile characteristics for the user specific to the resource.
ACI	Access Control Information
Administrator	A user who is authorized to initiate administrative action.
Agent	Software module that is part of the TOE, but distributed remotely from the central TOE business logic as the part of a connector that interacts directly with the managed resource (service). The module implements the connector commands by translating them in to resource specific commands.
Assets	Information or resources to be protected by the countermeasures of a TOE.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
EAL	Evaluation Assurance Level
Element	An indivisible security requirement.
Entitlement	A construct to define a set of permissions, or privileges, on a managed resource. This construct will be organized into a provisioning policy to grant those permissions to a set of persons.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Extension	The addition to an ST or PP of functional requirements not contained in Part2 and/ or assurance requirements not contained in Part 3 of the CC.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Group	A construct representing a number of defined users, which are the members of the group.
Identity	See Person.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Iteration	The use of a component more than once with varying operations.
Managed Resource	An item that can be owned or accessed by a set of identities. This resource will be represented as a service in the TOE. Provisioning policies will entitle the appropriate identities to ownership of, or access to, a resource. Agents enforce the entitlements on the resources.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Person	Object within the TOE representing a human or computing entity that is being managed, or controlled, and audited. Persons can be entitled (by a Provisioning Policy) to use services in the IT environment.
PP	Protection Profile
Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Protection Profile	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Provisioning Policy	A Provisioning Policy grants permissions to persons by entitling them to have accounts on dedicated remote services in the IT environment.
Refinement	The addition of details to a component.
Resource	Also: Remote Resource. See Managed Resource.
Secret	Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
Security attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Security Function	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.
Security Target	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection	The specification of one or more items from a list in a component.
Service	A service represents the definition of a managed resource that is known to the TOE.
SF	Security Function
SFP	Security Function Policy
SOF	Strength of function
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SSL	Secure Socket Layer.
ST	Security Target
Strength of function	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.
Subject	An entity within the TSC that causes operations to be performed.
System	A specific IT installation, with a particular purpose and operational environment.
Target of evaluation	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE	Target of evaluation
TOE data store	TSF data and user data maintained by the TOE.
TOE resource	Anything useable or consumable in the TOE.
TOE security functions	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Functions Interface	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
TSC	TSF scope of control
TSF	TOE security functions
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF scope of control	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

TSFI	TSF Interface
TSP	TOE Security Policy
User data	Data created by and for the user that does not affect the operation of the TSF.
IT	Information Technology

END OF DOCUMENT