Tivoli software

IBM

IBM Tivoli Identity Manager 4.6
Security Target

BSI-DSZ-CC-0237

Version Number 1.41

Date: January 12, 2006

Status: Final

Author: David Ochel

Owner: Brian Matthiesen

Table of Contents

Figures

Tables

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 Security Target Document are:

Area	Approver Name	Date Approved
Product Testing	Brian Matthiesen	

Approval is by formal review.

History

Version	Date	Summary of Changes
1.00	October 31st, 2003	First complete release; incorporates draft comments from ITSEF, CB, and internal review. Submitted for formal evaluation.
1.01	November 4th, 2003	Clarified A.GLOBAL_SECURITY. Added JCE to the J2EE provided services.
1.10	December 16th, 2003	Updated references. Incorporated comments from Tony Gullotta. Minor clarifications. Re-structured chpts 2 and 3 after discussion with ITSEF and CB. Added Reporting, ad-hoc Reporting and Reporting ACIs. Moved references and glossary to Appendix. Added philosophy to chpt. 1.
1.11	December 17th, 2003	Incorporated feedback from formal evaluation. Added tables of figures and tables. Formatting improvements.
1.20	January 29th, 2004	Achieved IMPP compliance.
1.30	February 18th, 2004	Implemented IMPP modifications.
1.31	July 2, 2005	Removed FAU_SAR.3.
1.32	July 12, 2005	Updated sections 2.7 and 2.8 to reflect correct version numbers.
1.33	July 23, 2005	Changed Access Control Informations to Access Control Items. Changed conformance claim to CC 2.2. Updated version number for PP reference.
1.34	August 15, 2005	Adopted ITIM 4.6 terminology “adapter” instead of “agent”. Modified T.UNAUTHORIZED in 3 to match updated PP. Changed IMPP reference in 7 to 1.14. Resolved wrong adapter identification in 2. Editorial changes in 2.5.
1.35	September 02, 2005	Updated adapter versions and names in 2.7; updated figures 2 and 3 to display adapters; changed examples that were tailored to Win2k throughout document; updated definition of terms in Appendix A.
1.36	October 11, 2005	Removed inconsistency in 6.1.1.

1.37	October 17, 2005	Updated A.2.
1.38	October 19, 2005	Editorial updates.
1.39	October 20, 2005	Removed FIA_SOS.2. Ensured consistency with latest version of IMPP, including the split of FIA_ATD.1 in two iterated SFRs. Editorial changes.
1.40	January 04, 2006	Addressed CB comments.
1.41	January 12, 2006	Clarification on threats.

1. Security Target (ST) Introduction

This document defines the Security Target (ST) for the Common Criteria (CC) Evaluation of IBM Tivoli Identity Manager 4.6 developed by IBM.

1.1. ST Identification

Title: IBM Tivoli Identity Manager 4.6 Security Target Version 1.41 Status: Final

Keywords: Identity Management, TIM, ITIM, IMPP

This document is the Security Target for the Common Criteria evaluation of IBM Tivoli Identity Manager (ITIM) 4.6 provided by IBM Inc. for a Common Criteria evaluation. It is conformant with the Identity Management Protection Profile.

1.2. ST Overview

The target of evaluation (TOE) is the IBM Tivoli Identity Manager (ITIM) 4.6. This Security Target describes the TOE, its boundary, IT environment, IT security requirements and security functions.

IBM's Tivoli Identity Manager provides the software and services needed for deploying policy-based provisioning solutions. Tivoli Identity Manager helps companies automate 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.

People are organized in business units, which are part of a hierarchical structure: Organizations may contain subsidiary entities such as Organizational Units, Business Partner Organizations, and Locations. Organizational Roles are used to group people according to their function in the Organization. Services represent different types of managed resources such as Oracle databases, Windows machines, etc.. An Organizational Role can be linked to Services by means of Provisioning Policies, entitling persons in the Organizational Roles to an account on the managed resource that is linked to that Service.

ITIM Groups, which allow access to the central Tivoli Identity Manager Server, are granted rights within Tivoli Identity Manager by the use of Access Control Item (ACI), and people are assigned to ITIM Groups to allow them to use those granted rights (e.g. management of accounts by users, and management of Organizations and Policies by administrators).

The TOE provides the following identity management security functionality:

- provisioning of user account information to remote services
- import and management of person, or identity, 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

1.3. CC Conformance Claim

The evaluation is based upon the Common Criteria [CC] and Common Evaluation Methodology [CEM].

This Security Target claims the following CC conformance:

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

This Security Target claims conformance to the following PP:

Identity Management Protection Profile, Version 1.14 as of 2005-08-11. Registration ID: n/a.

1.4. Strength of Function

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

1.5. Rationale for the Selection of the 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 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 identity provisioning products.

In line with this medium level of assurance the functions provided by the TOE that are subject to probabilistic or permutational analysis are claimed to have a medium strength (SOF-medium).

1.6. Philosophy

Security is a trade-off. IBM Tivoli Identity Manager (ITIM) is a complex product that allows customer-specific extensions and replacements of existing functionality in many places and relies heavily on the services provided by the J2EE framework for its operation. To allow a Common Criteria evaluation of any product, its security functions need to be unambiguously specified. Functional tests have to be performed to verify these functions in all supported configurations. Setups and configurations that introduce vulnerabilities must be avoided.

The Common Criteria evaluation and certification of IBM Tivoli Identity Manager is a trade-off between ITIM's flexibility, the need to specify a dedicated evaluated configuration in order to narrow down the behavior of the assessed security functionality and to encounter threats that cannot be addressed by ITIM itself, and last but not least the efforts that are required to analyze and test the possible setups and configurations of the Target of Evaluation. In other words, the supported configurations of ITIM that have been specified for its evaluation are a trade-off between all possible scenarios of use that are functionally supported by the product and the amount of time required to evaluate the product in all of these scenarios, plus the exclusion of scenarios that would not withstand the vulnerability assessment that is part of the evaluation.

This Security Target specifies the evaluated configuration, security functions and the intended operational environment for ITIM as basis for an evaluation. The evaluated configuration is as well reflected in the IBM Tivoli Identity Manager Common Criteria Guide, which provides hands-on advice on how to operate the product in the evaluated configuration. IBM has taken great care to define an evaluated configuration that allows the usage of ITIM in a large number of customer scenarios. However, it is acknowledged that for the initial evaluation certain restrictions have been imposed (such as the support of only a limited number of available adapters for managed resources). Comments on and discussion of the evaluated configuration with respect to the certification of future releases of IBM Tivoli Identity Manager are therefore greatly appreciated.

2. TOE Description

The TOE is software only. The TOE consists of IBM Tivoli Identity Manager (ITIM) Server, ITIM Oracle Database Adapter for Windows, and ITIM Windows AD Adapter

The following sections provide a description of the structure of the TOE and the TOE boundary, and an overview of the 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. In large computer networks operated by organizations with a huge number of employees, an employee typically will need accounts on several operating systems and applications provided by the network infrastructure. Not only is it a significant effort to administrate the accounts for each of those systems separately (imagine a distributed operating system, an email system, a work flow application, a collaboration solution), but also processes must be cultivated within the organization to cope with modifications in case of new or leaving employees to reflect the current employment status on all systems that provide accounts for such users. Last but not least, employees have to maintain passwords for all their accounts throughout the organization.

The IBM Tivoli Identity Manager (ITIM) provides a solution for central management of users and their accounts on the different systems in a network. First, each employee of an organization is represented by an identity within the ITIM server. Next, ITIM has a way of interacting with services (i.e. the systems) in a network infrastructure to manage accounts on these services. This interaction is provided by ITIM connectors that direct the management of accounts to so-called adapters: software that sits either directly on the remote system, e.g. on the operating system, interacting with the user management mechanisms of the operating system, or on a central adapter server with network interfaces to the managed system. By defining within ITIM which identity shall have access to which of the services managed by ITIM, ITIM is able to provide appropriate information for account creation for that identity to each of these services, or managed resources. This is called Provisioning.

Basically, identities within ITIM are managed by membership of Organizational Roles and ITIM Groups:

- Organizational Roles

  Identities within ITIM can be grouped by membership to Organizational Roles, or roles. Such Organizational Roles are intended to reflect the roles that exist within an organization that uses ITIM for identity management.

  Organizational Roles are used by Provisioning Policies to determine which identities shall have

accounts on which managed resources. A Provisioning Policy defines a number of services and attributes a user shall have on these services (e.g. membership of groups on the service) and is associated with dedicated Organizational Roles.

By adding an identity to an Organizational Role, this identity is subject to the Provisioning Policies referring to this role and therefore to the creation (or modification, deletion) of accounts on the services defined within these policies. Granting access to services is referred to as Entitlement.

- ITIM Groups

  An identity may be member of an ITIM Group, or group. This requires an identity to be entitled to the ITIM service, i.e. to have an account on the ITIM server (this is not the case per se for the identities managed by ITIM). ITIM Groups specify the kind of access a user has on ITIM. Fine grained access control is then performed by evaluating ACIs (Access Control Item, i.e. ITIM-specific access control policies) that delegate specified rights to ITIM Groups.

  In most environments, all identities will be members of an ITIM Group that delegates the right to change account passwords via the web-based user interface provided by the ITIM server to its members, whereas the modified password will then be provided by way of connectors to all managed resources the identity has an account on. Only dedicated identities will belong to ITIM Groups that delegate the right of system administration or Organizational Role management to these users. Membership of the pre-defined Administrator group exempts an user from all access control on the ITIM server.

Note: while ITIM provides the necessary functionality to provision accounts to managed resources, i.e. to provide a service with the necessary information to create an account and to trigger this creation, the enforcement of (security) functionality on the managed resources for such an account is by nature left to the managed resource.

2.2. Organizations and Policies

The basic purpose of Identity Manager is to provide a delegable and scalable way of policing and provisioning a large body of identities with privileges on multiple heterogeneous resources.

Before a person can be associated with ITIM Groups or Organizational Roles, there needs to exist an identity in ITIM representing the person. Upon creation, identities are assigned to an Organization or subordinated elements within a organization tree (i.e. business units). ITIM provides the concept of Organizations, which can be organized on lower hierarchies by defining Locations, Organizational Units, Administrative Domains, and Business Partner Organizations (see section 2.3 for additional details).

The arrangement of identities within these organizational elements provides some additional implications:

- A customer can reflect his own organization by emulating an appropriate hierarchy within ITIM.
- Administrative Domains can be used to define object spaces that can be managed by assigned domain administrators – such administrators are restricted to manage only what is within their administrative domain.
- Supervisors for organizational branches can be defined for the approval of requests within ITIM (this relates to the concept of managers in an organization).

In addition to assigning identities to organizational elements, identities can also be categorized through the concept of an Organizational Role (see section 2.1). This eliminates having to administer privileges on a per individual basis. ITIM distinguishes between static and dynamic Organizational Roles:

- Static Organizational Roles are available globally; any person can be added as a member of a static Organizational Role. Assigning a person to a static Organizational Role is a manual process. Persons can be added to a static Organizational Role's membership manually, through the person's detailed information. Users can also be added through an Identity Feed.
- A Dynamic Role has a matching rule specified that uses Lightweight Directory Access Protocol (LDAP) filters to determine which identities belong to the Dynamic Role. The system automatically manages the membership list of the Dynamic Role based on this matching rule. Dynamic Roles can be targeted to organizational entities, while static Organizational Roles are globally available throughout ITIM and are assigned manually to identities.
- Dynamic Organizational Roles allow placement of persons into specific roles based on valid LDAP filters. Dynamic Organizational Roles are evaluated whenever new persons are added to the system or a person's personal information changes. Dynamic Organizational Roles apply to any container at any level depending on the scope defined for the dynamic Organizational Role within the organizational tree.

The resources in an IT environment that Identity Manager is providing provisioning for are represented as Services (cf. section 2.1). When an identity is provisioned access to a Service, an Account creation is triggered on the service (i.e. the managed resource in the IT environment) to represent the association. An account may have a password associated with it. Identity Manager provides the possibility to manage (e.g. create, modify) passwords for all accounts on the services a user is entitled to.

In order to complete the goal of scalable policing and provisioning, the concept of a Provisioning

Policy exists to associate multiple Organizational Roles with possibly multiple Services. The association is made through an Entitlement which specifies the service (and permissions on that service) on which the identities within the listed roles are granted an account. At any time a provisioning request is made for an identity against a Service (e.g. to create an account on that service), the relevant Provisioning Policies are evaluated and enforced. An Entitlement can also be defined as automatic. ITIM will automatically provision that identity with an account and the correct privileges, in opposite to a manual entitlement, where the person (or another user authorized to do so on the person's behalf, e.g. an administrator) manually creates a request (via the ITIM user interface) to trigger account generation on a service the person is entitled to. The system can also retrieve account information from a managed resource, or Service, so that it can police any changes that have been made at the managed resource without ITIM's knowledge (e.g. if access rights or group memberships on the managed resources have been altered on the resource directly, ITIM will be able to notice this, and – if necessary – to re-enforce the Provisioning Policy).

To provide delegable administration of these concepts, the system has a comprehensive authorization engine. This engine follows rules, named Access Control Item (ACI), which can be defined by administrators (cf. section 2.1). These ACIs can be defined to provide just the right users of the system with discrete permissions on the objects described above.

In addition, ITIM provides the concept of

- Service Selection Policies that may be referenced from Provisioning Policies for dynamic provisioning of services to identities based on certain identity attributes.
- Identity Policies to specify naming schemes for user IDs for accounts created on services.
- Password Policies to define global or service specific password constraints.
- Workflows to enhance the Provisioning of accounts on a Service, e.g. by requesting management (supervisor) approval for an account creation that has been requested for an entitled person.

2.3. Administrative Overview

The following is a basic overview of how the Tivoli Identity Manager system works.

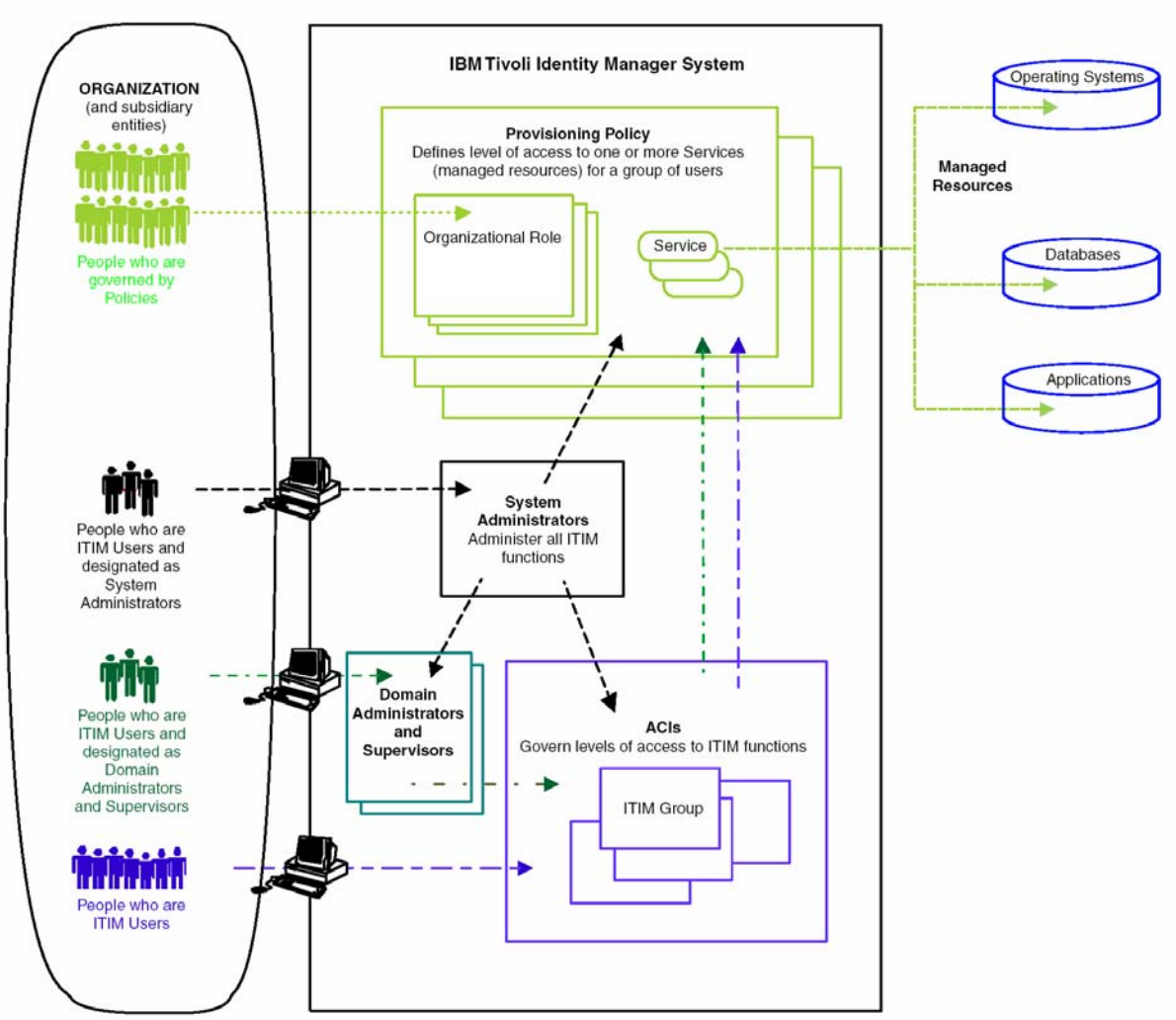

Figure 1: Administrative view of the TOE

People are added by administrators to Organizations or organizational entities below an Organization. They are then known to the TOE as persons, without the implication that they have an account to access the TOE. People can be added via an Identity Feed, or HR Feed, i.e. an interface for automated import of identities from human resource management software, which allows the import of identities that are already defined in an organization as persons into the TOE.

Accounts can be created for persons known to the TOE. This may be an account for the TOE (i.e. ITIM itself) or another Managed Resource (i.e. a service in the IT environment).

A person can be assigned to an Organizational Role, which in turn may entitle the person to access to Managed Resources through a corresponding Provisioning Policy, which allows automatic or manual provisioning of accounts for the person on the Managed Resources.

The people managed by a Tivoli Identity Manager system are grouped into one or more Organization entities that can contain subsidiary entities, such as Organizational Units, Locations, and Business

Partner Organizations, all in a parent-child relationship. Each Tivoli Identity Manager entity can contain people, who can then be assigned to Organizational Roles.

Any of the subsidiary entities can be subsidiaries of an Organization or of any of the other entities. There is no restriction on hierarchy for subsidiary entities, so, for example, a Location can contain other Locations, and Organization Units can contain other Organization Units, along with any of the other subsidiary entities. An Organization must always be at the top of the organizational hierarchy.

When adding people, they must be put into either an Organization or other container such as an Organizational Unit, Business Partner Organization, Admin Domain, or Location. Once a person is added to an Organization or other container, they can be provisioned with a Service which allows them to access a managed resource, including the Tivoli Identity Manager Server.

A workflow can be associated with a provisioning policy. If an account for a service is to be created for a person, a workflow may require specific information to be provided by a defined person (e.g. userID or other information required on the managed resource for creation of the account) or the account creation to be approved by a supervisor or other ITIM instance.

Access to the Tivoli Identity Manager via its user interface is granted by entitling persons to use the ITIM service. Users of the ITIM service can be grouped by ITIM groups. A pre-defined Administrator group can be assigned to users who need full access to all functional areas of Tivoli Identity Manager.

Users of the Tivoli Identity Manager, typically organized by means of ITIM Groups, are granted various types of access through access control mechanisms that enforce Access Control Item. An Access Control Item, or ACI, defines three things:

- types of functions that are granted to the ITIM Group
- organization or subsidiary entity types upon which the granted functions may be performed
- level within the organizational hierarchy at which the granted functions may be performed

Some people, usually only one or a few, are defined to be Administrators of the system by relationship to the pre-defined Administrator Group and have access to all Tivoli Identity Manager functions at all levels. Most users will have the possibility to manage certain aspects of their own account, e.g. to change their password or to request the creation of an account they are entitled to.

2.4. IT Environment

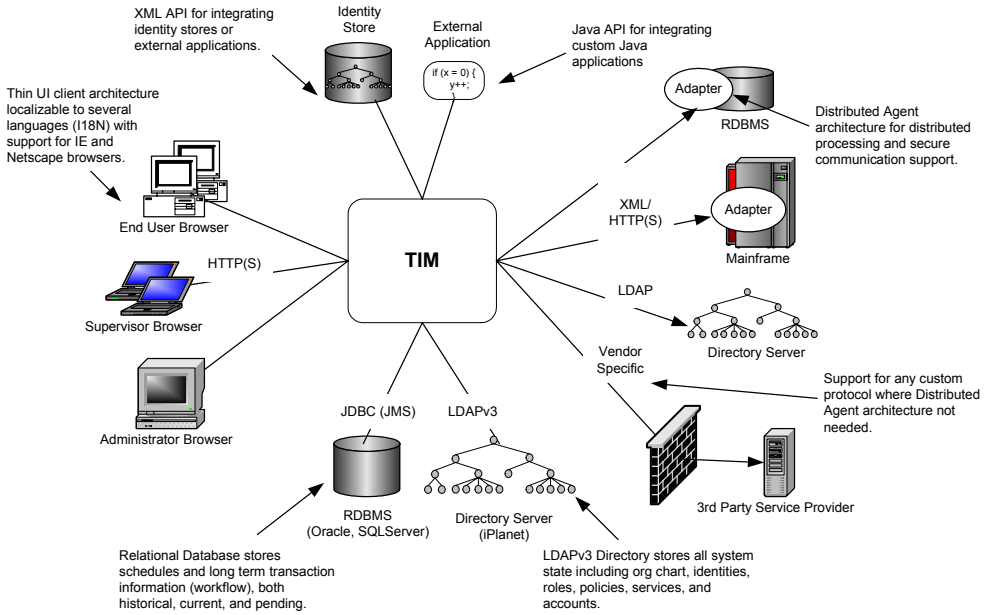

Figure 2: Product view of the TOE and IT Environment

Figure 2 presents a product-oriented overview on how Tivoli Identity Manager interfaces with its IT environment. Please refer to Figure 3 and section 2.6 for a definition of the TOE boundary.

The basic structure of the product is the ITIM server "TIM". This server runs on top of a web application server that provides the necessary Java 2 Platform, Enterprise Edition (J2EE) runtime environment. The ITIM server provides interfaces to:

- "Adapters" for about 65 different target systems (services), such as IBM's Advanced Interactive Executive (AIX), Microsoft's Windows, and IBM's Lotus Notes.

  The adapters run on dedicated adapter servers, or, as is the case for most operating systems, on the machine that is running the service itself (in special cases they may also be operated on the same system as the ITIM server). The adapters are limited to perform the following operations on the target systems: add, modify, delete, and lookup of user accounts and attributes related to those accounts (e.g., group memberships).

  Generic adapters (called tool kits) are provided as well as LDAP and vendor specific possibilities to address services in the IT environment.

  Please see section 2.7 for a list of the adapters that are included in the evaluated configuration. These are actually part of the TOE and not considered part of the IT environment.

- User and administrator (supervisor) systems.

The user and administrator interface for managing identities, roles, and policies and for performing other management aspects is web (i.e. HTML) based. Parts of the administrator interface use Java applets.

Users and administrators use the web browsers on their system to access the presentation services offered by ITIM.

- Directory Server

  A directory server for storing user identities, organizational roles, provisioning policies, and workflow policies is accessed via LDAP v3 (platforms supported by the ITIM product are either the IBM Tivoli Directory Server or Netscape iPlanet).

  Please refer to section 2.8 for an identification of the user registry supported by the evaluated configuration.

- Transaction data base

  An external data base is used to store transaction logs containing audit records that have been generated by the TOE. Platforms supported by the ITIM product are IBM DB2, Oracle, and Microsoft SQL Server.

  Please refer to section 2.8 for an identification of the RDBMS supported by the evaluated configuration.

- Identity Stores

  HR management software can be used as “HR Feeds” (also called Identity Feeds). The identities to be managed and provisioned to the services are then received from such an identity feed using DSML or via the IBM Directory Integrator.

- External Applications

  A Java API is provided by ITIM to provide an interface for user specific applications in the IT environment as well as for the Web User Interface subsystem.

- Messaging Service

  ITIM uses an external messaging service, IBM MQSeries, for the queuing of workflow actions.

- Key Generation and Certification Authority

  The ITIM components use Secure Socket Layer (SSL) server and client certificates for authentication of the SSL communication layer. This requires an external entity to provide key and certificate generation.

2.5. Subjects of the TOE Security Policy

The TOE decides in its notion of subjects between **persons** and **users**. While the TOE Security Functions (TSF) are primarily focused on users of the TOE, it is important to keep in mind that the

TSP also aim at protecting information related to identities that are not users of the TOE itself. Keeping this in mind, the different terms used throughout the SFR specification in chpt. 5 have to be interpreted as follows (cf. as well the Glossary provided in the Appendix):

- person (or, identity): a person is identified by name and further information associated with her or him, e.g. aliases and membership of an Organizational Role. Persons are part of an Organization or Organizational Unit within the organizational hierarchy managed by the TOE. When it comes to the management of a number of persons, they may be referred to as well as "people".
- user (or, ITIM user): a user is a person having an account on the TOE, i.e. the person has been provisioned with an account for the ITIM service. He is able to access the TOE's user or administrative interfaces, to authenticate against the TOE, and is subject to access control and auditing performed by the TOE. The term user includes all users of the TOE regardless of their role.
- group (or, ITIM group): a group is a concept to represent a number of dedicated users by membership. Groups relate to the ITIM service and can be subject of Access Control Item. All users that are members of a group which is subject to an ACI are therefore subject to that ACI.
- administrator: an administrator is a user that is member of the Administrator group of the ITIM service. Members of this group are not subject to any access control. This means that any administrator is per definition an "authorized user" for all transactions.
- account: persons can be provisioned with accounts on a remote service, or on the ITIM service. While the latter makes a user out of a person in terms of the TOE Security Policy, the term account does not refer to a not further specified resource (e.g., a Windows machine or Oracle Database), but to the concept of service entitlement and provisioning in general.
- service: a service represents the definition of a managed resource that is known to the TOE, i.e. the TOE is able to provision accounts on that service via an adapter. A special case is the ITIM service, which comprises the functionality that is offered to users of the TOE.
- role: an organizational role is a similar concept than a group, representing a number of persons (as opposed to users). It is used for people management, e.g. when it comes to the definition of provisioning policies. Association of a person with a role may be achieved e.g. by position of the person in the organization's hierarchy. All persons that are assigned to an organizational role which is subject to a Provisioning Policy are subject to this Provisioning Policy.

2.6. TOE Boundary and Runtime Environment

Figure 3 presents an abstract overview of the TOE, its runtime and general IT environment. The line identifies the TOE boundary. The following sections will give a detailed overview of the technology

that has been used to build the TOE and the underlying systems that are expected to provide the runtime environment for the TOE.

The TOE basically consists of the ITIM server, which is comprised by the Core Services, Applications and Web User Interface subsystems, and the adapters sitting on the managed resources.

While the ITIM server component is completely built on Java related technology, the adapters deployed on the services are usually written and compiled in other programming languages. Therefore, the runtime environment provided by the IT environment for running the TOE is a Web Application Server (WebSphere) for the ITIM server and a Windows operating systems for the respective adapters.

The Policy Directory (in fact an LDAP repository), the Workflow, or transaction, data base and the external sources for person information (i.e. the identity stores) are part of the IT environment.

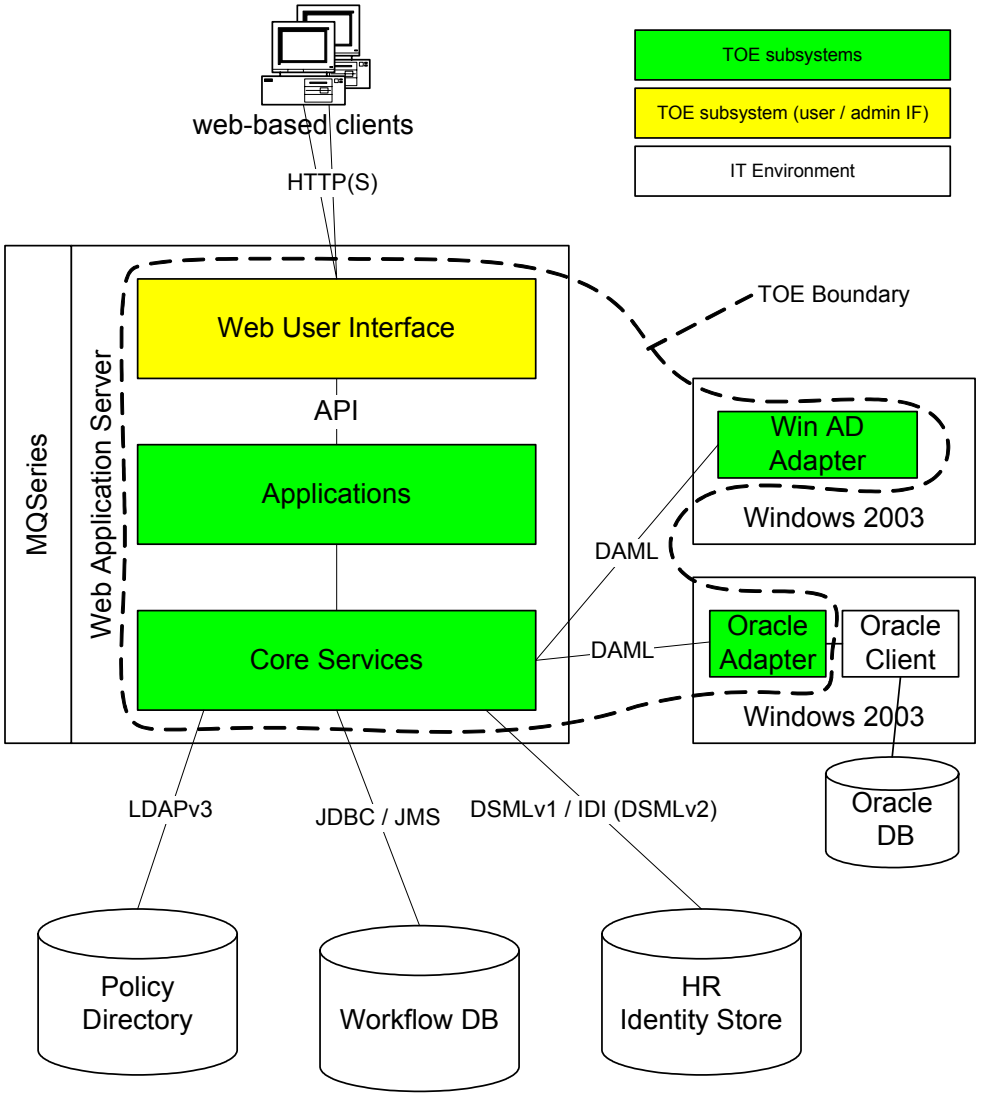

Figure 3: Abstract view of the TOE boundary

2.6.1 Runtime Environment for the ITIM Server

The ITIM server component is completely based on the Java 2 Platform, Enterprise Edition (J2EE) technology. The ITIM server component relies on services in the IT environment provided by the J2EE framework as implemented by the Web Application Server.

Services provided by the Web Application Server and, for the administrator accessible Java applets by the runtime environment on the administrator's client machine, are:

- J2EE (including Java 2 Platform, Standard Edition) services and interfaces to these services as specified in Java [TM] 2 Platform Enterprise Edition Specification, v1.4, and further specification referenced there within, in detail
    - HTTP and HTTPS, interfaces are specified by the java.net package (client-side) and servlet and Java Server Pages (JSP) interfaces (server side)

      Note: The implementation of the SSL layer itself is not part of the TOE. HTTPS connections to the user clients are provided by the application server in the TOE environment, SSL connections between the ITIM Server and adapters are provided by relying on a third-party application as well.
    - Java Transaction Service (JTS) – a transaction manager that can be accessed via the Java Transaction API (JTA) to establish a distributed transaction system
    - Remote Method Invocation (RMI) APIs, i.e. JavaIDL and RMI-IIOP
    - JDBC API – this API provides connectivity with relational database systems and is interfaced by the TOE via the JDBC 2.0 Core API (provided by J2SE) and the JDBC 2.0 Extension API
    - Java Naming and Directory Interface (JNDI) to access the naming service provided by the WAS for the referencing to the objects that comprise the TOE
    - Java Messaging Service (JMS) API to access the JMS provider (engine) provided by the Web Application Server for asynchronous messaging between the TOE components.
    - JavaMail API to access a JavaMail service provider implemented by the Web Application Server in the IT environment for handling of Internet emails.
    - Java API for XML Processing (JAXP) for the processing of XML documents.
    - JavaBeans Activation Framework (JAF) API for support of MIME data processing, e.g. by the JavaMail service.
    - J2EE Connector Architecture API for connectivity with enterprise information systems.

- Java Authentication and Authorization Service (JAAS) providing a PAM framework and API for user authentication and authorization.
- Java Cryptography Extension (JEC) providing cryptographic services (e.g. encryption and hashing).

Interpretation of bytecode by the Java Virtual Machine as specified in The Java [TM] Virtual Machine Specification (2nd Edition) is provided by

- the Java 2 SDK as delivered with the Web Application Server
- the Java 2 SDK or JRE on the client (administrator) machines

2.6.2 ITIM Adapters

The ITIM adapters run directly on native operating systems. They have been implemented in native programming languages, mostly C and C++. They rely on the services provided by these operating systems in terms of runtime environment, and interact with the managed resources via the interfaces provided for user account management by the managed resources (in case of the Windows AD Adapter this is the Active Directory Server Interface (ADSI), and in case of the Oracle Database Adapter for Windows this is the Oracle Client Software).

2.7. Product Packaging

The TOE is a distributed system, comprising the ITIM server and a defined set of adapters. It is delivered to the customer as follows:

- ITIM Server Release 4.6

  The ITIM server is delivered as installation image via IBM's Passport Advantage distribution channel. Optionally, it can be ordered on CD-ROM. The evaluated configuration assumes that the customer uses online access to Passport Advantage to download an installation image to install an evaluated configuration of the TOE.

  The customer is generally presented the choice between two packages for installation. An all-in-one package that supports only single-node deployment, and a clustered package that supports clustering of ITIM over several web application servers. Only the single-server installation process is to be used for an installation of the evaluated configuration of the TOE. This package will install

  - the runtime environment for the TOE comprised by IBM WebSphere Application Server and the deployment manager part of the WebSphere Application Sever Network Deployment product, version 5.1 Fix Pack 1 with Cumulative Fix 3, with the APARs PK00346, PK02976, PK02640 (i.e. web application server and JMS engine) and IBM WebSphere embedded

messaging support (part of the IT environment)

- ITIM application binaries and configuration files (part of the TOE)

- Oracle Database Adapter for Windows version 4.6.1 (part of the TOE)

  This adapter runs on 32 bit x86-based machines with Windows NT 4.0, Windows Server 2003 Enterprise Edition, or Windows 2000 Advanced Server. It interfaces the Oracle Client Software version 8i, 9i, or 10g for managing Oracle Databases for all platforms.

  The evaluated configuration is restricted to Windows Server 2003 Enterprise Edition running the Oracle Client Software version 9i as part of the IT environment.

- Active Directory Adapter version 4.6.2 (part of the TOE, also known as "Windows AD Adapter")

  This adapter runs on 32bit x86-based machines with Windows 2000 Advanced Server running Active Directory or Windows Server 2003 Enterprise Edition.

  The evaluated configuration is restricted to Windows Server 2003 Enterprise Edition.

User and administrator guidance for the TOE, including guidance for the secure installation and configuration of the TOE, is provided online at IBM's web site.

2.8. Evaluated Configuration

The following describes the specifics of the configuration of IBM Tivoli Identity Manager 4.6 and its IT environment that conforms to the description in this Security Target and is henceforth called the evaluated configuration:

- Only adapters that are part of the evaluated configuration of the TOE (i.e. the adapters identified in section 2.7) are to be used. No other adapters in the IT environment may be connected to the TOE, including LDAP or vendor specific adapters. The adapters that are part of the evaluated configuration use the DAML protocol (as opposed to FTP) for communication with the ITIM server.

- The ITIM server component of the TOE is installed and operated on a dedicated Web Application Server that communicates via network connections with clients, adapters and the resources in the IT environment (e.g. LDAP registry, RDBMS) as supportive to the TOE.

- "Event notifications" of adapters (remote password synchronization) and identity feeds are not supported in the evaluated configuration. The DSML and IDI identity feeds are operated by using their reconciliation functionality.

- Only the English user interface (and guidance) is to be used.

- The TOE must not be operated in a multi-tenant setup.

- The usage of low-level APIs (as opposed to the exported API) to extend the functionality of the TOE's Core Services by plugging in user-specific extensions is prohibited.
- The Web Application Server and MQSeries are installed on one dedicated machine that is physically and logically protected. Clustering is disabled.
- The Directory Server and RDBMS are installed either together on one or separated on two systems. They are for dedicated use by the TOE only and configured accordingly (e.g. restricted network availability). The underlying machine(s) are dedicated to run only these applications.
- All network communication is protected, either by cryptographic (SSL / TLS) or organizational (restricted network access) means.
- Access to network sockets opened by adapters for configuration with the agentCfg tool is restricted to "root" users, or administrators, on the local operating system hosting the adapter. High quality passwords must be set for the adapter configuration.
- Single Sign-On is not supported.

The evaluated configuration of the TOE restricts the choice of products that can be selected by the customer to fulfill the dependencies of the ITIM server on its IT environment to the following products:

- The underlying operating environment for the ITIM server is IBM WebSphere Application Server 5.1 as specified in section 2.7, the JDK as distributed with this WebSphere version and the embedded JMS engine, as delivered with the single-server installation process for the TOE.
- The underlying operating systems for the adapters that are part of the evaluated configuration are
    - Windows Server 2003 Enterprise Edition for the Windows AD Adapter
    - Windows Server 2003 Enterprise Edition for the Oracle Database Adapter for Windows
- The interface provided by the IT environment for the Oracle Database Adapter for Windows is the Oracle Client Software version 9i.
- IBM Tivoli Directory Server Version 5.2 with Fix Pack 2 as LDAP v3 compatible directory server.
- The Relational Database Management System (or, transaction database) is either
    - IBM DB2 Universal Database Enterprise Edition server and IBM DB2 runtime client, Version 8.2
    - Oracle Version 9i
    - Microsoft SQL Server 2000
- Mozilla 1.7 and Microsoft Internet Explorer 6.0 with Service Pack 1 for access to the presentation

services (i.e. the user and administration interface), using the Java Runtime Environment provided with them.

Note: The Java runtime environment of the WebSphere Application Server (WAS) as underlying system for the ITIM Server provides a level of abstraction that makes the ITIM Server component of the TOE independent from any native operating system in terms of functionality provided to support the TOE. Consequently, this Security Target makes no further restriction on the native operating system the Web Application Server for the ITIM Server runs on.

2.9. TOE Security Functionality

The TOE provides the following security functionality:

- Auditing of activities

  The TOE is capable of auditing internal events (e.g. the modification of provisioning policies or the creation of new users) by generating audit information for all transactions that is stored in a data base provided by the IT environment. The TOE offers functionality to review these audit records.

- Identification and authentication

  The TOE identifies users (including administrators) by user name and authenticates them by password. ITIM users are persons having an account on the TOE, they can be organized by membership to ITIM groups.

  The user identities are stored in a directory server provided by the IT environment. Only hashes of the passwords are stored in the TOE. Password policies can be applied to enforce requirements on the quality of the password that a user chooses. Lockout mechanisms prevent password guessing attacks.

- Authorization (access control)

  The ITIM server performs authorization for user actions, commonly referred to as requests, based on Access Control Item (ACI). ACIs can be assigned to ITIM groups and ACI principals (e.g. administrators). One pre-defined ITIM group exists for ITIM administrators, other groups can be defined by the customer.

  The TOE offers three groups of ACIs:

  - organizational (access control to functions related to entities within an organization or the organization itself)
  - provisioning (access control to functions related to provisioning and other policies)

- reporting (access control to functions related to the generation of reports)

ACIs can be created, modified, or deleted by either a system administrator or explicitly entitled users. Members of the pre-defined Administrator group are not subject to any access control.

- Provisioning

  Provisioning policies define the services the persons belonging to an organizational role shall have access to. If a person belongs to an organizational role defined within the TOE, and a provisioning policy specifies the entitlement of this organizational role to a certain service, the person is entitled to have an account on this service. Such an account may be created upon request of the user by interaction with the TOE (if the person belongs to an ITIM group), may be manually created by administrator request, or may be automatically created for the person during periodic policy enforcement.

- Service Reconciliation and Identity Feeds

  The TOE provides the capability of gathering account information from managed resources. Reconciliation retrieves and compares user information stored on a managed resource with the corresponding data stored in the Tivoli Identity Manager database.

  Data can be imported via Identity Feeds as well: user data (i.e. person, or identity, information) can be imported into an Organization managed by the TOE. This functionality releases the administrator from adding a potentially large number of persons manually to the TOE's database and allows automated reconciliation with systems used for human resource management within an organization.

3. TOE Security Environment

3.1. Assumptions

The description of assumptions describes the security aspects of the environment in which the TOE will be used or is intended to be used. This includes the following:

- information about the intended usage of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use; and
- information about the environment of use of the TOE, including physical, personnel, and connectivity aspects.

3.1.1 Intended usage of the TOE

A.CONFIGURATION It is assumed that in the evaluated configuration all configuration measures as indicated in section 2.8 are applied.

3.1.2 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 system administrative personnel 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 this Security Target.

They will perform administration activities from a secure environment using terminals and / or workstations they trust via secured connections to the ITIM server.

They will protect their passwords used for authentication against the TOE. Passwords must not be disclosed to any other individual. Passwords must be securely transmitted to users if generated on behalf of those users.

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

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

Connectivity aspects:

A.AGENT It is assumed that the runtime environment for an adapter 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 adapter and its interfaces.

A.DIRECTORY The directory server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the directory.

A.RDBMS The RDBMS used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the data base.

A.SERVER The machine(s) providing the runtime environment for all parts of the TOE other than adapters are assumed to be used solely for this purpose and are not used to run other application software except those required for the management and maintenance of the underlying system and hardware.

Especially it is assumed that the underlying system(s) are configured in such a way that no unauthorized access to functions provided by the underlying web application server and operating system software (including network services) 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, accounts, organizational structures, users, organizational roles and groups
- provisioning policies, password policies, service definitions, workflows, ACIs and other policies 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
- 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 Item 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 company intranet 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, Web Application Server, Transaction Data Base and Directory Server used 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.

The threats listed below are grouped according to whether or not they are countered by the TOE. Threats that are not countered by the TOE are to be countered by environmental or external measures.

3.2.1 Threats to be countered by the TOE

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.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.

3.2.2 Threat to be countered by the TOE environment

TE.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.

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 during Service Reconciliation or via Identity Feed 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 via Identity Feed 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. 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.

For a discussion of IMPP conformance, please refer to section 7.2.

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 rules 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 during Service Reconciliation or via Identity Feed are properly associated with the corresponding data already existent in the TOE database.

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 remote resource is only initiated for persons that are entitled to the corresponding service.

4.2. Security Objectives for the IT Environment

OE.AUDIT The runtime environment for the ITIM server must provide a reliable time source for audit record generation.

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

OE.DB_PROT The data base in the IT environment used by the TOE to store TSF data and user data must protect such data against unauthorized access.

OE.DIR_PROT The LDAP server in the IT environment used by the TOE to store TSF data and user data must protect such data against unauthorized access.

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.

4.3. Non-IT Security Objectives for the Environment

OE.ADMIN Those responsible for the TOE shall ensure that the TOE and underlying system administrative personnel – as well as administrators for the user registry, transaction data base and identity feeds – 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 this Security Target and initiate administrative actions from a secure environment using terminals and / or workstations they trust via secured connections to the ITIM server.

They do not disclose their passwords 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 adapter operates as specified and provides adequate protection measures against tampering with the adapter and its interfaces.

OE.FEED Those responsible for the TOE must ensure that the information provided by any Enterprise Identity Data Store in 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 machines providing the runtime environment for the TOE are protected against physical attack, which might compromise IT security objectives.

All parts of the TOE other than the adapters must be the only application(s) installed on the machines hosting their runtime environment, and 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 passwords 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 with all the required operations performed. Operations already performed in IMPP have been marked bold. Assignments and selections performed in this ST have been marked in bold and italics. In addition some refinements to SFRs as defined in the Common Criteria and IMPP respectively have been applied. Those are marked in bold, italics and underlined.

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.

5.1. TOE Security Requirements

Table 1 identifies the security functional requirements that have been derived from IMPP and CC Part 2, and the operations that have been applied to them in this Security Target.

SFR	**Source**	**Performed Operations in ST**
TOE		
FAU_GEN.1	IMPP	assignment, refinement, selection
FAU_GEN.2	IMPP	none
FAU_SAR.1	IMPP	assignment
FAU_SAR.2	IMPP	none
FDP_ACC.1 (ETC)	IMPP	refinement
FDP_ACC.2 (ACF)	IMPP	refinement
FDP_ACF.1 (ACF)	IMPP	assignment, refinement
FDP_ACF.1 (ETC)	IMPP	assignment, refinement
FDP_ETC.2	IMPP	assignment, refinement
FIA_AFL.1	IMPP	assignment, refinement
FIA_ATD.1 (AFC)	IMPP	none

SFR	Source	Performed Operations in ST
FIA_ATD.1 (ETC)	IMPP	refinement
FIA_SOS.1	IMPP	assignment
FIA_UAU.2	IMPP	none
FIA_UID.2	IMPP	none
FIA_USB.1	IMPP	none
FMT_MSA.1	IMPP	assignment, refinement
FMT_MSA.3 (ACF)	IMPP	assignment, refinement
FMT_MSA.3 (ETC)	IMPP	assignment
FMT_SMF.1	IMPP	assignment, refinement
FMT_SMR.1	IMPP	assignment
FPT_RVM.1	IMPP	none
FPT_TDC.1	IMPP	assignment, refinement
Managed Resources		
FPT_TDC.1	IMPP	assignment, refinement
Directory Server		
FIA_UAU.1	IMPP	iteration
FIA_UID.1	IMPP	iteration
Transaction Data Base Server		
FAU_STG.1	IMPP	none
FIA_UAU.1	IMPP	none
FIA_UID.1	IMPP	none
Secure Network Session		
FPT_ITT.1	IMPP	none
FTP_ITC.1	IMPP	selection
Runtime Environment of the TOE		

SFR	Source	Performed Operations in ST
FPT_SEP.1	IMPP	none
FPT_STM.1	IMPP	none

Table 1: Operations applied to SFRs derived from IMPP and CC Part 2

Note: IMPP allowed for several requirements the assignment of items in addition to items already assigned in IMPP – in case the ST did not add additional items to the component, the operation performed has been identified as assignment nevertheless.

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 ***not specified*** level of audit; and

c) **the following auditable events:**

- ***creation, deletion, suspension, restoration of a person***
- ***deletion, suspension, restoration of multiple persons***
- ***person business unit change***
- ***person data change***
- ***creation, modification, deletion, suspension, restoration of accounts for a service***
- ***deletion, suspension, restoration of multiple accounts***
- ***password change for accounts, multiple accounts***
- ***creation, modification, deletion of provisioning policies***
- ***creation, modification, deletion of service selection policies***
- ***creation, modification, deletion of dynamic roles***
- ***reconciliation, policy enforcement***

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, ***no additional information***.

Application Note: The TOE does not provide audit records as in FAU_GEN.1.1 a) for the start and stop of the audit functions. However, the TOE ensures by design that non of the auditable events in FAU_GEN.1.1 b) and c) can take place without being recorded: requests cannot be processed without the TOE and the RDBMS in the IT environment being available. If requests are processed, audit records are created by the same component that processes the requests. There is no separate audit function that could be started or stopped.

Application Note: The TOE views auditable events as requests. In general, a request can be issued by a subject that is distinct from the subject which is the target of the request. This leads to the distinction of requestor (i.e. the subject identity issuing a request) and requestee (i.e. the subject identity that is target of the requested action).

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** ***and other authorized users*** 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: A user being member of the Administrator role can read all audit information. All users can read audit information related to transactions, or requests, originated by them. Users might be explicitly authorized to read additional audit information.

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 The TSF shall enforce the ***Provisioning access control SFP*** on

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

FDP_ACC.2 (ACF) Complete access control

FDP_ACC.2.1 The TSF shall enforce the ***ITIM access control SFP*** 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 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.

FDP_ACF.1 (ACF) Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***ITIM access control SFP*** to objects based on **administrator-specified access control information, user names and roles**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***By examining the ACIs that apply to an entity due to the ACI's focus specified by origin, target, and scope,***

- ***read access to an entity's attribute***
  - ***is explicitly allowed if the ACI specifies "Grant" for that attribute***
  - ***is explicitly denied if the ACI specifies "Deny" for that attribute***
  - ***is implicitly denied if the ACI specifies "None" for that attribute***
- ***write access to an entity's attribute***
  - ***is explicitly allowed if the ACI specifies "Grant" for that attribute***

  - ***is explicitly denied if the ACI specifies "Deny" for that attribute***
  - ***is implicitly denied if the ACI specifies "None" for that attribute***
- ***removal of an entity***
  - ***is explicitly allowed if the ACI specifies "Grant" for the "Remove" operation***
  - ***is explicitly denied if the ACI specifies "Deny" for the "Remove" operation***
  - ***is implicitly denied if the ACI specifies "None" for the "Remove" operation***
- ***searching of an entity***
  - ***is explicitly allowed if the ACI specifies "Grant" for the "Search" operation***
  - ***is explicitly denied if the ACI specifies "Deny" for the "Search" operation***
  - ***is implicitly denied if the ACI specifies "None" for the "Search" operation***
- ***adding of an entity***
  - ***is explicitly allowed if the ACI specifies "Grant" for the "Add" operation***
  - ***is explicitly denied if the ACI specifies "Deny" for the "Add" operation***
  - ***is implicitly denied if the ACI specifies "None" for the "Add" operation***
- ***modification of an entity***
  - ***is explicitly allowed if the ACI specifies "Grant" for the "Modify" operation***
  - ***is explicitly denied if the ACI specifies "Deny" for the "Modify" operation***
  - ***is implicitly denied if the ACI specifies "None" for the "Modify" operation***
- ***an explicit denial by one ACI overrides an explicit grant by other ACIs***
- ***an explicit grant by one ACI overrides an implied denial by other ACIs***
- ***in cases of multiple ITIM Group memberships, a person's access is enabled based on the widest privilege granted to any of their ITIM Groups. However, if a type of access is explicitly denied to an ITIM Group of which the person is***

a member, the access that is explicitly denied to them in that one ITIM Group is be denied to them in all roles

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- ***Membership of the Administrator group authorizes access to all objects.***
- ***Domain administrators (i.e. users assigned as administrators for an administrative domain within ITIM) are allowed to perform the following actions only within their administrative domain:***
  1. Defining policies and roles
  2. Administering people (including the definition of ACIs)
  3. Defining and provisioning services

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***no additional rules***.

Application Note: Out of the box, TIM sets up a default Organization with an Access Control List that grants access rights to Self, Supervisor, and Domain Administrator. These ACI's grant enough permissions to administer (add, modify, remove, etc.) any type of object (Person, Organizational Unit) in a Supervisor's Organizational Unit or in a Domain Administrator's Admin Domain. There are also ACI's that grant a SystemUser permission to view their own TIM Account details and to change their Home Page, as well as permission to view their Personal Information (Self). No other permissions are defined in the system (out of the box) beyond those defined in the default ACIs.

FDP_ACF.1 (ETC) Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Provisioning access control SFP*** to objects based on **entitlement rules, persons and person attributes indicating organizational relationships**.

FDP_ACF.1.2 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.**

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on ***no additional rules***.

FDP_ETC.2 Export of user data with security attributes

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

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 TSC, 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 TSC:

- ***Administrator*-defined provisioning workflows associated with an entitlement and the managed resource respectively, *if part of the provisioning policy*;**
- ***The following conflict resolution rule:***
  - ***In case of conflicting provisioning policies (i.e. a person is entitled to a service by more than one provisioning policy, with different attribute values for the entitlements), the conflict is resolved by the join directives for the most specific provisioning policies.***

Application Note: The provisioning of user accounts on remote resources is considered export of user data: provisioning policies processed on the ITIM server trigger the export of account data via an adapter (which is part of the TOE) to the underlying managed resource of the adapter (which is part of the IT environment). This is modeled in terms of an access control policy – based on the provisioning (i.e. access control) policies, persons are granted access (in form of user accounts) to remote resources. This component specifies additional consistency rules for the provisioning process.

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 *positive integer within 1 and 5*** unsuccessful authentication attempts occur related to ***password-based client*** **authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***suspend the account***.

FIA_ATD.1 (ACF) User attribute definition

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

- **user name**
- **authentication credentials**
- **role memberships**

FIA_ATD.1 (ETC) User attribute definition

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

- **unique identifier *(common and distinguished person name)***
- **organizational relationships**
- **account data*:***
  - ***aliases for user names associated with a person (optional)***
  - ***status of the person (active, inactive)***
  - ***authentication credentials for accounts***

Application Note: The "user name for account on ITIM service" is referred to as "user" in the security functional requirements for the TOE, cf. also the information provided in section 2.5.

Application Note: While group and role memberships are considered security attributes that belong to individual persons, the implementation of the TOE merely maintains groups and roles as dedicated objects with person distinguished names as attributes, instead of assigning group and role attributes to individual persons.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***the following Password Policy:***

- ***minimum length: 6 characters***
- ***maximum length: not specified***
- ***maximum repeated characters: not specified***
- ***minimum unique characters required: 6 characters***
- ***minimum alphabetic characters required: 5 characters***
- ***minimum numeric characters required: 1 character***
- ***disallow user name: yes***
- ***disallow user ID: yes***
- ***repeated history length: 5***
- ***invalid characters: none***

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 instantiation of the SFR derived from the IMPP focuses on the authentication of ITIM users, i.e. all users that use the web-based interface or Application API to access and manage the TOE.

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.

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.

5.1.1.4 Security management

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***ITIM access control SFP*** to restrict the ability to **create, query, modify, delete** the security attributes **related to persons, users, access control information, entitlement rules, services and workflows** to **administrators** ***and other authorized users***.

FMT_MSA.3 (ACF) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the ***ITIM access control SFP*** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ***no roles*** to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TOE does not offer pre-defined ACIs. Upon creation of an ACI, rules have to be created explicitly – no initial values are pre-defined, or "None" as implicit denial is pre-defined for access rights.

FMT_MSA.3 (ETC) Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the ***Provisioning access control SFP*** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

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

Application Note: Provisioning Policies specifying the Provisioning information flow control SFP have to be explicitly defined by administrators.

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 organizational, provisioning and report ACIs***
- **management of entitlement rules**

- **management of workflows, or additional exportation rules**
- **management of persons**
- **management of users**
- **management of services (representing managed resources)**
- ***management of organizations and organizational units***

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **user, administrator**.

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. However, users that are member of the Administrator group are considered to be in the administrator role. The definition of these two roles in terms of the TSF does not prevent the administrator-specified definition of further ITIM groups to ease maintenance of users.

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.

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:

- ***identity feed:***
  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.

- ***service reconciliation:***

  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.

5.1.2 TOE Security Assurance Requirements

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

5.2. Security Functional Requirements for the IT Environment

This section contains security functional requirements that must be fulfilled by the IT environment in order to support the security functionality of the TOE.

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*, including passwords,* 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.**

5.2.2 Directory Server

The directory server in the IT environment is interfaced via LDAP and used to store TSF data and user data (e.g. identities, roles, policies, services, 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

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.

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 succesfully identified before allowing any other **IT environment**-mediated actions on behalf of that user.

5.2.3 Transaction Data Base Server

The RDBMS in the IT environment is interfaced via JDBC and used to store TSF data and user data (transaction data resulting out of user or system generated requests).

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
- protection of the audit, or transaction, records against unauthorized deletion

FAU_STG.1 Protected audit trail storage

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

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

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.

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 succesfully identified before allowing any other **IT environment**-mediated actions on behalf of that user.

5.2.4 Secure Network Sessions

The internal TOE TSF data transfer, as well as the data transfer between the TOE and other trusted IT products, 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

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.

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 ***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**.

5.2.5 Runtime Environment of the TOE

The Web Application Server providing the runtime environment for the ITIM server 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: In conformance with IMPP the evaluated configuration satisfies this requirement by imposing the assumptions A.AGENT and A.SERVER. In addition, the runtime environment for the ITIM server makes use of Websphere's role-based authentication model to prevent access to internal subsystem interfaces.

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.

6. TOE Summary Specification

6.1. Statement of TOE Security Functions

The following is a summary of the security functionality provided by the TOE.

6.1.1 F.I&A

Identification and authentication of ITIM users is performed and enforced via the API interface of the Applications subsystem. The web user interface supplied with the ITIM server provides a Java/HTML based graphical user interface that can be used by clients to perform a log in and access the functionality provided by the TOE using a web browser. The TOE supplied web user interface as well as other applications (either replacements of the TOE supplied user interface or data feeds from applications of the TOE environment) can access the security functionality of identification and authentication using the API exposed by the Applications subsystem only.

Users are identified by the name associated with their account on the ITIM server and authenticated by password. The TOE enforces administrator-defined password policies for the verification of passwords. The server-based generation of secrets and authentication by answers to questions asked by the ITIM server (challenge-response authentication) is disabled in the evaluated configuration.

If allowed by configuration, ITIM users can change their password via the web interface or any application utilizing the API of the ITIM server. Administrators can change passwords of users as well.

A password expiration time can be configured, specifying a certain amount of time after which a password cannot longer be used for authentication. Also, a maximum number of invalid logon attempts can be specified – if consecutively wrong authentication information (i.e. passwords) is supplied for a certain account on the ITIM service, the account will be suspended after the defined number of wrong authentication attempts.

User credentials (identities and their security attributes) are stored in an external LDAP server. This includes cryptographic hash sums of the passwords used to authenticate ITIM users.

The TOE provisions passwords to other services than the ITIM service as well, i.e. to managed resources in the IT environment. This is done by interfacing with the managed resource's way of handling passwords and promoting a password for an account to the managed resource. Clients are allowed to alter those passwords via the user interface of the TOE, and such passwords are subject to the password policy that applies to the individual holding the respective accounts on the managed resource. However, the enforcement of identification and authentication for other services than the ITIM service itself (e.g., the Windows operating system and the Oracle database) is left to the managed resource and therefore not part of this security function. The provisioning of passwords to

remote services is addressed in F.Provisioning.

The following mechanisms used to implement this security function are subject to an SOF rating:

- enforcement of the password policy by the ITIM server

Note: Session management for HTTP sessions is used to avoid performing identification and authentication prior to each HTTP request from the user. Session management between clients and the TOE is performed by the underlying Web Application Server.

Note: the TOE in its evaluated configuration uses SSL certificate based authentication for the authentication between ITIM Server and adapters. The implementation of SSL and therefore this authentication mechanism is part of the IT environment.

6.1.2 F.Authorization

This TSF comprises the authorization of actions requested by ITIM users (including administrators). Each action requested is individually authorized prior to its execution.

Authorization decisions are made and enforced according to Access Control Item (ACI), which specifies whether to deny or grant the execution of an action.

ACIs control access to two types of features:

- attributes
- operations

ACIs define whether a user can read and modify entities and their attributes. ACIs also define whether a user can add, modify, delete, or search for an entity or process. (An entity is a concept or structure in ITIM. Examples of entities are Organizations, Persons, Accounts, Organizational Roles, and policies.)

The following types of ACI are provided by the TOE for controlling access to certain entities:

- Organizational ACIs, e.g. for controlling access to functions related to entities within an organization or the organization itself
- Provisioning ACIs, e.g. for controlling access functions related to provisioning or other policies
- Reporting ACIs, for controlling access to the report generation mechanisms

All ACIs have in common that they grant (or deny) access requested by clients (either users being member of a dedicated ITIM group; or an ACI Principal being “self”, Supervisors or Domain Administrators) and are evaluated and enforced by the ITIM server. The focus of an ACI is controlled by its origin (branch in the organization tree where the ACI is located), target (the entity type the ACI controls access to) and scope (range within the organization tree the ACI applies to).

For example, an organizational ACI with the target “account / Oracle Database” would control read and write access to the attributes associated with the Oracle Database service and control access over the remove, search, restore, suspend, add and modify operations for accounts of that service for the ACI Principals and ITIM groups that are specified as being subject to this ACI.

An ACI can be created, modified, or deleted by either a system administrator or someone assigned to an ITIM Group that has been designated an Authorization Owner. Authorization Owner status can be assigned to an ITIM Group, providing its users with the ability to set up and modify ACIs within an Organization or the organizational tree branch at and below the organizational level the status is assigned to.

The TOE recognizes the notion of roles. The pre-defined ITIM Group “Administrator ITIM Group” grants system administrator status to all of its members. A system administrator has complete access to all items of an organization in Tivoli Identity Manager and all of the associated subunits, including policies and services. The Administrator ITIM Group therefore represents the administrator role within the TOE. All non-members are constrained by access control as enforced by this TSF, and are therefore in the user role.

The TOE recognizes the notion of administrative domains for business units within its model of an organizational structure. A domain administrator can be assigned to an administrative domain, having the privilege of defining and managing provisioning entities, policies, services, workflow definitions, roles, and users within his or her own administrative domain.

ACIs are stored in an external LDAP server.

6.1.3 F.Auditing

The TOE generates audit records for transactions, i.e. user (and administrator) requests. The following request types are covered by the auditing mechanism:

- creation, suspension, restoration of a new person
- suspension, restoration of multiple persons
- creation, modification, deletion, suspension, restoration of accounts for a service
- deletion, suspension, restoration of multiple accounts
- password change for accounts, multiple accounts
- creation, deletion of dynamic roles
- creation, deletion of provisioning policies
- reconciliation

- person business unit change
- person data change

Audit records can be reviewed by authorized users via the user interface.

Audit records are stored in the transaction data base provided by the IT environment.

6.1.4 F.Provisioning

The TOE provides, by means of connectors and adapters for managed resources, user credentials to managed resources. This is done upon Entitlement of an identity to use certain managed resources, or services. Each managed resource is configured in the TOE as a service. A service adheres to a service profile (e.g., several services for Windows machines can be defined that all belong to the Windows service profile). User identities are entitled to a service, or all services belonging to a service profile, based on Provisioning Policies. As a result, a user may (automatically or upon request) be provisioned an account on the services he is entitled to.

Creation (as well as modification and deletion) of an account on a remote service is provided by software adapters that typically reside on the machines providing the managed resources and are able to interface with the user or account data base of a managed resource. These adapters are part of the TOE, while the managed resources belong into the IT environment.

A Provisioning Policy may have the following members that can be entitled to a service: all identities in an organization, identities in designated Organizational Roles, or people that are not in any Organizational Role. Provisioning Policies entitle their members to either a specific instance of a service, all instances of a service type (e.g., Windows), a Service Selection Policy, or all services. Additional parameters – depending on the provisioned service (e.g. group membership on the managed resource) – can be configured as part of the Provisioning Policy.

Conflicting Provisioning Policies are evaluated following the join directives specified for those policies. Only the most specific policies will be joined. (E.g. if policies for single service instances exist as well as policies for the service type, only the ones for service instances will be evaluated.)

The entitlement to a service may be associated with a Workflow that is executed each time the Provisioning Policy is applied. Workflows can be specified by the administrator to reflect special business processes, as a rule involving interactions with users, for provisioning actions. For example, such a workflow could require management approval before a service is provisioned to an identity which is entitled to that service (e.g. the approval of a Supervisor assigned to a business unit in ITIM). Workflows can be designed using the GUI and by specifying additional JavaScript extensions to be executed.

As a special case, Provisioning Policies do not only mandate the entitlement to (and provisioning of)

accounts for services in the IT environment, but also to the "ITIM service", i.e. for accounts to access the TOE itself. The existence of a person (or identity) in the organizational structures managed by the TOE does not grant access to the TOE itself – only users (and administrators) that are provisioned an account on the TOE are then able to access the (security) functionality provided by the TOE.

An administrator-specified Identity Policy may be used to define how the account name for an identity is specified on the managed resource. This is not considered security relevant, though.

An external LDAP server is used to store the appropriate provisioning policies. Workflow definitions are stored in the relational database.

6.1.5 F.Data_Feed

In addition to the distribution of account data to managed resources via F.Provisioning the TOE provides the capability of gathering account information from managed resources. Reconciliation retrieves and compares user information stored on a managed resource with equivalent data stored in the Tivoli Identity Manager database.

The ITIM server updates account information for an identity (if such account information is already present in its database) to reflect the information gathered from the service. If no account information is present, i.e. no account ownership is known to the TOE, it attempts to find the account owner, i.e. the identity that an account belongs to, by comparing the user login IDs on the service to the aliases known for identities managed by the TOE.

Optionally, all accounts returned from the service during the reconciliation that have an owner are then evaluated against corresponding Provisioning Policies. A Provisioning Policy defines (as configured by the administrator) how to handle deviations, e.g. a group membership on the service that is mandated by the Provisioning Policy but not existent according to the gathered account information. Options for such policy enforcement are either to mark non-compliance with a flag, to suspend a non-compliant account on the managed service or to correct the non-compliance on the service in a way that establishes conformance with the Provisioning Policy.

If no ownership for an account could be established during reconciliation, the account is marked and listed as an orphaned account, or orphan account, for the service. The administrator can review the list of orphaned accounts for a service and choose for each account to either deprovision (i.e. to remove it on the managed resource), suspend, adopt (i.e. assign it to an existing identity), or restore it (i.e. reverse a suspension on the managed resource).

Reconciled account data is processed on a per-service basis by the TOE, i.e. changes based on reconciliation only affect accounts provisioned for the corresponding service.

As a special case of data import, the TOE offers Identity Feeds: the DSML service and IDI service

offer the possibility to import user data (i.e. person, or identity, information) into an Organization managed by the TOE. This functionality prevents the administrator from adding a potentially large number of persons manually to the TOE's database and allows automated reconciliation with systems used for human resource management within an organization.

By performing a Reconciliation of the DSMLv1 service, an XML file is evaluated and identities not yet known to the TOE are automatically added into the organizational structure. The IDI service connects to an IBM Directory Integrator (IDI) in the IT environment via DSMLv2 and receives updates of person information via this IDI.

The usage of the JNDI Identity Feed is not part of the evaluated configuration.

6.2. Assurance Measures

The following table provides an overview of the assurance measures that meet the security assurance requirements from section 5.1.2:

Assurance Component	Description how the requirements are met
ACM_CAP.3	IBM uses CVS as the configuration management system for source code, design documentation, guidance, test documentation, and other evaluation evidence. DevTrack is used for tracking of (security related) defects. For design documentation, also Lotus Team Room is used as a configuration management tool. All systems are capable to authenticate users and restrict the access of individual users to configuration items. A CM plan describes the use of those tools within the development environment.
ACM_SCP.1	As mentioned above, source code, design documentation, user and administrator documentation as well as test documentation are maintained within the CM system.
ADO_DEL.1	Delivery procedures are described as part of the developer documentation. This includes also the measures taken to ensure the integrity and authenticity of the TOE during the delivery process.
ADO_IGS.1	The guidance documentation provided to the customer includes a detailed description how to install and configure the individual components that define the TOE. Additional guidance for the installation and configuration of exactly the evaluated configuration is provided as part of the guidance documentation.
ADV_FSP.1	The TSFI are identified in a separate document which points to the documents

Assurance Component	Description how the requirements are met
	describing the different interfaces.
ADV_HLD.2	A high level design document exists that describes the internal structure of the TOE into subsystems, how the security functions of the TOE are implemented and how the subsystems contribute to the security functions.
ADV_RCR.1	Correspondence between the TSF as defined in the TOE summary specification and the functional specification as well as correspondence between the functional specification and the high level design is provided in form of commented tables that show the correspondence
AGD_ADM.1	Administrator guidance documents exist for the ITIM server and adapters comprising the TOE. They describe the administrative tasks, the commands to be used and the different management aspects.
AGD_USR.1	User guidance exists for the TOE, providing instructions for users on how to use the basic functionality offered to manage their own identities and accounts.
ALC_DVS.1	The security measures for the IBM development environment are derived from the IBM Global documents that define the minimum requirements for the physical and organizational security.
ALC_FLR.1	Problems that are reported either from the development process or by a customer will result in a “defect” that is managed with DevTrack. Defects are classified with respect to their impact and one of the possible classifications is “security”. Since all defects are tracked and managed, it is easily possible to extract all security relevant defects, their status and what has been done to fix them.
ATE_COV.2	Testing is performed as functional verification testing using defined test suites in accordance with defined test procedures as described in the test plan. Coverage of security functions is provided in form of a table showing which test cases test which security functions at which interface. The table shows that all security functions and their parameter are tested at the interfaces defined in the functional specification.
ATE_DPT.1	A mapping is produced that shows the mapping of test cases to details defined in the high level design. The mapping shows that those details are covered by test cases and the test cases themselves show that the TOE operates in

Assurance Component	Description how the requirements are met
	accordance with its high level design.
ATE_FUN.1	A test plan is provided that describes the test procedures, test cases, purpose of each test and expected results. Records of actual tests performed and their results are maintained under CM.
ATE_IND.2	Independent testing is performed as part of the evaluation by the evaluation facility. The developer's test plan and test cases as well as the TOE suitable for testing will be provided to the evaluation facility such that all the test cases can be repeated by the independent evaluator.
AVA_MSU.1	An analysis of the user provided documentation describing the installation and configuration, the administrator interface and commands and the configuration files is performed to ensure that those documents are consistent and provide all the required guidance for an administrator to install, configure and administer the TOE in a secure manner.
AVA_SOF.1	A strength of function analysis is provided for the mechanisms based on permutational or probabilistic properties to demonstrate that those mechanisms have a strength of SOF-medium or better.
AVA_VLA.1	A process is in place and documented to search for vulnerabilities of the TOE using open sources of vulnerabilities on the Internet like CVE or CERT advisories. The results of this process are documented and provide the developer vulnerability analysis as required.

7. PP claims

7.1. Conformance

This Security Target claims conformance to the Identity Management Protection Profile (see section 1.3)

7.2. Security Objectives

The ST does not contain security objectives that are additional to the security objectives contained in IMPP. However, refinements have been applied to the security objectives, and the objective OE.REPOSITORY has been renamed OE.DB_PROT and iterated in OE.DIR_PROT to reflect the fact that the TOE uses two data stores in the IT environment for storage of user data.

7.3. IT Security Requirements

Please refer to chapter 5 for a discussion of IT security requirements that are additional to the IT security requirements contained in IMPP.

7.4. Terminology

The Identity Management Protection Profile identifies remote connectors for the provisioning of identities “agents”. While providing exactly the same functionality, the TOE’s connectors are called “adapters”.

8. Rationale

This chapter provides the rationale for the selection of security objectives and requirements within this Security Target.

8.1. Security Objectives Rationale

8.1.1 Security Objectives Coverage

The mapping in Table 2 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.BYPASS T.UNAUTHORIZED
O.AUDIT	P.ACCOUNTABILITY T.BYPASS
O.FEED	P.FEED
O.I&A	P.ACCOUNTABILITY T.UNAUTHORIZED
O.PROVISION	P.PROVISION

Table 2: security objectives traced back to threats and organizational security policies

The mappings in Table 3 and Table 4 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	TE.COM_ATT
OE.DB_PROT	A.RDBMS P.ACCOUNTABILITY
OE.DIR_PROT	A.DIRECTORY
OE.ENFORCEMENT	T.BYPASS
OE.MANAGED	P.PROVISION

Table 3: 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 A.CONFIGURATION
OE.AGENT	A.AGENT A.CONFIGURATION
OE.FEED	P.FEED
OE.SERVER	A.PHYS_PROT A.SERVER
OE.USER	A.USER

Table 4: security objectives for the non-IT environment traced back to threats, organizational security policies and assumptions

8.1.2 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 mitigation of 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.UNAUTHORIZED	O.ACI seeks to implement 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.
TE.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.

Table 5: 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 this audit records available to authorized users. OE.AUDIT supports the generation of audit records by providing a reliable time source. OE.DB_PROT protects the audit records that are stored in the transaction data base.
P.FEED	O.FEED requires that the TOE offers a consistent way of relating imported user data to data already present in the TOE's data store. OE.FEED covers the assumption on proper management of data in identity 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 6: 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 adapters and protect the adapter against tampering by requiring that this is ensured in the IT environment.
A.CONFIGURATION	OE.ADMIN requires secure configuration and operation of the TOE and well trained administrators that abide by the instructions provided – this ensures a proper setup of the evaluated configuration as assumed. Proper configuration of the adapters that are part of the TOE is also supported by OE.AGENT, which requires protection measures to prevent tampering with the adapter and its interfaces.
A.DIRECTORY	OE.DIR_PROT covers the assumption on TSF data and user data protection by the LDAP server in the IT environment by requiring protection of the data stored in the LDAP server.
A.PHYS_PROT	OE.SERVER requires that the ITIM server is physically protected, thus covering the corresponding assumption.
A.RDBMS	OE.DB_PROT covers the assumption on TSF data and user data protection by the transaction data base in the IT environment by requiring protection of the data stored in the RDBMS.
A.SERVER	OE.SERVER requires a configuration and operation of the TOE that limits the usage of the runtime environment for the ITIM server to TOE purposes.
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 7: sufficiency of objectives covering assumptions

8.2. 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 an ST-conformant implementation of the TOE.

8.2.1 Security Requirements Coverage

The following tables illustrate which security objectives are implemented by which security functional requirements. Table 8 indicates how each TOE security functional requirement can be traced back to at least one security objective for the TOE, Table 9 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	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

SFR	Objective
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 8: SFRs for the TOE traced back to objectives for the TOE

SFR (environment)	Objective (environment)
Managed Resources	
FPT_TDC.1	OE.MANAGED
Directory Server	
FIA_UAU.1	OE.DIR_PROT
FIA_UID.1	OE.DIR_PROT
Transaction Data Base Server	
FAU_STG.1	OE.DB_PROT
FIA_UAU.1	OE.DB_PROT
FIA_UID.1	OE.DB_PROT
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 9: SFRs for the environment traced back to objectives for the environment

8.2.2 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 rules. This objective is achieved by imposing the ITIM access control SFP in *FDP_ACC.2 (ACF)*, which is specified in *FDP_ACF.1 (ACF)*. This SFP covers, according to *FMT_MSA.1*, also access control to the security attributes 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 authorization 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*). To allow a proper relationship between authenticated users and their representation in the TOE, *FIA_USB.1* establishes a user-subject binding. *FIA_SOS.1* ensures that passwords comply with a dedicated password policy. 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 continuous password guessing.

O.PROVISION requires that accounts are only provisioned 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 access control SFP defined in *FDP_ACC.1 (ETC)*, which is applied to the export of account data (Provisioning) in *FDP_ETC.2* and specified in *FDP_ACF.1 (ETC)*. Management of this SFP (*FMT_SMF.1*) is restricted to authorized users by the ITIM access control SFP as in *FMT_MSA.1*, whereas users having the role of an administrator (*FMT_SMR.1*) are always authorized. Security attributes for the enforcement of the Provisioning access control SFP are defined in *FIA_ATD.1 (ETC)*. Restrictive default values for the definition of the Provisioning information flow SFP are provided in *FMT_MSA.3 (ETC)*. Consistent interpretation of the data provisioned to the 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.DB_PROT requires the transaction data base to protect the TSF data and user data stored against unauthorized access. 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*.

OE.DIR_PROT requires the user registry to protect the TSF data and user data stored against unauthorized access. This is achieved by implementing authentication as in *FIA_UAU.1* and identification as in *FIA_UID.1*.

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*.

8.2.3 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). No additional dependencies exist for the security functional requirements in this Security Target.

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 this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target 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	[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

SFR	Dependencies	Fulfillment of dependencies
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 10: Dependency Analysis for TOE SFRs

SFR	Dependencies	Fulfillment of dependencies
FPT_TDC.1	%	%

Table 11: Dependency Analysis for the Managed Resources in the IT environment

SFR	Dependencies	Fulfillment of dependencies
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	%	%

Table 12: Dependency Analysis for the Directory Server 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 13: Dependency Analysis for the RDBMS in the IT environment

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

Table 14: Dependency Analysis for Transaction Security in the IT environment

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

Table 15: Dependency Analysis for the Runtime Environment of the TOE in the IT environment

8.2.4 Internal Consistency and Mutual Support

Chapter 8.2.2 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 **ITIM access control SFP** 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*. Authentication of users is implemented by passwords, which are subject to a password policy as defined in *FIA_SOS.1*. Password guessing attacks are prevented by *FIA_AFL.1* Actions of users within the system is tied to 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 to 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 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 access control SFP** 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*. 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 ITIM Access Control SFP, 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 (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 **Web Application Server** (i.e. the runtime environment for the ITIM server) 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, i.e. a **LDAP user registry** and a **transaction data base**, which both 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, the **transaction data base** has to protect the audit records against unauthorized modification (*FAU_STG.1*).

Network communication between the ITIM server and adapters, 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*.

8.2.5 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 this Security Target.

The assurance level EAL3 was augmented with ALC_FLR.1 to address the flaw remediation process used within Tivoli. Since the evaluation methodology for ALC_FLR.1 has been harmonized and is also covered by the Mutual Recognition Arrangement, this was considered to be a useful augmentation for the assurance level chosen.

The ST 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.

The security functional requirement subject to a SOF rating is FIA_SOS.1 (password policy), supported by FIA_AFL.1 (authentication failure handling).

8.3. TOE Summary Specification Rationale

8.3.1 Security Functions Justification

The following table shows that the IT security functions as specified in the TOE summary specification, meet all the security functional requirements for the TOE and work together to satisfy the TOE security functional requirements.

SFR	Security Functions from the TOE Summary Specification
FAU_GEN.1	The requirement to generate audit records is met by F.Auditing, providing for the generation of audit data for the auditable events listed in FAU_GEN.1.
FAU_GEN.2	User identity association is achieved by storing the subject's DN in audit records generated as part of F.Auditing, and supported by identification of users provided by F.I&A.
FAU_SAR.1	F.Auditing offers functionality to review audit records to authorized users.
FAU_SAR.2	Access to audit records is granted based on the ITIM access control SFP realized by F.Authorization
FDP_ACC.1 (ETC)	The enforcement of the Provisioning access control SFP is provided by F.Provisioning.
FDP_ACC.2 (ACF)	The enforcement of the ITIM access control SFP is implemented by F.Authorization.
FDP_ACF.1 (ACF)	The implementation of the access control mechanism as defined in FDP_ACF.1 is provided by F.Authorization.

SFR	Security Functions from the TOE Summary Specification
FDP_ACF.1 (ETC)	The implementation of the access control mechanisms for data export is provided by F.Provisioning.
FDP_ETC.2	Export of user data is governed by the provisioning implemented by F.Provisioning.
FIA_AFL.1	Authentication failure handling is implemented by F.I&A.
FIA_ATD.1 (ACF)	User attributes for TOE users are maintained in order to implement the security functions F.Audit, F.Authorization, and F.I&A.
FIA_ATD.1 (ETC)	User attributes for persons managed by the TOE are maintained in order to implement the security function F.Provisioning.
FIA_SOS.1	The password policy is implemented by F.I&A.
FIA_UAU.2	User authentication is implemented by F.I&A, prior to any request a user can issue.
FIA_UID.2	User identification is implemented by F.I&A as part of the authentication process.
FIA_USB.1	User-subject binding is offered by F.I&A by credentials that are assigned to authenticated users.
FMT_MSA.1	F.Authorization enforces the ITIM access control SFP in order to restrict management of security attributes to authorized users.
FMT_MSA.3 (ACF)	F.Authorization provides restrictive default values for the ITIM access control SFP.
FMT_MSA.3 (ETC)	Restrictive default values for the Provisioning information flow SFP are provided by F.Provisioning.
FMT_SMF.1	Management of users, groups, and user credentials is provided by F.I&A; management of ACIs is provided by F.Authorization; management of person and account data, organizational roles, provisioning policies, workflow policies and service definitions is provided by F.Provisioning.
FMT_SMR.1	Maintenance of user roles is primarily implemented by F.I&A, the administrator role is privileged in the authorization

SFR	Security Functions from the TOE Summary Specification
	mechanisms implemented by F.Authorization.
FPT_RVM.1	F.I&A ensures that all users are authenticated prior to further action, which in turn is subject to access control by F.Authorization.
FPT_TDC.1	Consistent interpretation of imported user data is provided by F.Data_Feed.

Table 16: Mapping Security Functional Requirements to Security Functions

8.3.2 Mutual Support of the Security Functions

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.

In order to allow users (including those in the role of an administrator) the management of user (person) data, identification and authentication of users is provided by **F.I&A**. This includes the optional generation of passwords for users and the enforcement of a password policy, as well as authentication failure handling.

Management is subject to access control implemented by **F.Authorization**, which enforces access control decisions based on administrator-defined Access Control Item (ACI). Administrators themselves are not subject to any access restrictions.

Auditing of security-relevant user requests is provided by **F.Auditing**. Audit records are generated and can be reviewed by authorized users. Thus, accountability (as a result of prior authentication) and misuse detection is provided.

Policies can be defined to specify export (provisioning) and import (reconciliation and identity feed) rules, provided by **F.Provisioning** and **F.Data_Feed**.

As a result

- no transactions can be requested by users without being authenticated
- all transactions requested by users are subject to access control
- accountability for transactions is provided
- the management of person data, as well as the definition of services, service entitlements and means to import user data is controlled and restricted to authorized users

8.3.3 Rationale for Strength of Function Claim

The minimum strength of function claimed is SOF-medium. This affects the security function F.I&A and its mechanisms providing password policy enforcement and password generation. SOF-medium means that those mechanisms be resistant to attackers with a moderate attack potential, which is in line with the intended operational environment of the TOE (commercial computing environments with a medium level of security required). This corresponds as well to the definition of the attack potential as in section 3.2.

A. Appendix

A.1 Definition of Terms

Access Control Item	Controls user access by defining the access privileges of an ITIM Group or ACI principal. An ACI grants or denies the ability to perform Tivoli Identity Manager 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 Item
Adapter	Software module that is part of ITIM, but distributed remotely from the ITIM server 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. The adapters that are part of the evaluated configuration are identified in section 2.8.
Administrator	An ITIM User being member of the Administrator Group. An Administrator is not subject to any access control.
Agent	The Identity Management Protection Profile identifies remote connectors for the provisioning of identities “agents”. While providing exactly the same functionality, the TOE’s connectors are called adapters in the product documentation (see Adapter).
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.

BPOrganization	Business Partner Organization. One of the types of subsidiary entities that can be added to an Organization.
BPPerson	Business Partner Person. A Person in a Business Partner Organization.
Business Unit	A subsidiary entity of an Organization.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Connector	Connectors support a specific resource. One element of the connector, the service provider, executes at the ITIM Server machine to cause data to be delivered to the managed resource. The other element of the connector, the adapter, executes at the managed resource. The connector is responsible for receiving directives from the ITIM Server and implementing changes at the managed resource, using the primitives of the managed resource.
Delegation	The act of empowering one to act for another. In the ITIM context, this means giving another ITIM user, or group of users, a set of permissions to perform operations using ITIM.
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.
DSMLv2	Directory Services Markup Language.
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 identities (represented by roles).
Entity	1) A Person or object for which information is stored. 2) One of the following classes, as referred to by the Tivoli Identity Manager system: Person, BPPerson, Organization, BPOrganization
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	See ITIM Group.
HR Feed	Human Resources Feed. See Identity Feed.
HTML	Hypertext Markup Language.
HTTP	Hypertext Transfer Protocol.
Identity	See Person.
Identity Feed	An automated process in which the Tivoli Identity Manager system imports user data from a human resources database or file and feeds the information into the Tivoli Identity Manager directory.
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.
ITIM	IBM Tivoli Identity Manager. Also: TIM.
ITIM Group	An ITIM Group delegates management rights to ITIM Users on the ITIM server. Management can be restricted to only change its own password, over being able to manage Organizational Roles and membership of other identities to those roles, up to being allowed to perform system management for the TOE. Adding an identity to at least one ITIM Group implies creation of an account for that identity on the ITIM server.
ITIM User	A Person provisioned with an ITIM account, i.e. an account to access the TOE. This requires an entitlement for the Person to the ITIM Service. Users can be delegated (by membership of an ITIM Group) to perform certain management actions within ITIM

J2EE	Java [TM] 2 Platform, Enterprise Edition
J2SE	Java [TM] 2 Platform, Standard Edition
JDBC	Java Database Connectivity.
JMS	Java Messaging Service.
LDAP	Lightweight Directory Access Protocol.
LDAP v3	LDAP Version 3.
Managed Resource	An item that can be owned or accessed by a set of identities. This resource will be represented as a service in ITIM. Provisioning policies will entitle the appropriate identities to ownership of, or access to, a resource. Adapters enforce the entitlements on the resources. Examples of resources are NT domains, SAP systems, RACF systems, mail servers, and databases. The adapters that are part of the evaluated configuration are identified in section 2.8.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organization	A logical construct that stands on the top of an organizational hierarchy (Organization Tree) managed with Tivoli Identity Manager. Generally, an organization represents a company.
Organizational Element	Organization, Organizational Unit, Location, Business Partner Organization, or Administrative Domain
Organizational Role	A named set (group) of identities. The determination of which identities should belong to a role is specific to the customer's business objectives.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.
Orphan Accounts	Accounts on a Managed Resource whose owner in the Tivoli Identity Manager system cannot be determined.
Person	Object within ITIM representing a human or computing entity that is being managed, or controlled, and audited. Persons can be entitled (by membership of an Organizational Role that is subject to a Provisioning Policy) to use services in the IT environment. In such case of account provisioning, a Person will be represented as a user on a resource. This

	relationship is modelled in ITIM as a Person *owning* zero up to many accounts.
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 a set of identities (i.e. to the members of an Organizational Role) by entitling them to have accounts on dedicated services in the IT environment.
RDBMS	Relational Data Base Management System. ITIM employs a RDBMS in the IT environment as transaction database, which includes storage of audit records.
Refinement	The addition of details to a component.
Resource	See Managed Resource.
Role	See Organizational Role.
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	Object that represents a managed resource that supports actual users. A service is protected via the creation of policies. The user information on the service is represented with accounts. These accounts are updated by ITIM through a connector.
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.
TIM	Tivoli Identity Manager. Also: ITIM.
TOE	Target of evaluation
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. The TOE security functions (TSF) are identified and described in the TOE Summary Specification in chapter 6.
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. The TOE Security Policy (TSP) is modeled in the security functional requirements for the TOE in chapter 5.
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
UML	Unified Modeling Language.
User	See ITIM User.
User data	Data created by and for the user that does not affect the operation of the TSF.
WAS	Web Application Server.
XML	Extensible Markup Language.
IT	Information Technology

A.2 References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3: Introduction and General Model; Version 2.2, Revision 256

[CEM] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.2, Revision 256

END OF DOCUMENT