Primavera® P6™ Enterprise Project Portfolio Management

(Version 6.2.1)

Security Target

Version 1.2.5
July 6, 2009

Prepared for:
Oracle Primavera
Three Bala Plaza West
Bala Cynwyd, PA 19004

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Primavera P6 Enterprise Project Portfolio Management (Version 6.2.1). The TOE is a project management product that is implemented using a centralized (i.e. client/server) architecture. The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section describes the assumptions about the environment and method of use of the TOE and the threats that are to be countered by the TOE and its IT environment.
- Section 4 – TOE Security Objectives
  This section details the security objectives for the TOE and its environment.
- Section 5 – IT Security Requirements
  This section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL4.
- Section 6 – TOE Summary Specification
  This section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title –Primavera® P6™ Enterprise Project Portfolio Management (Version 6.2.1) Security Target

ST Version – Version 1.2.5

ST Date – July 6, 2009

TOE Identification –Primavera P6 Enterprise Project Portfolio Management (Version 6.2.1)

TOE Developer – Oracle Primavera

Evaluation Sponsor – Oracle Primavera

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 2, September 2007.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 2, September 2007.

- Part 3 Conformant
- EAL 4 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is Primavera P6 Enterprise Project Portfolio Management, (Version 6.2.1).

The TOE is a project management product that is implemented using a centralized (i.e. client/server) architecture. The TOE can be used to manage both projects and resources, where resources can represent either people or materials, depending on how the project is defined within the TOE.

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE can be used to plan and control thousands of projects. Project data is stored in a central project management database that is located in the IT environment. The TOE can also provide centralized resource management, including providing a timesheet capability. Resources can represent either people or materials. The timesheet capability allows resources to record time against projects that they are assigned to that are being managed by the TOE. The TOE can be used to plan and control a large number of projects as follows.

- Project management capability – allows users to plan and control thousands of projects. Project data is stored in a central project management database. Project management capabilities include centralized resource management, including resource timesheet approval and the ability to communicate with project resources web-based timesheet interfaces.
- Methodology management capability – allows users to author and store methodologies, which are also called project plan templates. Methodology management capabilities include providing the ability to define project management methodologies, which are called “best practices”, and store them in a central methodology management database.
- Timesheets capability – allows users to enter and track time in a timekeeping system. Team members use timesheets to enter information for assignments across projects, including recording time against a project.

The TOE restricts the ability to access it by requiring users to identify themselves and by authenticating that identity using an LDAP server in the IT environment. Furthermore, it provides the capability of controlling access to user data through access control policies. Lastly, it provides administrators with the ability to administer security attributes to manage the security of the TOE.

2.2 TOE Architecture

The TOE organizes project management using two primitives: projects and resources. Projects represent work that needs to be done while resources represent what the project manager has at his disposal to get those things done. A project represents a collection of related activities focused on achieving a common goal. Resources represent people, materials, equipment, and other assets that are used to accomplish the activities that make up the project.

The TOE arranges projects in a hierarchy called the Enterprise Project Structure (EPS). The EPS can be subdivided into as many as 50 levels or nodes, as needed, to represent project organization in the enterprise. Nodes at the highest, or root, level might represent divisions within a company, project phases, site locations, or other major groupings that meet the needs of an organization, while projects always represent the lowest level of the hierarchy. Every project in the enterprise must be included in an EPS node.

To restrict or grant access to projects and their data, administrators associate project profiles with users. A project profile is a role-based profile that grants privileges to specific project data. Project profiles are linked to users through one or more OBS assignments. The OBS (Organizational Breakdown Structure) is a global hierarchy that represents the managers responsible for the projects in an enterprise. Administrators assign responsibilities to specific projects and work within projects by assigning OBS elements to various levels of the EPS. Each node in the EPS must have an OBS element assigned. The combination of the project profile/user assignment to an OBS assignment, and the OBS assignment to the EPS, determines which projects and data the user can access. The TOE assigns the root OBS element to an EPS element by default.

The TOE arranges resources in another hierarchy, separate from the OBS, called the resource hierarchy. The resource hierarchy defines a series of nodes to which users may be assigned. The position of the node in the resource hierarchy determines the resources to which the user has access. A user will be granted access to the resource node to which that user is assigned and any nodes below that node (referred to as child nodes) in the hierarchy branch. The user can be assigned to no more than one resource node in the resource hierarchy. If the user is not assigned to a resource node, the user will not have access to any resources.

The TOE can be described in terms of the following components:

- Client interface types – There are three types of client interfaces provided by the TOE.
    - Heavy client applications – Provide user interfaces to access project management and methodology management application services:
        - Project Management: allows management of data regarding projects and resources – including user data.
        - Methodology Management: allows authoring and management of project plan templates. These templates represent best practices and standards for project creation. Methodology data are a subset of project data.
    - Web-based client interfaces – Provide user interfaces to access project management and timesheet services:
        - Used to access light-weight project management and
        - Used to access timekeeping system capabilities.
    - Application programming interfaces – provides direct access to project management and methodology management data through a JDBC interface with the project database.
- P6 Web Access Application Server – Provides lightweight[1] project management and methodology management capabilities.
- Group Server – Provides timekeeping system capabilities.
- Primavera Stored Procedures – Provide automation of database tasks. These stored procedures aggregate multiple database commands as atomic behaviors. They do not enable any access to the database that isn't available by making direct calls to the database.

[1] Lightweight project management represents the ability to manage a subset of the project management data. Access to security management data (including access control and user data) is not provided via this interface.

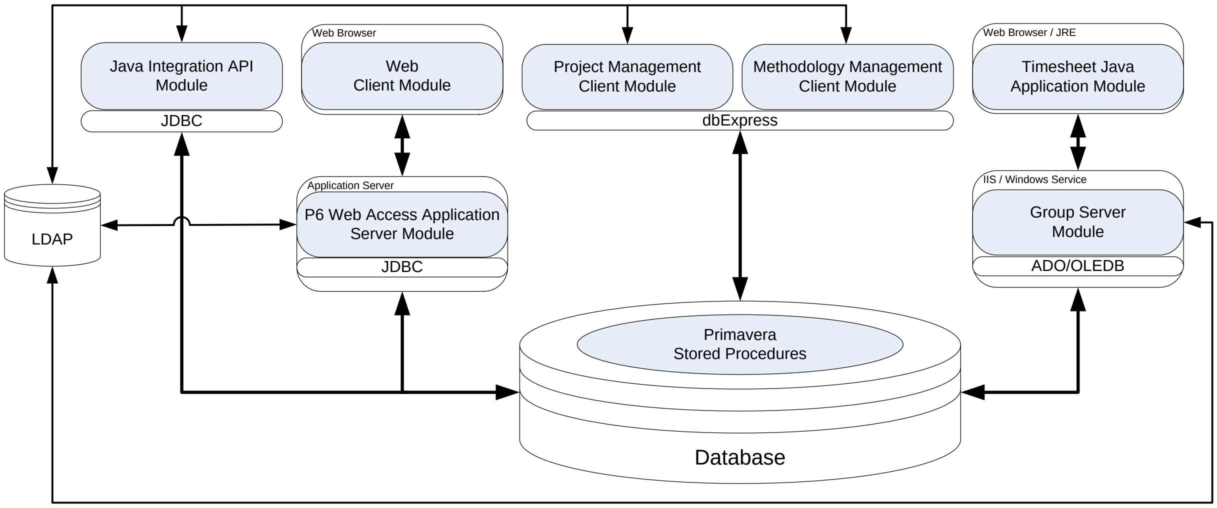
Java Integration API Module
JDBC
Web Browser
Web Client Module
Project Management Client Module
Methodology Management Client Module
dbExpress
Web Browser / JRE
Timesheet Java Application Module
LDAP
Application Server
P6 Web Access Application Server Module
JDBC
IIS / Windows Service
Group Server Module
ADO/OLEDB
Primavera Stored Procedures
Database

Figure 1 - Primavera (v6.2.1) Logical Overview

Note: TOE components are represented in shaded blocks.

The intended environment of the TOE can be described in terms of the following components:

- Web Client Hosts (Timesheet client)
  - Microsoft Internet Explorer 6 (SP3) on Microsoft Windows XP (SP3), Microsoft Internet Explorer 7 on Microsoft Windows Vista SP1 (Business Edition), or Firefox 3.0.3 on Ubuntu Linux 7.0.4
  - Sun Java Runtime Environment (JRE) JRE 1.5.0_18 or JRE 1.6.0_14.
- Web Client Hosts (Web Access client)
  - Microsoft Internet Explorer 6 (SP3) on Microsoft Windows XP (SP3), Microsoft Internet Explorer 7 on Microsoft Windows Vista SP1 (Business Edition)
  - Sun Java Runtime Environment (JRE) JRE 1.5.0_18 or JRE 1.6.0_14.
- Application Client Hosts – Provides a runtime environment for client-side TOE application components (Project Management, and Methodology Management Client Modules).
  - Hardware:
    - 1 GB RAM free and
    - 1 GB available hard-disk space (per module).
  - Operating System:
    - Microsoft Windows XP (SP3), or
    - Microsoft Windows Vista (Business Edition, SP1).
- Database Server – Used to store TOE configuration information as well as project, methodology, and timesheet data. Database requirements:
  - Microsoft SQL Server 2005 (SP2) on Windows Server 2003 R2 (SP2), or Windows 2008 Server (SP1) with Microsoft sqljdbc.jar driver: version 1.2.2828.100
  - Oracle version 10.2.0.3 on Windows Server 2003 R2 (SP2) or Red Hat Enterprise Linux AS 5.0 with Oracle OJDBC5.jar driver: version 11.1.0.6.0
  - Oracle version 11.1.0.6 on Windows Server 2003 R2 (SP2), or Windows 2008 Server (SP1), or Red Hat Enterprise Linux AS 5.0 with Oracle OJDBC5.jar driver: version 11.1.0.6.0

Note: For database server hardware sizing, please refer to Primavera Administrator's Guide – Database Server Sizing Guide.

- LDAP Server – Used to store authentication information and to authenticate TOE users.
    - Microsoft Active Directory on Windows Server 2003 R2 (SP2)
    - SunOne Directory Server v.5.2 on Windows Server 2003 R2 (SP2)
- P6 Web Access Server:
    - Hardware:
        - 1 GB RAM free and
        - 1 GB available hard-disk space;
    - Operating System / Web Server
        - Microsoft Windows Server 2003 R2 (SP2) with Internet Information Services v 6.0, or
        - Microsoft Windows Server 2008 (SP1) with Internet Information Services v 7.0, or
    - Application Server
        - JBoss 4.0.5 with Sun Java 2 JDK 1.5.0_15
        - BEA WebLogic Express (ISV) 10 MP1 with Sun JDK 1.5.0_11,
        - BEA WebLogic Enterprise Edition 10 MP1 with Sun Java 2 JDK 1.5.0_11,
        - IBM WebSphere Application Server 6.1 fp17 with IBM Java 2 JDK 1.5,
- Group Server:
    - Hardware:
        - 512 MB RAM free and
        - 200 MB available hard-disk space.
    - Operating System / Web Server:
        - Windows Server 2003 R2 (SP2) with Internet Information Services v 6.0.

Note that there is no separate administrator console application to manage TOE services. The heavy client application can be used for example to manage users, while the web-based client can be used to manage projects.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- P6 Web Access server application,
- Group Server application,
- Java Integration API library,
- Heavy client applications, and
- Database stored procedures.

Note that web-based client interfaces are provided by the P6 Web Access server and the Group Server applications.

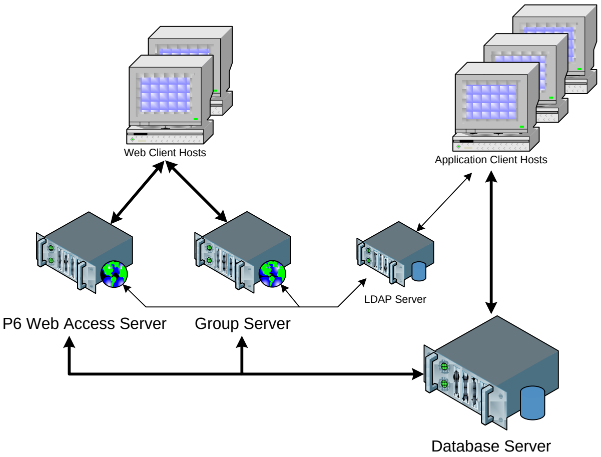

Figure 2 - Typical Primavera (v6.2.1) Physical Configuration

The physical boundaries of the TOE extend to the process boundaries of the applications developed by the vendor. Process isolation and the execution environment are provided by the underlying operating system. The vendor does not own nor does the vendor have any control over the interfaces between physically separate parts of the TOE. The TOE relies on access to interfaces that facilitate communications with the database server, including the Java Database Connectivity (JDBC) interface, the ActiveX Data Objects (ADO) interface, and the dbExpress interface. Furthermore, network communications rely on the TCP/IP network protocol and are configured to use SSL connections. Optional email features of the TOE use SMTP or MAPI interfaces, and rely on SMTP/POP or MAPI servers in the IT environment.

Physical Elements

	Database Server	P6 Web Access Server	Group Server	Web Client Hosts	Application Client Hosts	LDAP Server
Logical Elements	Database	Application Server	IIS/Windows Service	Web Browser	Project Management Client Module	LDAP
	Primavera Stored Procedures	P6 Web Access Application Server Module	Group Server Module	Web Client Module	Methodology Management Client Module	
		JDBC	ADO/OLEDB	Web Browser / JRE	dbExpress	
				Timesheet Java Application Module	Java Integration API Module	
					JDBC	

Table 1 – Mapping Logical Elements to Physical Elements

2.2.2 Logical Boundaries

This section summarizes the security functions provided by Primavera P6 Enterprise Project Portfolio Management, (Version 6.2.1):

- User data protection,
- Identification and authentication, and

- Security management.

2.2.2.1 User data protection

The TOE implements three separate access control policies, one controls access to EPS nodes, another controls access to resources, and the third controls access to methodology objects. Access control decisions are made differently for each type of object. Users access EPS nodes, resources and methodologies using either heavy or web clients.

2.2.2.2 Identification and authentication

The TOE defines users in terms of security attributes comprised of user identity and global profiles, which contain authorizations corresponding to functions a role may perform. The TOE offers no TSF-mediated functions using its heavy and web clients until the user is identified. Authentication is performed by an LDAP server in the IT environment.

2.2.2.3 Security management

Through the Project Management client module, the TOE provides an administrator with the ability to manage access controls on EPS nodes and resource objects and to manage user data.

Managing methodology access control data is controlled by interfaces in the Methodology Management client module.

The TOE maintains both administrator and user roles.

2.3 TOE Documentation

Primavera P6 Enterprise Project Portfolio Management (Version 6.2.1) offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features:

- Primavera P6 Administrator’s Guide
- P6 Methodology Management Reference Manual
- Primavera P6 Project Management Reference Manual
- Primavera P6 Integration API Administrator’s Guide
- P6 Web Access Help
- Primavera Timesheets Help
- Primavera Integration API Programmer’s Reference
- Primavera Integration API Javadoc
- Evaluated Configuration for Primavera P6 Enterprise Project Portfolio Management (Version 6.2.1)

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 4) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T. MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized user to gain access to the TOE.

T. TSF_COMPROMISE

A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

T. UNAUTH_ACCESS

An authorized user may gain unauthorized access (view, modify, delete) to user data through the TOE.

3.2 Assumptions

A.LOCATE

The TOE will be located within controlled access facilities and connected to networks that are protected from external tampering by a network firewall, which will prevent unauthorized physical access and mitigate unauthorized network access.

A.ADMIN

The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.ACCESS The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.

O.USER_IDENTIFICATION The TOE will uniquely identify users.

O.MANAGE The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.

4.2 Security Objectives for the Environment

OE.TOE_PROTECTION The IT environment will protect the TOE and its assets from external interference or tampering.

OE.USER_AUTHENTICATION The IT environment will verify the claimed identity of users.

4.3 Security Objectives for the Non-IT Environment

OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

OE.PHYCAL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been drawn from version 3.1 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Primavera P6 Enterprise Project Portfolio Management (Version 6.2.1).

Table 2 - TOE Security Functional Components

Requirement Class	Requirement Component
FDP: User data protection	FDP_ACC.2a: Complete access control
	FDP_ACC.2b: Complete access control
	FDP_ACC.2c: Complete access control
	FDP_ACF.1a: Security attribute based access control
	FDP_ACF.1b: Security attribute based access control
	FDP_ACF.1c: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.1c: Management of security attributes
	FMT_MSA.1d: Management of security attributes
	FMT_MSA.1e: Management of security attributes
	FMT_MSA.3a: Static attribute initialization
	FMT_MSA.3b: Static attribute initialization
	FMT_MSA.3c: Static attribute initialization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles

5.1.1 User data protection (FDP)

5.1.1.1 Complete access control (FDP_ACC.2a)

FDP_ACC.2a.1 The TSF shall enforce the [**Project Access Control Policy**] on [**the following subjects and objects:**

a.) **subjects: project users**

b.) **objects: EPS nodes**]

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

FDP_ACC.2a.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.1.1.2 Complete access control (FDP_ACC.2b)

FDP_ACC.2b.1 The TSF shall enforce the [**Methodology Access Control Policy**] on [**the following subjects and objects:**

a.) **subjects: methodology users**

b.) **objects: methodologies**]

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

FDP_ACC.2b.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.1.1.3 Complete access control (FDP_ACC.2c)

FDP_ACC.2c.1 The TSF shall enforce the [**Resource Access Control Policy**] on [**the following subjects and objects:**

a.) **subjects: project users**

b.) **objects: resources**]

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

FDP_ACC.2c.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.1.1.4 Security attribute based access control (FDP_ACF.1a)

FDP_ACF.1a.1 The TSF shall enforce the [**Project Access Control Policy**] to objects based on the following: [**security attributes:**

a.) **subject security attributes:**

- **user identity**
- **global profile**
- **project profile**

b.) **object security attributes:**

- **EPS node identifier**
- **OBS elements**].

FDP_ACF.1a.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a.) **the requested access is allowed if:**

- **if the OBS element associated with the requested EPS node contains the user identity, and**
- **if the project profile associated with the user identity possesses the necessary privilege to perform the requested operation**

b.) **otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1a.3**].

FDP_ACF.1a.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**if the user identity is associated with either the Admin Superuser (project) role (via the global profile) or the Project Superuser role (via the project profile), the requested access is allowed**].

FDP_ACF.1a.4 The TSF shall explicitly deny access of subjects to objects based on the [**there are no explicit access denial rules**].

5.1.1.5 Security attribute based access control (FDP_ACF.1b)

FDP_ACF.1b.1 The TSF shall enforce the [**Methodology Access Control Policy**] to objects based on the following: [**security attributes:**

a.) **subject security attributes:**

- **user identity**
- **methodology global profile**
- **methodology profile**

b.) **object security attributes:**

- **methodology name**].

FDP_ACF.1b.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a.) **the requested access is allowed if:**

- **if the user identity is associated with the methodology name, and**
- **if the methodology profile allows requested operation**

b.) **otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1b.3**].

FDP_ACF.1b.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

a.) **the requested access is allowed if the user possesses the Admin Superuser (methodology) role (via the methodology global profile),**

b.) **the requested access is allowed if the user possesses the Methodology Superuser role (via the methodology profile) and the requested access is either to read from or to write to the methodology**].

FDP_ACF.1b.4 The TSF shall explicitly deny access of subjects to objects based on the [**there are no explicit access denial rules**].

5.1.1.6 Security attribute based access control (FDP_ACF.1c)

FDP_ACF.1c.1 The TSF shall enforce the [**Resource Access Control Policy**] to objects based on the following: [**security attributes:**

a.) **subject security attributes:**

- **user identity**
- **global profile**

b.) **object security attributes:**

- **resource identity**
- **resource parent**].

FDP_ACF.1c.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a.) **the user identity is granted 'All Resource Access', or**

b.) **the user identity is associated with the resource identity of the requested resource, or**

c.) **the user identity is associated with the resource identity of a parent resource of the requested resource,**

d.) **otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1c.3**].

FDP_ACF.1c.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**if the user identity is associated with the Admin Superuser (project) role (via the global profile), the requested access is allowed**].

FDP_ACF.1c.4 The TSF shall explicitly deny access of subjects to objects based on the [**there are no explicit access denial rules**].

5.1.2 Identification and authentication (FIA)

5.1.2.1 User attribute definition (FIA_ATD.1)

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

a.) **user identity**

b.) **global profile**].

5.1.2.2 User identification before any action (FIA_UID.2)

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

5.1.3 Security management (FMT)

5.1.3.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the [**Project Access Control Policy**] to restrict the ability to [***modify***] the security attributes [**OBS element assignment to EPS node**] to [**Admin Superuser (project), Project Superuser, Authorized user role**].

5.1.3.2 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the [**Methodology Access Control Policy**] to restrict the ability to [***modify***] the security attributes [**user identity association with methodology name**] to [**Admin Superuser (methodology), Authorized user**].

5.1.3.3 Management of security attributes (FMT_MSA.1c)

FMT_MSA.1c.1 The TSF shall enforce the [**Resource Access Control Policy**] to restrict the ability to [***modify***] the security attributes [**user identity association with resource identity, resource parent**] to [**Admin Superuser (project), Authorized user**].

5.1.3.4 Management of security attributes (FMT_MSA.1d)

FMT_MSA.1d.1 The TSF shall enforce the [**Project Access Control Policy**] to restrict the ability to [***manage***] the security attributes [**of project users**] to [**Admin Superuser (project), Authorized user**].

5.1.3.5 Management of security attributes (FMT_MSA.1e)

FMT_MSA.1e.1 The TSF shall enforce the [**Methodology Access Control Policy**] to restrict the ability to [***manage***] the security attributes [**of methodology users**] to [**Admin Superuser (methodology), Authorized user**].

5.1.3.6 Static attribute initialization (FMT_MSA.3a)

FMT_MSA.3a.1 The TSF shall enforce the [**Project Access Control Policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3a.2 The TSF shall allow the [**Admin Superuser (project), Project Superuser, Authorized user role**] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.7 Static attribute initialization (FMT_MSA.3b)

FMT_MSA.3b.1 The TSF shall enforce the [**Methodology Access Control Policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The TSF shall allow the [**Authorized user**] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.8 Static attribute initialization (FMT_MSA.3c)

FMT_MSA.3c.1 The TSF shall enforce the [**Resource Access Control Policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3c.2 The TSF shall allow the [**Admin Superuser (project), Authorized user**] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.9 Specification of Management Functions (FMT_SMF.1)

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

a.) **manage projects**
b.) **manage methodologies**
c.) **manage resources**
d.) **manage users**].

5.1.3.10 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [

a.) **Admin Superuser (project)**
b.) **Admin Superuser (methodology)**
c.) **Project Superuser**
d.) **Methodology Superuser**
e.) **Authorized user**].

Application Note: The role of "Authorized user" represents a user assigned any of the global project or methodology privileges that grant the capability to perform a security management action as specified in the SFRs.

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

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 3 - EAL4 Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.4: Complete functional specification
	ADV_IMP.1: Implementation representation of the TSF
	ADV_TDS.3: Basic modular design
AGD: Guidance Documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle Support	ALC_CMC.4: Production support, acceptance procedures and automation
	ALC_CMS.4: Problem tracking CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.2: Testing: security enforcing modules
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3: Focused vulnerability analysis

5.2.1 Development (ADV)

5.2.1.1 Security architecture description (ADV_ARC.1)

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

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

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

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

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

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

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

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

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

5.2.1.2 Complete functional specification (ADV_FSP.4)

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Implementation representation of the TSF (ADV_IMP.1)

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

5.2.1.4 Basic modular design (ADV_TDS.3)

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

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

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

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

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

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

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

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

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

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Production support, acceptance procedures and automation (ALC_CMC.4)

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

ALC_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Problem tracking CM coverage (ALC_CMS.4)

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.3.5 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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

5.2.3.6 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

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

5.2.4 Tests (ATE)

5.2.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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

5.2.4.2 Testing: security enforcing modules (ATE_DPT.2)

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

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

5.2.4.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

5.2.4.4 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Focused vulnerability analysis (AVA_VAN.3)

AVA_VAN.3.1D The developer shall provide the TOE for testing.

AVA_VAN.3.1C The TOE shall be suitable for testing.

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

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions and how the TOE meets the security functional requirements.

6.1 TOE Security Functions

6.1.1 User data protection

The TOE implements three separate discretionary access control policies:

- Project Access Control Policy,
- Methodology Access Control Policy, and
- Resource Access Control Policy.

The TOE objects that are subject to the access control policies are EPS nodes (including projects), methodologies, and resources.

- EPS nodes are subject to the Project Access Control Policy,
- Methodology objects are subject to the Methodology Access Control Policy, and
- Resource objects are subject to the Resource Access Control Policy.

The TOE provides a fine-grained access control model, based on privileges granted via global profiles, project profiles, and methodology profiles. Refer to Part 5 of the Primavera P6 Administrator's Guide for information regarding specific privileges.

Please note that in a default installation of the TOE the only global, project, and methodology profiles defined are the built-in profiles that define the Admin Superuser (projects), Admin Superuser (methodologies), Project Superuser, and Methodology Superuser roles, and the "No Global Privileges" global profile. The Admin Superuser has the discretion to create additional global, project and methodology profiles and to assign users to those profiles.

6.1.1.1 Project Access Control Policy

Projects are objects that are used to manage tasks and resources used to perform tasks. Projects include, for example, information about task start dates and task durations.

There are two important constructs that must be understood in order to comprehend access control in the TOE.

1) The Organizational Breakdown Structure (OBS) is a global hierarchy that represents the management structure of the organization, from top-level personnel down through the various levels of the business. Each element in the OBS represents a manager responsible for the projects being managed by the enterprise.
2) The Enterprise Project Structure (EPS) is a hierarchy that represents the breakdown of projects in the enterprise. Each node in the EPS might represent divisions within the organization, project phases, site locations, or other major groupings that meet the needs of the organization. The lowest level node of the EPS hierarchy is always the individual projects in the enterprise. Every project that will be managed by the TOE must be represented by an EPS node. Each EPS node is represented by an EPS node identifier – which is the name of the EPS node.

When project users are created they are assigned a user identifier and they must be associated with a global profile. Global profiles define a user's access to application-wide information and settings. Each user must be assigned a global profile. There are two default global profiles, "Admin Superuser" and "No Global Privileges". The Admin Superuser global profile has access to all project application global data while the no global privileges global profile prevents access to all project application global data. At least one user must be assigned to the Admin Superuser global profile. If only one user is assigned to this profile, that user cannot be deleted.

Users are assigned to OBS elements. Multiple users may be assigned to the same OBS element and/or each user may be assigned to multiple OBS elements. When a user is assigned to an OBS, a “Project Profile” can be associated with the user to authorize access to projects. The project profile specifies a set of project privileges associated with that particular user for that OBS element. The “Project Superuser” project profile is a default project profile that contains all project privileges. The full set of project privileges are specified in the “Defining Project Profiles” section of the Administering Users and Security chapter of the Primavera Administrator’s Guide.

An OBS element is assigned to an EPS node. The act of assigning the OBS element to an EPS node provides the members of that OBS element with the access specified by their respective project profiles to that EPS node and all child nodes of that EPS node. The EPS level to which the OBS is assigned determines the nodes/projects the associated users can access. The access provided by this assignment is only applicable to the EPS node and children down the hierarchy branch[2] – no access flows up the hierarchy. Only one OBS element can be assigned to each EPS level. If a user is assigned to either the Admin Superuser global profile or the Project Superuser project profile, the user is granted access to all projects and project data.

In summary, the combination of the user/project profile assignment to an OBS, and the subsequent assignment of the OBS to the EPS node determines the users’ access to projects and project data, as depicted in the following diagram.

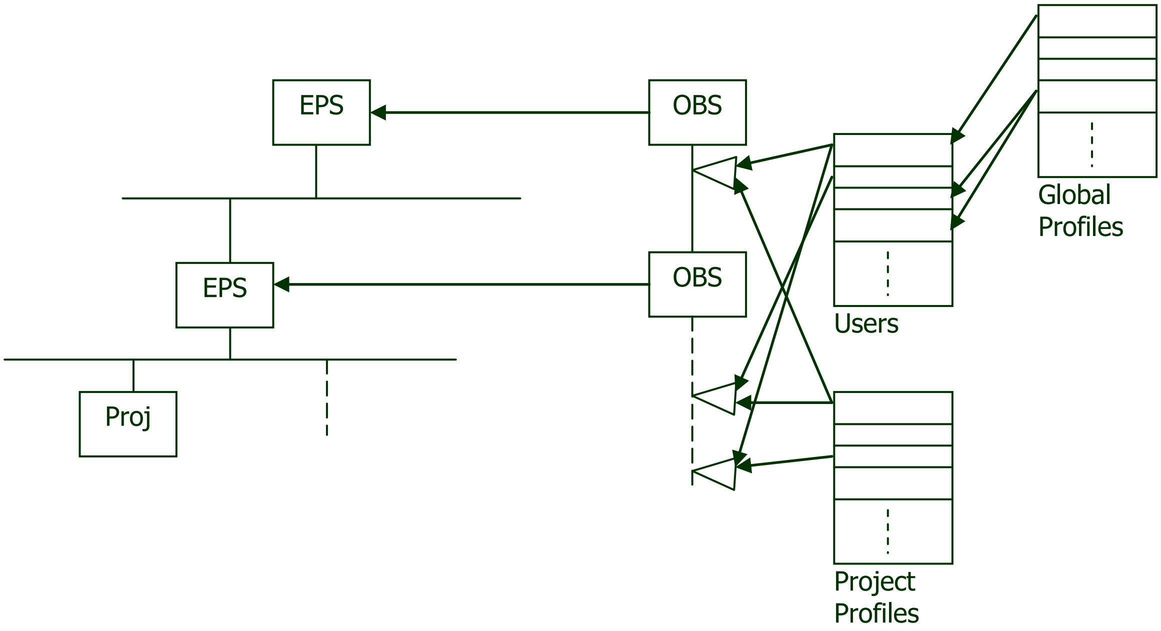

Figure 3 – User Access To Projects

6.1.1.2 Methodology Access Control Policy

Methodologies are objects that define project templates. A methodology object can be used to create a project object. Methodologies are used to capture and store an organization’s best practices, in terms of how projects should be defined.

The Methodology access control policy uses its own independent set of users, global profiles, and methodology profiles. No security data is shared between the project management and methodology management access control policies. Each Methodology object is identified by a Methodology name. Methodology profiles are not assigned to OBS elements (as in the project management access control policy). Methodology profiles (which define allowed operations) are assigned to individual methodology users. There is no EPS in the methodology management access control policy.

[2] If a user is assigned, via OBS assignments, to multiple nodes in the EPS hierarchy, an assignment at a lower node aggregates all of the user’s permissions from higher nodes in the hierarchy (e.g. access flows down the hierarchy branch).

When methodology users are created they are assigned a user identifier and they must be associated with a methodology global profile. Methodology global profiles define a user's access to application-wide information and settings. Each user must be assigned a methodology global profile. There is one default methodology global profile: "Admin Superuser". The Admin Superuser methodology global profile has access to all methodology application global data. At least one user must be assigned to the Admin Superuser methodology global profile. If only one user is assigned to this profile, that user cannot be deleted.

A methodology profile specifies a set of methodology privileges. The full set of methodology privileges are specified in the "Create methodology profiles" section of the Administering Users and Security chapter of the Primavera Administrator's Guide

Access control for methodologies is defined by assigning a methodology user to a methodology name. When a methodology user is assigned to a methodology name, that methodology user is associated with a methodology profile. The methodology profile specifies the operations that the methodology user may perform on that methodology. If a methodology user is assigned to either the Admin Superuser methodology global profile or the Methodology Superuser methodology profile, the user is granted access to all methodologies and methodology data.

In summary, the assignment of a methodology user to a methodology and the assignment of the security profile to that methodology determine the methodology user's access to methodologies and methodology data.

6.1.1.3 Resource Access Control Policy

Resources are objects that are used to track the people, materials or equipment used to perform tasks for reporting and/or billing purposes.

Resources are organized in a hierarchy, separate from the OBS, called the resource hierarchy.

The resource access control policy restricts a user's access to resources. Each project user can have access to all resources, no resources, or a subset of resources in the resource hierarchy. The user's access to resources is governed by the resource to which the user is assigned (the resource identity with which the user is associated), and the structure of the resource hierarchy. The position of the assigned resource in the resource hierarchy determines the user's resource access. When a project user logs in to the TOE and accesses the resource hierarchy, the user will only see the resource node to which the user is assigned and any children of that node in the hierarchy. A resource's "parent" is any higher level resource in the same branch of the resource hierarchy. Only one resource node can be assigned to each project user.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2a, FDP_ACF.1a: All subjects are subject to the Project Access Control Policy for all available operations on projects.
- FDP_ACC.2b, FDP_ACF.1b: All subjects are subject to the Methodology Access Control Policy for all available operations on methodologies.
- FDP_ACC.2c, FDP_ACF.1c: All subjects are subject to the Resource Access Control Policy for all available operations on resources.

6.1.2 Identification and authentication

The TOE defines users in terms of:

- user identity and
- global profile.

The TOE provides its own username and password authentication mechanism but use of this mechanism is not supported in the evaluated configuration. SSO authentication is not supported in the evaluated configuration. The only authentication mechanism the product supports in the evaluated configuration is LDAP authentication. In order to access the TOE, a user account including a user identity must be created for the user. When a user accesses the

TOE a valid user identity and password must be entered. The TOE relies on the LDAP server in the IT environment to authenticate the user before accessing any other TOE interfaces.

The TOE defines more than one type of user. The TOE defines one set of users that are subject to the project management access control policy and the resource access control policy. The TOE defines another set of users that are subject to the methodology access control policy. User information for each set of users is maintained separately. The user in this case would have two separate user accounts, each with its own user identity and global profile.

The TOE relies on an LDAP server in the environment to authenticate users. The TOE does not perform any user authentication in the evaluated configuration.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE defines users in terms of user identities and global profiles.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security management

The TOE defines the following roles:

- Admin Superuser (project),
- Admin Superuser (methodology),
- Project Superuser,
- Methodology Superuser, and
- Authorized user.

A user possessing the Admin Superuser (project) role can access project objects and project application global data. A user possessing the Admin Superuser (methodology) role can access methodology objects and methodology application global data. A user possessing the Project Superuser role can access project objects. A user possessing the Methodology Superuser role can access methodology objects. Users that do not possess a Superuser role are simply considered "users".

The TOE implements roles using profiles that contain information that defines the functions that a role may perform. The Admin Superuser (project) profile allows complete access to projects, resources and global project application data. The Admin Superuser (methodology) profile allows complete access to methodologies and global methodology application data. The Project Superuser profile allows complete access to projects and project data. Project users can be authorized to access projects and global project data. Methodology users can be authorized to access methodologies and methodology global data. The Methodology Superuser profile grants read-write privileges to methodologies and methodology data. Methodology Access Control Policy authorizations include individual authorizations to create and delete methodologies.

The TOE provides administrator interfaces to perform the following:

- manage projects,
- manage methodologies,
- manage resources, and
- manage users.

The TOE administrator interfaces consist of the GUI interfaces provided by the heavy clients. There are no other interfaces to manage the TSF. The TOE restricts access to management functions that are accessible using the client. For example, while a user who does not possess a Superuser role and a user that possesses a Project Superuser role may both access instances of the heavy client, the user who does not possess a Superuser role would not be able to access restricted management interfaces.

Client connections are protected from disclosure and from modification using SSL which is provided by the web browser and the application servers in the IT environment. The setup, configuration, and operation of SSL falls entirely in the IT environment. The TOE has no ability to manage SSL and TOE administrators have no inherent (TOE provided) ability to impact the use, configuration, or management of SSL, other than to configure TOE modules to communicate through SSL ports. TOE connections which can be configured to use SSL include

a) Web browser to P6 Web Access application server, and to Timesheets (GroupServer)

b) P6 Web Access application server to LDAP directory server and to PMDB database

c) Primavera GroupServer to LDAP directory server and to PMDB database

d) Integration API server to LDAP directory server (Remote mode installation) and to PMDB database

e) Project Management module to LDAP directory server and to PMDB database

f) Methodology Management module to LDAP directory server and to MMDB database

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1a: The ability to manage project access is limited to users possessing either the Admin Superuser (project) or Project Superuser role, or authorized user by restricting access to interfaces. An authorized user possesses the “Edit EPS Except Financials” and “Edit Project WBS Except Financials” privileges.
- FMT_MSA.1b: The ability to manage methodology access is limited to users possessing either the Admin Superuser (methodology) role, or authorized user by restricting access to interfaces. An authorized user possesses the “Edit Users” global (Methodology) privilege.
- FMT_MSA.1c: The ability to manage resource ownership is limited to users possessing the Admin Superuser (project) role or an authorized user by managing user accounts. An authorized user possesses the Edit Users global privilege, and the Edit Resources global (Project) privilege. Additionally, the authorized user has access to resources.
- FMT_MSA.1d: The ability to manage project users is limited to users possessing the Admin Superuser (project) role and authorized users by restricting access to interfaces. An authorized user possesses the Edit Users global privilege.
- FMT_MSA.1e: The ability to manage methodology users is limited to users possessing the Admin Superuser (methodology) role or authorized users by restricting access to interfaces. An authorized user (Methodology) possesses the Edit Users global privilege.
- FMT_MSA.3a: By default, access to projects must be explicitly granted by users possessing Admin Superuser (project) or by an authorized user. An authorized user granting users access to projects (assigning OBS nodes to users) possesses the Edit Users global privilege. An authorized user assigning OBS nodes to EPS nodes possesses the Edit EPS Except Financials project privilege and the Edit Project WBS Except Financials project privilege.
- FMT_MSA.3b: By default, access to methodologies must be explicitly granted by users possessing Admin Superuser (methodology) or authorized user using restricted interfaces. In this case, an authorized user possesses the “Edit Users” global (Methodology) privilege.

  A user with the “Create New/Copy Methodology” global (Methodology) privilege is authorized to create a new methodology. A user that creates a methodology can specify the name of the methodology and is granted Methodology Superuser for that methodology, but no other users are granted access by default.
- FMT_MSA.3c: By default, access to resources is restricted to the Admin Superuser (project).

  The Admin Superuser (project) and an authorized user (one that has “Add Resources” global (Project) privilege and some level of resource access) can add resources to the resource hierarchy and can specify the resource identity and resource parent when the resource is created.

- FMT_SMF.1: The TOE provides administrator console interfaces to manage projects, methodologies, and users.
- FMT_SMR.1: Roles are implemented by assigned users pre-defined profiles that each correspond to a separate role as follows:
  - Users that have been assigned the Admin Superuser (project) profile allow complete access to projects, resources and project application global data.
  - Users that have been assigned the Admin Superuser (methodology) profile allow complete access to methodologies and methodology application global data.
  - Users that have been assigned the Project Superuser profile allows complete access to projects.
  - Users that have been assigned the Methodology Superuser profile grant read-write privileges to methodologies.
  - Users that have not been assigned any one of the above-listed profiles are simply considered “users”.

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

Table 4 - Environment to Objective Correspondence

	O.ACCESS	O.USER_IDENTIFICATION	O.MANAGE	O.ADMIN_ROLE	OE.TOE_PROTECTION	OE.USER_AUTHENTICATION	OE.CONFIG	OE.PHYCAL
T.MASQERADE		x	x		x	x		
T.TSF_COMPROMISE	x		x		x			
T.UNAUTH_ACCESS	x		x	x				
A.LOCATE					x			x
A.ADMIN							x	

8.1.1.1 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized user to gain access to the TOE.

This Threat is countered by ensuring that:

- O.USER_IDENTIFICATION: The TOE will uniquely identify users and will identify them reliably.
- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
- OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from tampering or interference by external entities.
- OE.USER_AUTHENTICATION: The IT environment will verify the claimed identity of users.

8.1.1.2 T.TSF_COMPROMISE

A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

This Threat is countered by ensuring that:

- O.ACCESS: The TOE ensures that users gain only authorized access to the TOE and the resources protected by the TOE.
- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
- OE.TOE_PROTECTION: The IT Environment will protect the TOE and its assets from external interference or tampering.

8.1.1.3 T.UNAUTH_ACCESS

An authorized user may gain unauthorized access (view, modify, delete) to user data through the TOE.

This Threat is countered by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to it and to the resources that it controls.
- O.ADMIN_ROLE: The TOE will provide authorized administrator roles to isolate administrative actions.
- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

8.1.1.4 A. LOCATE

The TOE will be located within controlled access facilities and connected to networks that are protected from external tampering by a network firewall, which will prevent unauthorized physical access and mitigate unauthorized network access.

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from external interference or tampering.

8.1.1.5 A. ADMIN

The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that table 4 indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Table 5 - Objective to Requirement Correspondence

	O.ACCESS	O.USER_IDENTIFICATION	O.MANAGE	O.ADMIN_ROLE
FDP_ACC.2a	x			
FDP_ACC.2b	x			
FDP_ACC.2c	x			
FDP_ACF.1a	x			
FDP_ACF.1b	x			
FDP_ACF.1c	x			
FIA_ATD.1		x		
FIA_UID.2	x	x		
FMT_MSA.1a			x	
FMT_MSA.1b			x	
FMT_MSA.1c			x	
FMT_MSA.1d			x	
FMT_MSA.1e			x	
FMT_MSA.3a			x	
FMT_MSA.3b			x	
FMT_MSA.3c			x	
FMT_SMF.1			x	
FMT_SMR.1				x

8.2.1.1 O.ACCESS

The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2a, FDP_ACF.1a: All subjects are subject to the Project Access Control Policy for all available operations on projects.

- FDP_ACC.2b, FDP_ACF.1b: All subjects are subject to the Methodology Access Control Policy for all available operations on methodologies.
- FDP_ACC.2c, FDP_ACF.1c: All subjects are subject to the Resource Access Control Policy for all available operations on resources.
- FIA_UID.2: All users must successfully identify themselves before being provided access to the TOE.

8.2.1.2 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE defines users in terms of user identities and authorizations that correspond to functions a user may perform. Users are associated with security attributes after a connection has been made using either the web or heavy clients.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

8.2.1.3 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1a: The ability to manage project access is limited to users possessing either the Admin Superuser (project) or Project Superuser role by restricting access to interfaces.
- FMT_MSA.1b: The ability to manage methodology access is limited to users possessing either the Admin Superuser (methodology) or Methodology Superuser role by restricting access to interfaces.
- FMT_MSA.1c: The ability to manage resource ownership is limited to users possessing the Admin Superuser (project) role by managing user accounts.
- FMT_MSA.1d: The ability to manage project users is limited to users possessing the Admin Superuser (project) role by restricting access to interfaces.
- FMT_MSA.1e: The ability to manage methodology users is limited to users possessing the Admin Superuser (methodology) role by restricting access to interfaces.
- FMT_MSA.3a: By default, access to projects must be explicitly granted by users possessing Admin Superuser (project) or Project Superuser role using restricted interfaces.
- FMT_MSA.3b: By default, access to methodologies must be explicitly granted by users possessing Admin Superuser (methodology) or Methodology Superuser role using restricted interfaces.
- FMT_MSA.3c: By default, access to resources is restricted to the Admin Superuser (project).
- FMT_SMF.1: The TOE provides administrator console interfaces to manage projects, methodologies, resources, and users.

8.2.1.4 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: Roles are implemented by assigned users pre-defined profiles that each correspond to a separate role as follows:
  - Users that have been assigned the Admin Superuser (project) profile allows complete access to

projects, resources and project application global data..

- Users that have been assigned the Admin Superuser (methodology) profile allows complete access to methodologies and methodology application global data.
- Users that have been assigned the Project Superuser profile allows complete access to projects.
- Users that have been assigned the Methodology Superuser profile grants read-write privileges to methodologies.
- Users that have not been assigned any one of the above-listed profiles are simply considered "users".

8.3 Security Assurance Requirements Rationale

EAL4 was selected as the assurance level because the TOE is a commercial product whose users require a moderate to high level of independently assured security. Primavera Version 6.2.1 is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have an attack potential that can be characterized as enhanced basic. As such, EAL4 is appropriate to provide the assurance necessary to counter the perceived potential for attack.

8.4 Attack Potential Rationale

In accordance with the assurance requirements for a claim of EAL4, under CC version 3.1, this security target includes the security assurance requirement AVA_VAN.3. This requirement stipulates that the TOE is resistant to attacks performed by an attacker with an enhanced-basic attack potential. The TOE does not provide any permutational or probabilistic mechanisms that are subject to direct attack. The authentication mechanism utilized is implemented by the LDAP server in the IT environment. The vulnerability analysis, performed by the evaluation team, will substantiate that the attack potential is sufficiently mitigated.

8.5 Requirement Dependency Rationale

Table 6 identifies dependencies among the claimed security requirements that are working together to accomplish the overall objectives defined for the TOE.

Table 6 - Requirement Dependencies

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.2a	FDP_ACF.1	FDP_ACF.1a
FDP_ACC.2b	FDP_ACF.1	FDP_ACF.1b
FDP_ACC.2c	FDP_ACF.1	FDP_ACF.1c
FDP_ACF.1a	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2a and FMT_MSA.3a
FDP_ACF.1b	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2b and FMT_MSA.3b
FDP_ACF.1c	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2c and FMT_MSA.3c
FIA_ATD.1	none	none
FIA_UID.2	none	none
FMT_MSA.1a	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2a
FMT_MSA.1b	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2b
FMT_MSA.1c	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2c
FMT_MSA.1d	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2a
FMT_MSA.1e	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2b
FMT_MSA.3a	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1a and FMT_SMR.1

ST Requirement	CC Dependencies	ST Dependencies
FMT_MSA.3b	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1b and FMT_SMR.1
FMT_MSA.3c	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1c and FMT_SMR.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.4 and ADV_TDS.3
ADV_FSP.4	ADV_TDS.1	ADV_TDS.3
ADV_IMP.1	ADV_TDS.3 and ALC_TAT.1	ADV_TDS.3 and ALC_TAT.1
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4
AGD_OPE.1	ADV_FSP.1	ADV_FSP.4
AGD_PRE.1	none	none
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, and ALC_LCD.1	ALC_CMS.4, ALC_DVS1, and ALC_LCD.1
ALC_CMS.4	none	none
ALC_DEL.1	none	none
ALC_DVS.1	none	none
ALC_LCD.1	none	none
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.4 and ATE_FUN.1
ATE_DPT.2	ADV_ARC.1, ADV_TDS.3, and ATE_FUN.1	ADV_ARC.1, ADV_TDS.3, and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, and ATE_FUN.1	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, and ATE_FUN.1
AVA_VAN.3	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1

8.6 Extended Requirements Rationale

There are no extended requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 6 demonstrates the relationship between security requirements and security functions.

Table 7 - Security Functions vs. Requirements Mapping

	User data protection	I&A	Security management
FDP_ACC.2a	x		
FDP_ACC.2b	x		
FDP_ACC.2c	x		
FDP_ACF.1a	x		
FDP_ACF.1b	x		
FDP_ACF.1c	x		
FIA_ATD.1		x	
FIA_UID.2		x	
FMT_MSA.1a			x
FMT_MSA.1b			x
FMT_MSA.1c			x
FMT_MSA.1d			x
FMT_MSA.1e			x
FMT_MSA.3a			x
FMT_MSA.3b			x
FMT_MSA.3c			x
FMT_SMF.1			x
FMT_SMR.1			x

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.