NWAS Java 7.02
Security Target

Version 1.16

2010-12-20

Table of Content:

1 ST Introduction

This chapter presents Security Target (ST) and TOE identification information as well as a general overview of the ST.

An ST contains the security requirements of the Target of Evaluation (TOE) and specifies the functional security measures offered by that TOE to meet stated requirements.

The ST defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment and a set of Organizational Security Requirements with which the TOE must comply (chapter 3, Security Problem Definition).
- A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6, Security Objectives and IT Security Requirements, respectively).
- The IT security functionality provided by the TOE to meet the set of requirements (chapter7, TOE Summary Specification).

1.1 ST and TOE Identification

ST Title:	Security Target NWAS Java
ST Version:	1.16
Date:	2010-12-20
Author:	SAP AG
Certification-ID:	BSI-DSZ-CC-0659
TOE Identification	SAP NetWeaver Application Server Java[1] and its related guidance documentation ([SAP_Library] and [AGD_ADD])
TOE short name:	NWAS Java
TOE Release:	7.02 SP3 with Common Criteria Addendum (material no. 51039496)
TOE Operating System:	Microsoft Windows Server 2008, Enterprise Edition
TOE CPU architecture	x64
CC version:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3 as of July 2009 ([CC])
PP conformance	none
Evaluation Assurance Level:	EAL4 augmented by ALC_FLR.1

[1] Aka NWAS Java

1.2 TOE Overview

The TOE described in this Security Target is the NetWeaver Application Server Java. This server provides a framework for the development and execution of applications based on the J2EE software architecture.

As such the NetWeaver Application Server provides a complex set of services and infrastructure to be used by applications.

The descriptions in this Security Target form the basis for the evaluation of the core Security Features of the NetWeaver Application Server according to Common Criteria. The evaluation focuses on the core security services, namely:

- Audit,
- Users and authorization,
- Identification and Authentication,
- Security Management.

1.3 TOE Description

1.3.1 Product Type

To support the understanding of the role of the TOE in a SAP installation this chapter introduces necessary details about the product „NetWeaver Application Server Java“. The NWAS Java is an application server. Its role in an SAP system is depicted in Figure 1.

The role of an application server for enterprise applications is similar to that of an operating system in relation to office applications (word processors etc.): Applications are started on top of it and it mediates between user input and applications, and supplies applications with data objects, watching all the time that users have appropriate authorization for the execution of the actions they require, and so on.

The Application Server provides a layer of abstraction over the used hardware, the Operating System and additional infrastructure (e.g. databases) and provides a harmonized infrastructure and interface for the execution of services and applications. In case of the NetWeaver Application Server this includes applications of SAP as well as customer designed and driven applications.

While SAP has the full control over the design of the applications they develop they can only provide a framework for the use by customer driven applications. As such it is hardly possible to limit the use of the NetWeaver Application Server to customers in a way that Security Policies are consistently applied all thru their applications. This evaluation therefore focuses on the core of the system providing fundamental security policies and some security services to be used by applications.

1.3.2 TOE details

NWAS Java is a software product that is a fundamental component of modern SAP systems. It provides fundamental security features like identification and authentication, audit, users and authorization and security management. The functional applications (enterprise applications) of the SAP system are executed in the work processes respectively server processes of the NWAS Java

Applications use the access control functions of the TOE by either requesting authorization checks from it and enforcing an according access control policy (programmatic access control) or by describing the access control constraints and relying on the TOE for their enforcement (declarative access control). In case of programmatic access control it is, of course, intended that the applications process the results of the authorization checks correctly (performing requested operations or not, according to the meaning of the result in the given context), but this is outside of the scope of this evaluation. Instead, it is assumed that development conforms to the guidelines and restrictions specified in the SAP programmer's guidance.

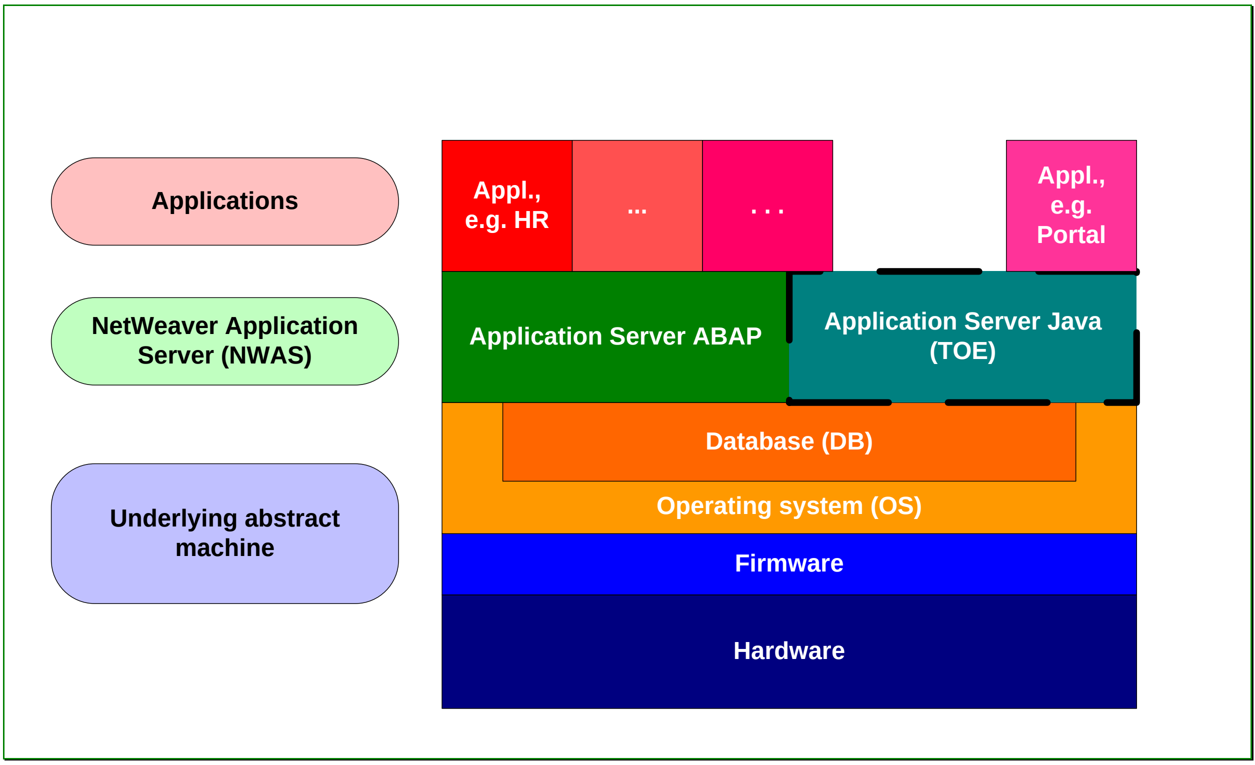

Figure 1: The role of the TOE in a SAP installation

Note: Figure 1 shows a logical layering of the TOE (depicted by the dashed line) in operation. It disregards that much of the executables of the applications and the NWAS are stored in the database. Further it disregards details of interfaces. An application may interface to the NWAS Java or the NWAS ABAP (the Portal e.g. is an application on top of the NWAS Java).

The Net Weaver Application Server exists in two different personalities: a NWAS ABAP (Application Server ABAP, also known as ABAP engine) and a NWAS Java (Application Server Java, also known as J2EE Engine).

The Application Server can be set up in a so called Single Stack configuration of either NWAS ABAP or NWAS Java as well as in a so called Dual Stack configuration in which both parts are existing.

The TOE described in this Security Target is the NWAS Java. The evaluation focuses to verify that the Security Functionality as defined in this Security Target is provided by the NWAS Java and is working correctly. As such the evaluation described in this Security Target focuses on the evaluation of a single stack installation of NWAS Java

1.3.3 Physical Scope and Boundary of the TOE

The TOE is a software package that can be installed in an appropriate IT environment. As such the physical scope of the TOE is given by the identification of the software that needs to be installed according to the corresponding guidance documentation.

The following figure shows an overview of the TOE in a single stack configuration from a component based point of view.

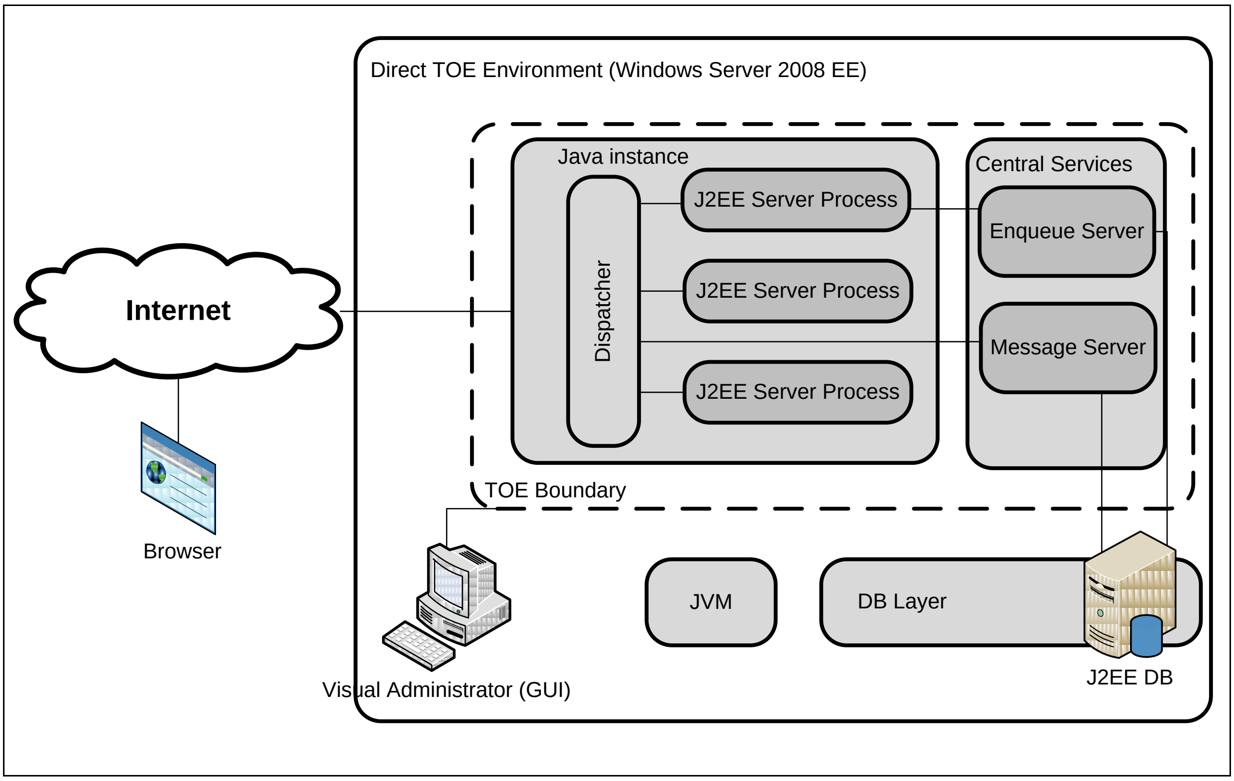

Figure 2: System Architecture of a minimal installation

Note: Applications are not displayed in this figure. Moreover, the figure provides only an architecture overview and may thus not be technically complete.

The complete details about the setup and configuration of NWAS Java in its evaluated version can be found in the guidance addendum ([AGD_ADD]) and its referenced documents.

Figure 2 shows the important components of the TOE from an architectural perspective:

The Central Services provide a Message Server that provides the infrastructure for the exchange of information between the processes of the TOE and an Enqueue Server that is responsible to maintain lock information on objects.

The Dispatcher is responsible to accept incoming connections for the TOE and forwards the requests to the responsible J2EE process.

The J2EE server processes build the core of the NWAS Java. They operate incoming requests and contain the actual application logic.

As indicated in the figure, the NWAS Java can be reached via web based protocols (i.e. using a web browser) or via the Visual Administrator (a Java application providing access to a subset of the management features of the TOE).

As indicated in the figure the TOE relies on its direct environment for its operation. Beside the Operating System (Windows Server 2008 Enterprise Edition) this environment also includes the Java Virtual Machine (JVM) and the database (layer) in which the relevant data for all applications are stored.

The TOE as described in this Security Target is set up as a single system, i.e. its environment does not connect to other SAP systems or application servers. The TOE's usage is limited to an environment presenting with cooperative and well-behaved users and administrators in which the attack potential of potential attackers is limited.

The following table lists the minimum hardware and software requirements for the operation of the TOE. Please note that those requirements define the absolute minimum for the operation of the TOE. A concrete recommendation for hardware characteristics has to be seen in the context of the concrete installation. Please refer to [AGD_ADD] for more information.

Aspect	Requirement
CPU	1.4 GHz (x64 processor)
RAM	5 GB RAM
Hard Disk	64 GB or greater
Other	Super VGA (800 × 600) or higher resolution monitor, DVD Drive, Keyboard and Microsoft Mouse (or compatible pointing device), Internet access
Software	Microsoft Windows Server 2008, Enterprise Edition

Table 1: Minimum hardware and software requirements for the TOE

A purchaser of the TOE receives the TOE in form of its media in electronic form, typically as a collection of DVDs and a set of additional downloads. The scope of the product delivery for the TOE includes:

- The installation media for the SAP NetWeaver Application Server Java,
- the Common Criteria Addendum DVD containing additional installation data,
- the installation media for the required Java Development Kit (JDK) (as a download),
- the installation data for the documentation of the product [SAP_Library],
- accompanying documents for the understanding and secure use of the TOE, in particular: this Security Target and the Guidance Addendum [AGD_ADD].

The website https://service.sap.com/commoncriteria contains additional information about all Common Criteria evaluations of SAP AG. This website contains extended information about the TOE and its certified configuration. Further, the guidance addendum ([AGD_ADD]) describing specific aspects of the certified version can be obtained via this site. The guidance addendum extends the general guidance of the product that ships along with the product.

This website shall be visited before using the TOE.

1.3.4 Logical Scope and Boundary of the TOE

The logical boundary of the TOE is the interfaces that can be seen in Figure 2 via which the TOE provides its security functionality.

For clarity it should be mentioned that the following components are not part of the TOE:

- Client-side software for user interfaces – e.g. a Web browser
- Java stand-alone applications on the operating system console – are not part of the TOE in the current evaluation,
- the underlying Operating System,
- the Java Virtual Machine
- used Database systems, and
- applications that can be installed and run on top of the TOE. Examples for applications are business-oriented applications like HR, and CRM or technically-oriented ones like the SAP Portal.

The TOE provides a set of security functionality via its external interfaces as follows:

- Security Audit: The TOE maintains a security log to keep track of security relevant events. It further provides functionality for review of the audit to authorized administrators.
- Users and authorizations: The TOE provides an access control functionality in order to ensure that only authorized administrators can use the management functionality of the TOE. It further provides functionality for authorization checks to applications that are hosted by the TOE.
- Identification and Authentication: In order to allow access control the TOE has to be aware of the identity of the connection user. Therefore the TOE provides an identification and authentication function based on usernames and passwords.
- Security Management: The TOE provides the management functionality necessary for the administration of the security functionality.

The TOE provides its security functionality via two major interfaces:

- Web-based (i.e. via http and https): The web based services are provided via the Internet Communication Manager (ICM). The ICM ensures that communication between the SAP System and the outside world via HTTP(S) protocols works properly. In its role as a server, the ICM can process requests from the Internet that arrive as URLs with the server/port combination that the ICM can listen to. The ICM then calls the relevant local handler for the URL in question.
- Via the Graphical User Interface of the Visual Administrator: The Visual Administrator is a graphical user interface (GUI) that enables administration of the NWAS Java It provides remote monitoring and management of managers, services, libraries, and interfaces working on each element in a single GUI.

With respect to access control, the TOE has a double nature. On the one hand, it provides access control for its administration interfaces; in particular its user management features and ensures that only authorized administrators have the capability to use these features.

On the other hand, the authorization checking features of the TOE serve as parts of a “toolbox” for implementing access control features in applications that can run on top of the TOE. This includes applications of SAP as well as customer designed and driven applications.

Applications use the access control functions of the TOE by either requesting authorization checks from it and enforcing an according access control policy (programmatic access control) or by describing the access control constraints and relying on the TOE for their enforcement (declarative access control).

It has to be clearly stated that the TOE has no functionality to ensure that an access control policy for applications using the programmatic access control functionality of the TOE is actually enforced. The TOE provides functionality to the applications to check for the permissions of users and guarantees for correct results. However, it falls into the responsibility of each application to enforce a comprehensive security policy based on the decisions of the TOE.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be

- CC Part 2 (Version 3.1, Revision 3) conformant as only security functional requirements as defined in part II of [CC] have been used.
- CC Part 3 (Version 3.1, Revision 3) conformant as only assurance components as defined in part III of [CC] have been used.

Further, this Security Target claims to be conformant to the Security Assurance Requirements package EAL 4 augmented by ALC_FLR.1.

2.2 PP Conformance Claim

This Security Target does not claim conformance to any Protection Profile.

3 Security Problem Definition

This chapter describes:

- The subjects that are interacting with the TOE,
- the assets that have to be protected by the TOE,
- assumptions about the environment of the TOE and
- organizational security policies that the TOE shall comply with.

3.1 Subjects and external entities

While external entities are entities interacting with the TOE from externally and generally comprise human users and other IT entities, each external entity is usually represented by a so called subject internal to the TOE.

Therewith, subjects are entities within the TOE that cause operations to be performed. Subjects are acting on behalf of external entities and usually inherit their identity when causing operations. Though external entities and subjects are not identical they are often used synonymously.

The TOE knows the following subjects:

Anonymous user — This subject belongs to an identifiable human user. Such a subject may have access to public services of the system, e.g. Web based services that are open to the general public. An example of a public service is an I&A dialog: necessarily, a user is not yet authenticated when launching I&A, only after successfully completing it.

Authenticated user — This subject belongs to a user of the operational functions (e.g. HR, FI) of an SAP system who has gone through a logon process and is thus identified and authenticated.

Administrator — This subject belongs to a person responsible for configuring, maintaining, and administering the SAP system, particularly the TOE, in a correct manner. (Administrative tasks always require certain authorizations, so an administrator must always be identified and authenticated.)

Note: The administrative tasks in an SAP system can be distributed among different persons and roles. Therefore, there may be one or several user administrators, one or several system administrators, one or several auditors, and so on and each of them will be represented by a dedicated subject when interacting with the TOE. As such a distribution is not mandated by the system, so that all administrative tasks could be performed by the same person, only one type of subject has been defined for administrators.

It should be noted that the TOE also supports an emergency user named SAP*. The subject associated with this user has literally every permission. However, as this emergency user account has to be enabled explicitly before it can be used and must not be used during operational use of the TOE it has not been listed as a subject here and will not be considered in the rest of this document. Please refer to [AGD_ADD] for more information.

3.2 Assets

The TOE knows two types of assets:

The primary assets are represented by the data that shall be protected by the access control mechanism of the TOE. They specifically comprise:

- the UME Application (the application responsible for user management),
- servlets,
- management data accessed via a web based interface or via the Visual Administrator,
- user data (for the use by applications)

The secondary assets comprise the TSF data that the TOE maintains and relies on for its own operation. They specifically comprise:

- User names,
- passwords,
- audit data.

3.3 Assumptions

The following assumptions are indispensible for the correct operation of the TOE.

A.ADMIN It is assumed that one or more competent and well trained administrators are assigned to manage the TOE and the security of the information it contains.

The administrators are neither careless, willfully negligent, nor hostile. The administrator know and follow all instructions provided in the relevant guidance documentation.

Further, it is assumed that the emergency user account SAP* is not used in the operational use of the TOE.

A.AUTHDATA Administrators and users must ensure that the authentication data for each user account for the TOE is held securely and not disclosed to persons not authorized to use that account. The administrators and users must specifically ensure that no hardware or software key loggers are installed on the machines used to enter the authentication data.

A.CONNECT The TOE is connected to the Internet (via the ICM) and/or terminals and workstations. Connections to the TOE are possible via Web protocols (e.g. http or https) and/or the Visual Administrator (that implements a RMI/P4 protocol).
It is assumed that authentication and authorization data transported between client and server data is protected e.g. by an adequate encryption method and protocol and that the TOE is appropriately protected by a firewall.

A.IT It is assumed that the necessary IT infrastructure for the TOE is available. This specifically includes the following aspects:

- An appropriate hardware architecture and a suitable operating system as set out in the TOE guidance documents will be available. This underlying hardware and software are assumed to perform according to their specifications.
- The TOE is used in conjunction with a suitable database management system (DBMS) and Java Virtual Machine (JVM) as set out in the TOE guidance documents. This underlying DBMS and JVM is assumed to perform according to its specification.
- The IT environment of the TOE contains a clock that is appropriately set and maintained by administrators and/or synchronized with a reliable external time source.

A.PROTECT The TOE and its underlying abstract machine are located within controlled access facilities that will prevent unauthorized physical access.

A.UI It is assumed that the TOE is used with suitable user interfaces as set out in the TOE guidance documents, for example Web browsers, or Visual Administrator.

A.DEVELOP It is assumed that the development of applications (for the NWAS) will comply with all the guidelines and restrictions specified in the SAP Programmer’s Guidance.

3.4 Threats

This ST derives all security objectives for the TOE (section 4.1) from the statement of Organizational Security Policies (section 3.5) and all security objectives for the environment (section 4.2) from the assumptions about the environment of the TOE (section 3.3).

Therefore, there is no statement of explicit threats countered by the TOE described in this Security Target.

3.5 Organizational Security Policies

This section identifies any organizational security policy statements or rules with which the TOE must comply.

P.ACCESS The TOE shall provide access control as follows:

1) A declarative access control policy for J2EE applications. In this policy the TOE shall ensure that a user can only access an object under its control via an application if the user has the appropriate permission.
2) A programmatic access control functionality. In this case the TOE provides functionality to applications that allow checking whether a user has a certain permission. In this scenario the application itself is responsible to enforce the overall access control policy.

P.AUDITING The TOE shall write a security audit to track a set of events that will allow an administrator to get informed about the security relevant events in the TOE.

This set of events comprises events from the following areas:

- Principal Modification
- User Mapping
- Login/Logoff
- Permission Checking

Into each security audit record entry the TOE shall at least record the following information:

- Timestamp
- Severity (if relevant)
- Actor
- Event
- ObjectType
- ObjectID

Eventually the TOE shall provide only authorized administrators with functionality to review the audit logs.

P.I&A The TOE shall identify and authenticate each user prior to allow access to any object except for public operations.

For user chosen passwords the TOE shall ensure that they have a minimum length of 5 characters.

P.MANAGE The TOE shall provide only authorized administrators with the relevant management functionality for the configuration of the security functionality.

4 Security Objectives

4.1 Security Objectives for the TOE

O.ACCESS The TOE shall provide an access control policy as follows:

1) A declarative access control policy for J2EE applications. In this policy the TOE shall ensure that a user can only access an object under its control via an application if the user has the appropriate permission.
2) A programmatic access control functionality. In this case the TOE provides functionality to applications that allow checking whether a user has a certain permission. In this case the application itself is responsible to enforce the overall access control policy.

O.AUDITING The TOE shall write a security audit to track a set of events that will allow an administrator to get informed about the security relevant events in the TOE.

This set of events comprises events from the following areas:

- Principal Modification
- User Mapping
- Login/Logoff
- Permission Checking

Into each security audit record entry the TOE shall at least record the following information:

- Timestamp
- Severity
- Actor
- Event
- ObjectType
- ObjectID

Eventually the TOE shall provide only authorized administrators with functionality to review the audit logs.

O.I&A The TOE shall identify and authenticate each user prior to allow access to any object except for public operations.

For user chosen passwords TOE shall ensure that they have a minimum length of 5 characters.

O.MANAGE The TOE shall provide only authorized administrators with the relevant management functionality for the configuration of the security functionality.

4.2 Security Objectives for the Environment

The following objectives need to be met by the environment of the TOE to ensure the correct operation of the TOE:

OE.ADMIN

It has to be ensured that one or more competent and well trained administrators are assigned to manage the TOE and the security of the information it contains.

The administrators are neither careless, willfully negligent, nor hostile. The administrators know and follow all instructions provided in the relevant guidance documentation.

Further, it has to be ensured that the emergency user account SAP* is not used in the operational use of the TOE.

OE.AUTHDATA

It has to be ensured that administrators and users keep the authentication data for each user account for the TOE securely and not disclose it to persons not authorized to use that account. The administrators and users must specifically ensure that no hardware or software key loggers are installed on the machines used to enter the authentication data.

OE.CONNECT

It has to be ensured that the TOE is connected to the Internet (via the ICM) and/or terminals and workstations. Connections to the TOE are possible via Web protocols (e.g. http or https) and/or the Visual Administrator (that implements a RMI/P4 protocol).
It has to be ensured that authentication and authorization data transported between client and server data is protected e.g. by an adequate encryption method and protocol and that the TOE is appropriately protected by a firewall.

OE.IT

It has to be ensured that the necessary IT infrastructure for the TOE is available. This specifically includes the following aspects:

- An appropriate hardware architecture and a suitable operating system as set out in the TOE guidance documents will be available. This underlying hardware and software are performing according to their specifications.
- The TOE is used in conjunction with a suitable database management system (DBMS) and Java Virtual Machine (JVM) as set out in the TOE guidance documents. This underlying DBMS and JVM are assumed to perform according to its specification.
- The IT environment of the TOE contains a clock that is appropriately set and maintained by administrators and/or synchronized with a reliable external time source.

OE.PROTECT

The TOE and its underlying abstract machine are located within controlled access facilities that will prevent unauthorized physical access.

OE.UI

It has to be ensured that the TOE is used with suitable user interfaces as set out in the TOE guidance documents, for example Web browsers, or Visual Administrator.

OE.DEVELOP

It has to be ensured that the development of applications (for the NWAS) will comply with all the guidelines and restrictions specified in the SAP Programmer’s Guidance.

4.3 Security Objectives Rationale

4.3.1 Overview

The following table maps the security objectives to assumptions and OSPs.

Assumptions, OSP / Security Objectives	O.ACCESS	O.ADUDITING	O.I&A	O.MANAGE	OE:ADMIN	OE.AUTHDATA	OE.CONNECT	OE.IT	OE.PROTECT	OE.UI	OE.DEVELOP
P.ACCESS	X										
P.AUDITING		X									
P.I&A			X								
P.MANAGE				X							
A.ADMIN					X						
A.AUTHDATA						X					
A.CONNECT							X				
A.IT								X			
A.PROTECT									X		
A.UI										X	
A.DEVELOP											X

Table 2: Mapping of security objectives to assumptions and OSPs

The following chapters provide more details about the mapping between Organizational Security Policies and Security Objectives for the TOE as well as between assumptions and Security Objectives for the environment.

4.3.2 Rationale for TOE Security Objectives

The following table and its succeeding paragraphs provide the rationale for the TOE Security Objectives and show how they can be derived from the Organizational Security Policies.

No.	Organizational Security Policy	Security Objective
1	P.ACCESS	O.ACCESS
2	P.AUDITING	O.AUDITING
3	P.I&A	O.I&A
4	P.MANAGE	O.MANAGE

Table 3: Mapping: Organizational Security Policies ⇔ Security Objectives

The Security Objective **O.ACCESS** implements the OSP **P.ACCESS** as directly follows. Both descriptions consider the fact that the TOE is providing two kinds of access control.

The Security Objective **O.AUDITING** implements the OSP **P.AUDITING** as directly follows. Both descriptions require that the TOE shall log a set of security relevant events. They further describe that access to the audit logs has to be protected.

The Security Objective **O.I&A** implements the OSP **P.I&A** as directly follows. Both descriptions refer to the fact that only a very limited set of actions is available for users before being identified and authenticated.

The Security Objective **O.MANAGE** implements the OSP **P.MANAGE** as directly follows.

4.3.3 Rationale for environmental Security Objectives

The following table and its succeeding paragraphs provide the rationale for the Environmental Security Objectives and show how they can be derived from assumptions.

No.	Assumption	Security Objective
1	A.ADMIN	OE.ADMIN
2	A.AUTHDATA	OE.AUTHDATA
3	A.CONNECT	OE.CONNECT
4	A.IT	OE.IT
5	A.PROTECT	OE.PROTECT
6	A.UI	OE.UI
7	A.DEVELOP	OE.DEVELOP

Table 4: Mapping: Assumptions ⬄ Security Objectives for the environment

The assumption **A.ADMIN** is represented by the objective **OE.ADMIN.** The assumption requires well trained administrators who are not hostile. Further it prohibits the use of the emergency user SAP* in operational mode. Those aspects are restated by **OE.ADMIN**.

The assumption **A.AUTHDATA** is represented by the objective **OE.AUTHDATA.** As for every authentication mechanism basing on passwords it is important for the TOE to base on the assumption that the authentication data (i.e. the passwords) are not disclosed by the user or the administrator.

The assumption **A.CONNECT** is represented by the objective **OE.CONNECT**. The assumption and the objective for the environment ensure that the necessary connection to the internet is available for the TOE and that the connection to the internet is appropriately secured by the use of a firewall.

The assumption **A.IT** is represented by the objective **OE.IT**. As every TOE that is software only the NWAS Java has to rely on certain services of the underlying hardware and the Operating System. The aspects that are important for the operation of the TOE are addressed in **A.IT** and **OE.IT**.

The assumption **A.PROTECT** is represented by the objective **OE.PROTECT**. As the TOE is software only it cannot protect itself against physical tampering but has to rely on its environment for this aspect as expressed in **A.PROTECT** and **OE.PROTECT**.

The assumption **A.UI** is represented by the objective **OE.UI** as directly follows.

The assumption **A.DEVELOP** is represented by the objective **OE.DEVELOP**. The TOE provides the possibility for applications to implement the access control functionality by themselves (programmatic concept) and to only use the TOE as a service provider for authentication and authorization checks. In these cases a comprehensive security policy for access control can only be implemented if the applications using these services implement the enforcing part of access control.

5 Extended Component Definition

This Security Target does not use any extended components.

6 IT Security Requirements

This part of the ST defines the IT security and assurance requirements for the TOE.

6.1 Conventions

The SFRs are organized by CC class. The CC permits four functional component operations on SFRs to make the SFR more specific to the type of product or implementation required by the consumer.

The four operations are applied and marked in the following manner:

- *Assignment***:** Allows the specification of an identified parameter. Completed assignments are indicated by italic text. Further the brackets from CC are kept.
- ***Refinement*****:** Allows the addition of details. Performed Refinements are indicated using bold, italics text.
- Selection**:** Allows the specification of one or more elements from a list. Performed selections are indicated using underlined text. Further the brackets from part II of CC are kept.
- **Iteration:** Allows a component to be used more than once with varying operations. Letters appended at the end of CC element names indicate iteration.

The ST uses instantiations of the following SFRs from [CC, Part 2].

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_STG.1	Protected Audit Trail Storage
Class FDP: User Data Protection	
FDP_ACC.2/D	Complete Access Control for declarative security
FDP_ACF.1/D	Security Attribute-based Access Control for declarative security
FDP_ACC.2/P	Complete Access Control for programmatic security
FDP_ACF.1/P	Security Attribute-based Access Control for programmatic security
Class FIA: Identification and Authentication	
FIA_AFL.1	Authentication Failure Handling
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of Authentication
FIA_UID.1	Timing of Identification
FIA_USB.1	User-Subject Binding
Class FMT: Security Management	
FMT_MOF.1	Management of Functions in TSF
FMT_MSA.1/D	Management of Security Attributes for Declarative Authorization SFP
FMT_MSA.1/P	Management of Security Attributes for Programmatic Authorization SFP
FMT_MSA.3/D	Static Attribute Initialisation for Declarative Authorization SFP
FMT_MSA.3/P	Static Attribute Initialisation for Programmatic Authorization SFP
FMT_MTD.1	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles

Table 5: List of TOE Security Functional Requirements

6.2 IT Security Requirements for the TOE

6.2.1 Class FAU: Security Audit

6.2.1.1 Security audit data generation (FAU_GEN)

6.2.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the [not specified] level of audit ***(as listed in column "event" of Table 6)***; and

c) [*No other specifically defined auditable events.*]

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 (if applicable), 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, [*details as outlined inTable 6*]

Event	Severity	Object ID	Details
Principal modification			
User creation	Medium	The new user	Company ID
	Low	The new user	All user attributes
User account creation	High	The new user account	Assigned user ID
Group creation	High	The new group	Assigned users and groups
Role creation	High	The new role	Assigned users and groups Assigned actions
User modification	Medium	The modified user	If user was assigned to a company: Company ID
	Low	The modified user	All changed user attributes
User account modification	High	The modified user account	Password was changed (Forced to change / Success / Failed: Reason) User was locked (reason). User was unlocked Certificate was modified Possible reasons for a locked

Event	**Severity**	**Object ID**	**Details**
			user are: 1) User was locked due to too many incorrect logon attempts. 2) User was locked by an administrator.
Group modification	High	The modified group	If group members were modified: Added or removed users and groups
Role modification	High	The modified role	If role members were modified: Added or removed users and groups If actions were modified: Added or removed actions
User deletion	Medium	The deleted user	(no details)
User account deletion	High	The deleted user account	Assigned user ID
Group deletion	High	The deleted group	(no details)
Role deletion	High	The deleted role	(no details)
User mapping			
User mapping creation	Medium	The mapped user	System alias Remote user ID Type of system (SAP_R3, SAP_BW, or SAP_CRM)
User mapping modification	Medium	The mapped user	System alias Remote user ID
User mapping deletion	Medium	The mapped user	System alias Remote user ID
User mapping usage	Medium	The mapped user	System alias Remote user ID
Login/Logoff			
Successful user logon	Medium	The used user account	User ID Logon method/ Authentication scheme
Failed user logon	High	The used user account	User ID Logon method/ Authentication scheme Reason why logon failed (wrong password, user locked, …)

Event	Severity	Object ID	Details
User logoff	Medium	The used user account	(no details)
Permission (checking)			
ACL creation	High	The object for which the ACL was created	Owner
ACL modification	High	The object whose ACL was modified	Added or removed owners Added or removed ACEs (access control entries): (Principle, Permission) Changed object ID
ACL deletion	High	The object to which the ACL was assigned	(no details)
Access violation or access denied	Very high	The object the user wanted to access (if available)	Permission the user would have needed to access the object
Access granted	Low	The object the user accessed (if available)	Permission that was needed to access the object

Table 6: Auditable Events for NWAS Java

6.2.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.2 Security audit review (FAU_SAR)

6.2.1.2.1 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*authorized administrators*] 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.

6.2.1.2.2 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.

6.2.1.3 Security audit event storage (FAU_STG)

6.2.1.3.1.1 FAU_STG.1 Protected Audit Trail Storage

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

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 Class FDP: User Data Protection

With respect to access control, the TOE provides two distinct sets of security features that are modelled in the following classes:

On the one hand, it provides a **declarative access control policy**. In this policy applications that are running within the TOE inform the TOE about the required permissions that users have to have in order to access a certain object. Every time an application is trying to access an object on behalf of a user the TOE will check whether the user has the appropriate permission and deny the access if this is not the case.

On the other hand, it provides a **programmatic access control policy**. In this policy applications that are running within the TOE are responsible for performing parts of the access control. The TOE serves as a kind of service provider providing functionality to those applications that allow to check whether the user has the appropriate permission.

6.2.2.1 Access control policy (FDP_ACC)

6.2.2.1.1 FDP_ACC.2/D Complete Access Control for declarative security

FDP_ACC.2.1/D The TSF shall enforce the [*NWAS Java Declarative Authorization SFP*] on

- [*The subjects*
  - *Anonymous User,*
  - *Authenticated User,*
  - *Administrator and*
- *Controlled objects*]

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

FDP_ACC.2.2/D 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.

6.2.2.1.2 FDP_ACC.2/P Complete Access Control for programmatic security

FDP_ACC.2.1/P The TSF shall enforce the [*NWAS Java Programmatic Authorization SFP*] on

- [*The subjects*
  - *Anonymous User,*
  - *Authenticated User,*
  - *Administrator and*
- *Controlled objects*]

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

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

Application Note: The Security Functional Policy as defined in FDP_ACC.2/P (and FDP_ACF.1/P) is used in the context of the programmatic access control functionality of the TOE. As outlined before in the scope of this policy the TOE offers services for applications in order to allow them to evaluate whether the current user has a certain permission. In the end the application that is using this functionality is responsible to act according to the decision of the TOE (i.e. to deny or allow access).

Application Note: The objects that are protected by the Declarative Authorization SFP are applications or parts of those applications.

6.2.2.2 Access control functions (FDP_ACF)

6.2.2.2.1 FDP_ACF.1/D Security Attribute-Based Access Control for declarative security

FDP_ACF.1.1/D The TSF shall enforce the [*NWAS Java Declarative Authorization SFP*] to objects based on the following:[

- *All subjects (and their corresponding User ID)*
- *All objects (and their corresponding Object ID)*
- *The list of permissions in form of J2EE roles*].

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

- *If the user requesting access to an object under the control of the TOE has the required J2EE role the access is granted*
- *Else the access is denied*].

FDP_ACF.1.3/D The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*No additional rules*].

FDP_ACF.1.4/D The TSF shall explicitly deny access of subjects to objects based on: [*No additional rules*].

Application Note: This SFP is not enforced on objects that are not accessed via their external interface (i.e. an EJB method calling another EJB method within the same EJB will always succeed, and a servlet only if requested by an external entity is subject to the SFP).

6.2.2.2.2 FDP_ACF.1/P Security Attribute-Based Access Control for programmatic security

FDP_ACF.1.1/P The TSF shall enforce the [*NWAS Java Programmatic Authorization SFP*] to objects based on the following:[

- *All subjects (and their corresponding User ID)*
- *All objects (and their corresponding Object ID)*
- *The list of permissions in form of UME roles*].

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

The TOE provides a functionality to check whether a user has a specific permission].

FDP_ACF.1.3/P The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*No additional rules*].

FDP_ACF.1.4/P The TSF shall explicitly deny access of subjects to objects based on: [*No additional rules*].

6.2.2.3 Class FIA: Identification and Authentication

6.2.2.4 Authentication failures (FIA_AFL)

6.2.2.4.1.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*1 through 99*]] unsuccessful authentication attempts occur related to [*authentication attempts under the same user identity*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*Block password logon attempts under the affected user identity until either (a) an authorized administrator removes the password lock or (b) if a parameter for automatic removal is set and no administrator intervenes before: a correct combination of user id and password is entered on a day after the day on which the password lock was set; when (a) or (b) occurs, the number of unsuccessful authentication attempts shall be reset to its minimum].*

6.2.2.5 User attribute definition (FIA_ATD)

6.2.2.5.1.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*User ID, J2EE roles, UME roles, groups*].

Note: The attributes as defined in FIA_ATD.1 are used by different policies of the TOE as follows.

User ID: The user id is used by all policies and unambiguously identifies the user.

J2EE roles: A J2EE role is used by the declarative access control policy of the TOE. Developers of applications define the required permission for access to objects in form of J2EE roles

UME roles: UME roles are used by the programmatic access control policy of the TOE. The definition of a UME role includes a set of actions and each action has a set of associated permissions. The programmatic access control functionality is able to provide applications with information on whether a user is a member of a UME role and therewith has the appropriate permission.

Groups: Groups are simply defined as a group of users.

6.2.2.6 Specification of Secrets (FIA_SOS)

6.2.2.6.1.1 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*user defined passwords shall have a minimum length of 5 characters, shall contain at least 1 alphanumeric character, and shall not contain the logon id*].

6.2.2.7 User authentication (FIA_UAU)

6.2.2.7.1.1 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [*user identification and those actions that are acceptable before user identification according to FIA_UID.1*] on behalf of the user to be performed before the user is authenticated.

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

6.2.2.7.2 User identification (FIA_UID)

FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [*actions that are admissible for anonymous users*] on behalf of the user to be performed before the user is identified.

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

6.2.2.8 User-subject binding (FIA_USB)

6.2.2.8.1 FIA_USB.1 User-Subject Binding

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

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

When a subject is acting on behalf of a certain user, it "inherits" the associated user security attributes]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*None.*[2]]

6.2.3 Class FMT: Security Management

6.2.3.1.1 Management of functions in TSF (FMT_MOF)

6.2.3.1.1.1 FMT_MOF.1 Management of Security Functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [*as defined by FAU_GEN.1, FAU_SAR.1, FDP_ACC.2. FIA_AFL.1, FIA_SOS.1, FIA_UAU.1 and FIA_UID.1*] to [*authorized administrators*].

Application Note: While the management of the rest of the security attributes is protected by the use of the SFRs FMT_MSA.1/D, FMT_MSA.3/P, FMT_MSA.1/D, FMT_MSA.3/P and FMT_MTD.1 this SFR shall ensure that all the other management functions as defined in FMT_SMF.1 can only be used by authorized administrators.

[2] When security attributes of a user are changed during the "lifetime" of a subject, the subject attributes remain unchanged. As no changes happen in this case, there is no "rule governing changes". On the other hand, when subjects are newly created after a change in user attributes, they receive the now changed attributes, but through FIA_USB.1.2. Altogether, there is no FIA_USB.1.3 rule, and no need for it.

6.2.3.2 Specification of management functions (FMT_SMF)

6.2.3.2.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [*List of security management functions as listed in Table 7*].

SFR	Related Management Activity
FAU_GEN.1	Configuration of the audit capabilities
FAU_GEN.2	See FAU_GEN.1
FAU_SAR.1	Maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_SAR.2	See FAU_SAR.1
FDP_ACC.2	Managing access control: • Management of user roles • Creating and deleting roles • Modifying (assigning, removing) and querying the set of roles Note: Access to these management activities is restricted to administrators
FDP_ACF.1	See FDP_ACC.2
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts.
FIA_SOS.1	Management of the password quality policy
FIA_UAU.1	Managing the list of actions that can be taken before the user is authenticated.
FIA_UID.1	Managing the list of actions that can be taken before the user is identified:
FIA_USB.1	None
FMT_MSA.1	• Management of Users accounts ○ Delete, ○ Create, ○ Lock, ○ Unlock • Management of J2EE Roles ○ Create ○ Modify ○ Delete • Management of UME Roles ○ Create ○ Modify ○ Delete

	- Manage the UME Roles of Users o Query o Modify - Manage the J2EE Roles of Users o Query o Modify - Authentication functionality o Managing the list of actions that can be taken before the user is authenticated. o Management of the threshold for unsuccessful authentication attempts.
FMT_MTD.1	- Modify the password of a user - Modify the password status of a user - Modify the account status of a user
FMT_SMR.1	Managing the group of users

Table 7: Management Activities

6.2.3.3 Management of security attributes (FMT_MSA)

6.2.3.3.1.1 FMT_MSA.1/D Management of Security Attributes for Declarative Authorization SFP

FMT_MSA.1.1/D The TSF shall enforce the [*NWAS Java Declarative Authorization SFP*] to restrict the ability to [*modify*] the security attribute [*as listed in* Table 8] to [*roles as listed in* Table 8].

Attribute/Subject	**Anonymous User**	**Authenticated User**	**Administrator**
User Identity	-	-	Delete Create Lock

			Unlock
J2EE Role	-	-	, Modify, Delete, Create
J2EE roles of other users	-	-	Modify
J2EE role for an administrator	-	-	Modify (only their own role)

Table 8: Management of Security Attributes for NWAS Java Declarative Authorization SFP

6.2.3.3.1.2 FMT_MSA.1/P Management of Security Attributes for Programmatic Authorization SFP

FMT_MSA.1.1/P The TSF shall enforce the [*NWAS Java Declarative Authorization SFP*] to restrict the ability to [*modify*] the security attribute [*as listed in* Table 11] to [*roles as listed in* Table 11].

Attribute/Subject	**Anonymous User**	**Authenticated User**	**Administrator**
UME Role	-	-	Query, Modify, Delete, Create
UME Role of other users	-	-	Query Modify
UME role for an administrator	-	-	Query Modify (only for their own role)
UME roles of authenticate users	-	Query (only for their own role)	-
I&A threshold	-	-	Modify
List of actions that can be taken before a user is identified	-	-	Modify

Table 9: Management of Security Attributes for NWAS Java Programmatic Authorization SFP

6.2.3.3.2 FMT_MSA.3/D Static attribute initialization for Declarative Authorization SFP

FMT_MSA.3.1/D The TSF shall enforce the [*NWAS Java Declarative Authorization SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/D The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.3.3.3 FMT_MSA.3/P Static attribute initialization for Programmatic Authorization SFP

FMT_MSA.3.1/P The TSF shall enforce the [*NWAS Java Programmatic Authorization SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/P The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.3.4 Management of TSF data (FMT_MTD)

6.2.3.4.1.1 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[*manage*]] the [*TSF data as listed in* Table 10] to [*the subjects as in Table 10*]].

Attribute/Subject	Anonymous User	Authenticated User	Administrator
own password and its password status	-	Modify [3] query (only for their own password)	**-**
Password of other users	-	-	Modify[4]
Account status	-	-	Modify Query[5]

[3] Note: Modifying password implies modifying password status as a side effect.

[4] Note: Here, modifying password means setting the password for the first time or resetting it. Modifying password implies modifying password status as a side effect.

Table 10: Management of TSF Data

6.2.3.4.2 Security management roles (FMT_SMR)

6.2.3.4.2.1 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles[

- o *anonymous users;*
- o *authorized user;*
- o *authorized administrator];*

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

6.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 (EAL4) components as specified in [CC, Part 3] augmented by ALC_FLR.1. No operations are applied to the assurance components.

6.4 Security Requirements rationale

6.4.1 Security Functional Requirements rationale

The following table summarizes how the Security Functional Requirements serve to implement the Security Objectives of the TOE

Assumptions, OSP / Security Objectives	**O.ACCESS**	**O.ADUDITING**	**O.I&A**	**O.MANAGE**
FAU_GEN.1		X		
FAU_GEN.2		X		
FAU_SAR.1		X		
FAU_SAR.2		X		
FAU_STG.1		X		
FDP_ACC.2/D	X			
FDP_ACC.2/P	X			
FDP_ACF.1/D	X			
FDP_ACF.1/P	X			
FIA_AFL.1			X	

[5] Note: A user identity can be seen as “locked” if the account status is set to “account lock” or the password status is set to “password locked”. “Account lock” needs an administrator action whereas “password lock” happens due to user interaction if the threshold for unsuccessful authentication attempts is reached.

Assumptions, OSP / Security Objectives	**O.ACCESS**	**O.ADUDITING**	**O.I&A**	**O.MANAGE**
FIA_ATD.1			X	
FIA_SOS.1			X	
FIA_UAU.1			X	
FIA_UID.1			X	
FIA_USB.1			X	
FMT_MOF.1				X
FMT_MSA.1/D				X
FMT_MSA.1/P				X
FMT_MSA.3/D				X
FMT_MSA.3/P				X
FMT_MTD.1				X
FMT_SMF.1				X
FMT_SMR.1				X

Table 11: Mapping: Security Objectives ⇔ Security Functional Requirements

The Security Objective **O.ACCESS** is described by a combination of FDP_ACC.2/D, FDP_ACF.1/D, FDP_ACC.2/P and FDP_ACF.1/P. FDP_ACC.2/D and FDP_ACF.1/D build the declarative access control policy as described by O.ACCESS. FDP_ACC.2/P and FDP_ACF.1/P describe the programmatic access control policy that basically comprises the decision service that can be used by applications to check whether a user has a certain permission.

The Security Objective **O.AUDITING** is described by a combination of FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2 and FAU_STG.1. The objective requires the definition of requirements for two major areas:

1) Audit generation: The aspect that an audit has to be written by the TOE and that certain events and information on events are written. This has been defined by the use of FAU_GEN.1 and FAU_GEN.2.

2) Audit review for administrators only: The objective O.AUDITING eventually requires that the TOE has to provide functionality for audit review and that this functionality is provided to authorized administrators only. This has been modeled by the use of FAU_SAR.1, FAU_SAR.2 and FAU_STG.1.

The Security Objective **O.I&A** is described by a combination of FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1 and FIA_USB.1. The core functionality required by O.I&A is the enforcement of a policy for the identification and authentication of users. This has been modeled in form of FAI_UAU.1 and FIA_UID.1. Further FIA_AFL.1 has been used to ensure that the use of the authentication mechanism is blocked after a certain amount of unsuccessful authentication attempts occurred. FIA_SOS.1 has been used to model that functionality that the TOE ensures a minimum password quality for user passwords. Finally FIA_ATD.1 and FIA_USB.1

have been used to define the required security attributes for users and to describe the behaviour of the TOE for binding user attributes to subjects.

The Security Objective **O.MANAGE** is described by a combination of FMT_MSA.1/D, FMT_MSA.1/P, FMT_MSA.3/D, FMT_MSA.3/P, FMT_MTD.1, FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1. The core objective described in **O.MANAGE** is that the TOE shall provide the relevant management functionalities for the administration of its security functionality. This has been modeled by the use of FMT_SMF.1. FMT_SMR.1 further models the required role model. FTM_MSA.1/D, FMT_MSA.1/P, FMT_MSA.3/D and FMT_MSA.3/P define requirements on the initialization of security attributes used for other security policies. Eventually FMT_MTD.1, FMT_MOF.1 and FMT_MSA.3 ensure another important aspect of **O.MANAGE**: The relevant management functionality must only be available for authorized administrators.

6.4.2 Rationale for satisfying all Dependencies

The following -provides information on how the dependencies of the used Security Functional Requirements for the TOE are met.

SFR	Dependency	Satisfied by
FAU_GEN.1	FPT_STM.1	Not satisfied by the TOE; see justification below table
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FDP_ACC.2/D	FDP_ACF.1	FDP_ACF.1/D
FDP_ACC.2/P	FDP_ACF.1	FDP_ACF.1/P
FDP_ACF.1/D	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/D, FMT_MSA.3/D
FDP_ACF.1/P	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/P, FMT_MSA.3/P
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	-
FIA_SOS.1	None	-
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	None	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/D	(FDP_ACC.1 or FDP_IFC.1), FMT_SMF.1, FMT_SMR.1	FDP_ACC.2/D, FMT_SMF.1, FMT_SMR.1

SFR	Dependency	Satisfied by
FMT_MSA.1/P	(FDP_ACC.1 or FDP_IFC.1), FMT_SMF.1, FMT_SMR.1	FDP_ACC.2/P, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3/D	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/D, FMT_SMR.1
FMT_MSA.3/P	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/P, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1

Table 12: Dependencies of the TOE Security Functional Requirements

The dependency of FAU_GEN.1 (Audit Data Generation) that requires the availability of reliable time stamps cannot be fulfilled by the TOE itself as the TOE is a pure software TOE. This dependency however, is met by the assumption A.IT and the corresponding Security Objective for the environment OE.IT that ensure that the environment will provide the TOE with reliable time stamps.

All other dependencies of SFRs are satisfied as specified in [CC, Part 2].

6.4.3 Rationale for Assurance Requirements

The TOE shall meet the security assurance requirements as defined in EAL4 augmented by ALC_FLR.1 [CC, Part 3].

As the TOE is an Application Server that can be used for multiple purposes the value of the assets that will be protected by the security functionality of the TOE cannot be predicted.

In this situation the developer of the TOE decided that the TOE shall provide a level of assurance that is adequate for the possible value of the many assets.

The evaluation assurance level EAL4 (methodically designed, tested, and reviewed) provides exactly this:

EAL4 permits a developer to gain assurance from positive security engineering based on good commercial development practices that, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

The augmentation by ALC_FLR.1 has been chosen to warrant basic flaw remediation procedures to ensure the security of the TOE after the evaluation/certification is finished.

7 TOE Summary Specification

This chapter presents an overview of the security functionality implemented by the TOE. This includes functionality from the following areas:

- Audit,
- Authentication on NWAS Java,
- Users and Authorizations,
- Security Management.

7.1 Audit

The J2EE Logging is a tool designed for administrators who need to take a detailed look at what occurs in the SAP System concerning security relevant events. By activating the J2EE Logging, you keep a record of those activities you consider relevant for auditing. Administrators can access the information for review by using the Log Viewer which is part of the TOE.

The security log contains the information on all events as outlined in Table 6.

Into each security audit record entry the TOE records the following information:

- Timestamp,
- Severity (if relevant),
- Actor,
- Event,
- ObjectType,
- ObjectID.

The TOE maintains a default directory for the security logs; the Visual Administrator can be used to change the location of this file.

This security functionality implements the Security Functional Requirements: FAU_GEN.1, FAU_GEN.2

7.2 Identification and Authentication (I&A)

The I&A functionality of the TOE bases on usernames and passwords. The identification of subjects can be used for attaching authorizations to these subjects and allows access control decisions based on a subject’s identity and authorizations.

The TOE ensures that for all user chosen passwords a minimum quality metric is maintained. Each password has to be at least of 5 characters length.

Requesting a service of the TOE is basically equivalent to entering a URL. With a browser, a user can request practically every Web-based service on the NWAS Java If the service does require an authenticated user (i.e. is not available for anonymous use) the TOE will ensure that the user is authenticated before getting access to the service.

Note: Although individual identification and authentication is not mandatory by the time a user requests a service, it is quite possible that the requesting user has gone through I&A before, e.g. in connection with an earlier request for a service that requires authentication.

Note: Although a service runs without authentication, i.e. anonymously, it still needs an identification under which it is known to the system. In the TOE, this is either (a) a purely technical name (e.g. SAPSYS), or (b) a non-personal identification that can be used by any user (thus a shared user id, e.g. j2ee_guest).

If the service does require identification and authentication, the NWAS Java determines whether the subject is already authenticated and initiates a logon process otherwise.

In either case, the service itself may implement additional authorization checks for all or part of its execution, and denies execution if the subject cannot present appropriate authorization.

This security functionality implements the Security Functional Requirements: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FIA_USB.1

7.3 Users and Authorizations

The TOE provides two different concepts for access control:

Declarative Security:

Within the declarative security concept for access control applications inform the TOE about the required permissions for users to access an object under access control. Every time the application requests access to an object under control (on behalf of a user) the TOE verifies the permissions of that user and denies the access to the object for the case that the user doesn't have the required permission.

Programmatic Security:

In an application using the programmatic access control concept the application itself forms an important part of the overall policy. The TOE provides the application with services to acquire the (confirmed) identity of the user and to check whether the current user has a certain permission.

However, it falls into the responsibility of the application to deny the access of the user to an access for the case that the user does not have the appropriate permission.

As the application forms an important part of the overall access control policy – for the case of programmatic security - it has to be assumed that the application follows the SAP Programming Guidelines (see A.DEVELOP).

This security functionality implements the Security Functional Requirements: FDP_ACC.2/D, FDP_ACC.2/P, FPP_ACF.1/D, FDP_ACF.1/P

7.4 Security Management

The focus of this security functionality is to provide only authorized administrators with the functionality to manage all relevant aspects of the security functionality of the TOE. The TOE provides its services for management via two interfaces:

1) Web based (i.e. the administrator uses any browser for administration)
2) Via the Visual Administrator

Specifically the TOE provides the following management functionality:

1) Management of User Accounts
    a. Delete,
    b. Create,
    c. Lock,
    d. Unlock,
    e. Assigning and removing roles to users,
    f. Modify the password and the password status of users,
    g. Managing the groups of users.

2) Management of J2EE Roles
    a. Create,
    b. Modify,
    c. Delete.
3) Management of UME Roles
    a. Create,
    b. Modify,
    c. Delete.
4) Management of authentication
    a. Managing the list of actions that can be taken before the user is authenticated.
    b. Management of the threshold for unsuccessful authentication attempts.
5) Management of audit
    a. Start and stop audit
6) Management of the password quality policy

This security functionality implements the Security Functional Requirements: FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FMT_MOF.1, FMT_MSA.1/D, FMT_MSA.1/P, FMT_MSA.3/D, FMT_MSA.3/P, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1

8 Appendix

8.1 Abbreviations and Acronyms

ABAP	Advanced Business Application Programming (SAPs proprietary programming language and environment)
ACM	Assurance Class “Configuration management” of CC Part 3
ADV	Assurance Class “Development” of CC Part 3
AGD	Assurance Class “Guidance documents” of CC Part 3
AIS	Application Notes and Interpretations of the Scheme
aka	Also known as
API	Application Programming Interface
AS	Application Server
AS-ABAP	Application Server ABAP
ASE	Assurance Class “Security Target Evaluation” of CC Part 3
AS-Java	Application Server Java
ATE	Assurance Class “Tests” of CC Part 3
BSI	Bundesamt fuer Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CC	Common Criteria (= Common Criteria for IT Security Evaluation = ISO 15408)
CPU	Central Processing Unit
CRM	Customer Relationship Management
DB	Database
DBMS	Database Management System
EAL	Evaluation Assurance Levels (CC levels range from EAL1 (lowest) to EAL7)
GUI	Graphical User Interface
http	Hypertext Transfer Protocol
HR	HumanRessources
I&A	Identification and Authentication
ICF	Internet Communication Framework
ICM	Internet Communication Manager
ISO	International Organization for Standardization
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
JVM	Java Virtual Machine
NWAS	SAP NetWeaver Application Server

OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RDBMS	Relational Database Management System
RFC	SAP: Remote Function Call (similar to RPC = ‘remote procedure call’ of other architectures)
RMI	Remote Method Invocation
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSS	TOE Summary Specification
UI	User Interface
UME	User Management Engine
URL	Uniform Resource Locator; previously Universal Resource Locator

8.2 Glossary

Assets entities that the owner of the TOE presumably places value upon

Assignment the specification of an identified parameter in a component (of the CC) or requirement

Assurance grounds for confidence that a TOE meets the SFRs

Augmentation addition of one or more requirement(s) to a package

Authentication Verifying the claimed identity of a user.

Authentication Data information used to verify the claimed identity of a user

Authorization The authority to execute a particular action in the SAP System. Each authorization references an authorization object and defines one or more permissible values for each authorization field contained in the authorization object. Authorizations are combined in profiles, which are entered in a user’s master record.

Authorized User TOE user who may, in accordance with the SFRs, perform an operation

Class et of CC families that share a common focus.

Client

SAP systems use the client concept to allow legally and financially independent entities to coexist in a system. In commercial, organizational, and technical terms, a client is a self-contained unit in an SAP system with separate master records and its own set of tables.

Thus; clients share the same system functions but their user data occupies separate portions of the database so that one client cannot access data of another. When you log on to an SAP System, you log on to a particular client of this system. Any activities you carry out in the system are always carried out in one client.

SAP itself utilizes the client concept by using some clients (usually client 000 and client 066) for its own technical purposes, in addition to the clients that exist for business reasons.

Do not confuse this use of the term “client” with the same term as appearing in “GUI client” or “client-server architecture” with a different meaning.

See also [ADM, section 4.3.8.1].

Evaluation Assurance Level (EAL)

set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Enterprise JavaBean (EJB)

Application module that implements the business logic of an application.

Instance

An instance represents the application layer of the TOE.

Iteration

use of the same component to express two or more distinct requirements

JVM

A Java Virtual Machine (JVM) is a virtual processor responsible for executing the platform independent byte-code of Java programs on the actual platform.

Object

passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

Organizational Security Policies (OSPs)

set of security rules, procedures, or guidelines for an organisation

Package

named set of either security functional or security assurance requirements

Protection Profile (PP)

implementation-independent statement of security needs for a TOE type

Refinement

addition of details to a component

RMI/P4 Protocol

An SAP proprietary implementation of Java Remote Method Invocation (RMI)

Role

CC: A predefined set of rules establishing the allowed interactions between a user and the TOE.

In SAP: The collection of actions that a person performs to participate in one or more business scenarios in an organization.

Secret

information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP

Security Function Policy (SFP)

set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs

Security Objective
statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions

Security Target (ST)
implementation-dependent statement of security needs for a specific identified TOE

Selection
specification of one or more items from a list in a component

Servlet
Application module that implements the representation logic of an application.

Subject
active entity in the TOE that performs operations on objects

Target of Evaluation (TOE)
et of software, firmware and/or hardware possibly accompanied by guidance

Transaction
A logical R/3 process.
From the user’s point of view, a transaction is a self-contained unit such as an address change for a customer or executing a program.
From a dialog programming point of view, a transaction is a complex object that consists of a module pool and screens, and is called by specifying a transaction code.

TSF Data
data for the operation of the TOE upon which the enforcement of the SFR relies

User
human or IT entity possibly interacting with the TOE from outside of the TOE boundary

User Data
data for the user, that does not affect the operation of the TSF

User Identity (User id)
Term used in SAP systems and in SAP documentation. Properly “subject identity”: The identity under which a subject is known in a SAP system.

This may either correspond to an identifiable human user or not. The latter case can be highlighted as “technical user identity”. In this case, several or even all the possible users of the system may act under this id.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Version 3.1, Release 3, July 2009

[SAP Library] The documentation for the TOE comprises the contents of the SAP NetWeaver Documentation DVD [SAP_DVD]

[SAP_DVD] SAP AG: Documentation SAP NetWeaver including BI Content Add-On 2 – HTML-Help for Windows – Standard HTML (Plain HTML). – DVD. Part of the installation media for the TOE.

[AGD_ADD] Guidance Addendum for the Common Criteria evaluation of NWAS Java , Version 0.97