TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor’s Thesis

Overview of Authorizations in an SAP Enterprise Portal Environment

Petteri Sorsa

**Degree Programme in
Business Information Technology
2010**

TURKU UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Degree Programme: Business Information Technology	
Author(s):Petteri Sorsa	
Title:Overview of Authorizations in an SAP Enterprise Portal Environment	
Specialization line: SBITS05 Business Information Systems Management	Instructor(s):
Date: 26.05.2010	Total number of pages: 41

This Bachelor’s thesis describes how authorizations for an SAP ERP system are built and what different aspects and components are involved when securing enterprise data in an SAP environment.

The first part of the work deals with basic theory of the authorizations and application security of SAP ERP system. Things that are covered also include Sarbanes-Oxley (SOX) act and in more detail the Internal Controls of and enterprise. We will have a look what are role based authorizations in and SAP environment and what are the different components of authorizations in a Portal solution.

The second part of the Thesis takes a more detailed look on different work phases that are needed when SAP ERP authorizations are built and what is needed from authorization’s point of view to a Portal solution. The thesis describes what different systems are needed and how roles are built for the back end system as well as how users are authorized to use the portal?

From the findings of the second part we can study what affects and challenges the portal brings to traditional authorization model?

Keywords: SAP, Authorizations, Enterprise Portal

Deposited at: Turun ammattikorkeakoulun kirjasto
Library, Turku University of Applied Sciences

1 INTRODUCTION

Nowadays large scale enterprises have very complex business processes and workflows inside the company as well as between other companies. Therefore it is more and more critical to ensure secure procedures for handling the data of an enterprise. One efficient way of securing the data is well designed authorizations in Enterprise Resource Planning systems such as SAP. Application security is maintained in SAP environment by restricting the operations one user can perform with configured role based authorizations.

The idea for this thesis was born while working in the field of SAP authorizations and I wanted to find out more how authorizations are built generally and what differences does the existence of Portal solutions bring to the overall implementation of authorizations. Therefore the goal of this thesis is to present the basic components of SAP Authorizations and what different things the SAP Enterprise Portal brings to the field of authorizations.

This thesis is structured in three main sections. The first section focuses in covering the theory behind SAP Authorizations in a traditional SAP system and also the basic idea of an SAP Enterprise Portal. The thesis will also take focus on the portal role and what are the different components inside a role that are needed to provide user specific content in the portal. I will also cover the theory of what internal controls are and what different steps are needed to create an Internal Control System.

The second part of the thesis investigates and demonstrates how the different components need to work together in order for a user to use SAP applications via web browser. The section demonstrates what data can be saved in the user master record and how roles are built in the back-end system. The section covers the work needed to create a portal role and how authorizations are linked with the portal role in order to provide access right for a user to the portal. Finally I will summarize the work performed with this thesis for example what different things need to be considered when a portal is taken in to use alongside with the traditional SAP applications.

2 SAP AUTHORIZATIONS

SAP is a world leading company in providing business software such as Enterprise resource planning and related applications such as Supply chain management, Customer relationship management, Product life-cycle management, and Supplier relationship management. SAP was founded in 1972 and to this date it has customers in over 120 countries and is therefore considered as the largest software enterprise in Europe and one of the fourth largest worldwide. SAP NetWeaver was introduced in 2004 as an integrated platform to deliver a synchronization of all the earlier released technology components. SAP NetWeaver provides a single product offering with all platform components fully synchronized, including SAP Mobile Infrastructure, SAP Enterprise Portal, SAP Business Intelligence, SAP Master Data Management, SAP Exchange Infrastructure, SAP Web Application Server, SAP Composite Application Framework and SAP Solution Manager.(SAP)

2.1 SAP Authorization concept

SAP Authorizations basic idea is to allow users to perform only tasks that are in their line of duty and at the same time prevent any unauthorized access to programs, services and transactions. Authorizations are assigned to users via role assignment in the user master data which is used to authenticate user when he/she logs in to the system. Authorization roles consists of authorizations objects that are designed to allow user access to specific transactions and business objects required in the users tasks. Composite roles consist of variety of roles to allow larger scale authorization assignment to users without having to assign large number of single roles. (IBM Business Consulting Services 2003, 42.)

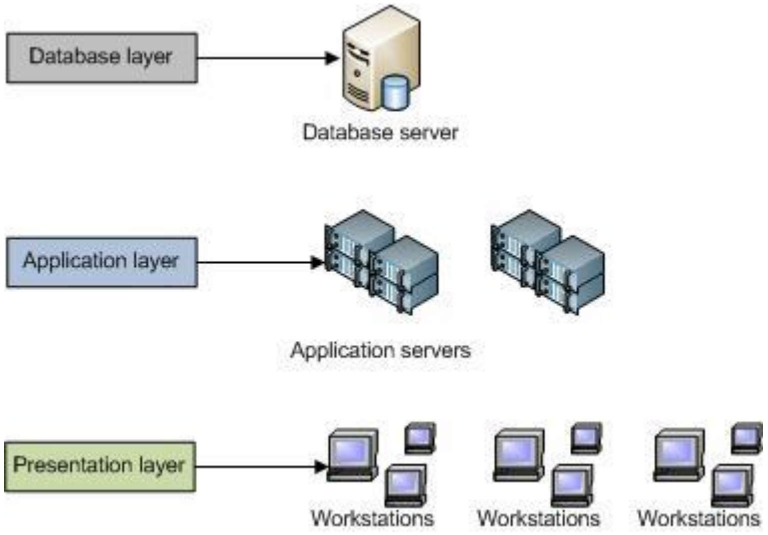
2.1.1 SAP Infrastucture and network security

Traditional SAP R/3 Infrastructure is divided in three layers including Database, Application and Presentation layers. SAP GUI is an application used for the presentation layer and is installed in personal computers. The GUI displays the graphical content of the SAP R/3 application data. Application servers form the application layer which is used together with the database layer to perform queries demanded by the presentation layer. Implementation of security concept with controlled authorizations for the access rights is very important throughout the landscape.

For the network security additionally to firewalls SAProuter is used to control network connections between SAP systems and different external networks. SAProuter can control and log connections to the SAP System. Secure Network Communications can further provide secure communications between different application servers and the GUI.

The database layer usually consists of many servers and they are physically in a different network than the application servers. It is very crucial that security measures are performed thoroughly as users should not be able to access the database directly and therefore servers are positioned in server rooms and detached from the company network. Application layer runs the SAP application and a SAP router controls the communication to the company network. Authorization checks are performed in the application layer level and are used to determine if user is allowed to perform the specific action in the presentation layer. Physically the application layer is protected the same way as the database layer

The presentation layer which is installed in the personal computers in form of the SAP GUI is usually part of the intranet. Authentication to provide application security can be perfomerd for example with username and password checks and in addition for example with the use of smart cards. Picture 1 illustrates the different layers of the infrastructure. (IBM Business Consulting Services 2003, 17-20.)



Picture 1: Basic SAP R/3 infrastructure

2.1.2 Internet transaction server

SAP Internet Transaction Server (ITS) allows SAP systems to connect to the Internet by enabling Internet Application components (IAC) that allow users to connect and interact with SAP R/3 from internet browsers. Component called WGate is used to communicate with the browser and is installed in a separate server. WGate communicates with the Agate that further communicates with the application server and therefore is usually located in the same network. (Internet Transaction Server, SAP Documentation)

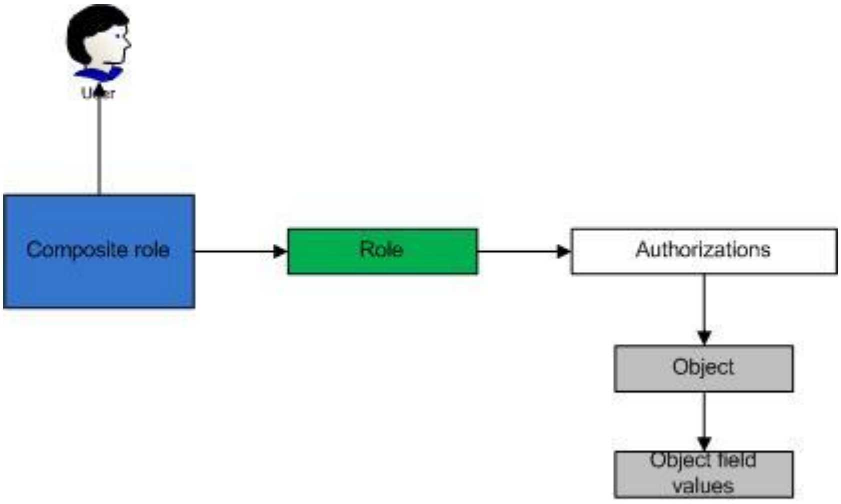
2.1.3 User master record

User data is saved in the user master record which is loaded into the user buffer when the user logs into the system. This data consist all the users personal information as well as the authorization profiles that are assigned to the user. User master records are usually maintained in Main systems and then distributed to Child systems where the actual authorizations in forms of roles are saved to the record. (IBM Business Consulting Services 2003, 32.)

2.1.4 Role

The authorizations of an SAP system are assigned to users in forms of profiles that are associated with a role. Business objects and SAP transactions are protected by authorizations objects which are combined in generic authorizations to serve the needs of the user's responsibilites and activities. These authorizations are assigned to the user in the User Master record. The single role is created in the role administarion tool which also generates the authorization profile. Furthermore the single roles can be combined and grouped in a Composite role that can fully provide all the needed authorizations that a user in the daily work.

Allowed values are stored in the fields of an authorization object that can hold ten different values. In addition when user tries to access a certain function in the SAP system an authorization check is performed by comparing the field values in the program with the values in the authorizations of the user master record. Authorization objects are additionally grouped in classes to provide easier understandment and usability, these classes corresponds for example to an application such as accounting. Picture 2 shows the basic components of an authorization. (IBM Business Consulting Services 2003, 49-50.)



Picture 2: Components of an authorization

2.2 The Sarbanes-Oxley Act

In the year 2002 United States government passed a nearly unanimous vote for a new corporate legislation known as Sarbanes-Oxley (SOX) act. Since then this legislation has made a significant impact in global public companies trading with the United States. Reason for the legislation was to prevent such corporate scandals such as Enron to take place where finance book keeping was altered and evidence were hidden from the public before filing for bankruptcy. The legislation was created “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.” (Sarbanes-Oxley (SOX) Act 2002).

2.2.1 SOX and internal controls

Section 404 of the SOX act mandates that management needs to provide an internal control report along with the financial reporting. Companies must create the internal controls for the financial reporting and also the controls need to be tested all the time to to provide strict requirements for the reporting and furthermore minimizing the possibility of a fraud. SAP Authorization concept plays an important part for the internal control system and the required control mechanisms can be implemented with specific SAP tools and integration of other control types.

First steps when implementing and defining the internal controls are to identify risks in the business processes that need to be mitigated by the controls and what the controls need to achieve. Main objectives include such things as the ensurance of efficient operations, the integrity of the financial data and compliance to the applicable laws. Once the control's objectives are properly defined next step is to determine what factors can cause a possible risk? Such factors can be found within the organization itself for example simply its size in personnel, outsourced services in support functions and hardware providers or anything that can pose a threat to the business. Additional regulations and laws concerning accounting and data processing can also create risks if not fully taken into consideration and also existing rules within the organization needs to be evaluated.

Furthermore the factors that cause the possible risks need to be analyzed by their criticality to be secured with the Internal Controls. Business processes can be analyzed if they can cause such risks from mistakes and errors that can for example produce a violation of a law, loss of money or delays in operations. In addition the risks can be further categorized by severity and possibility of occurance. With this mapping of possible risks and their severity the enterprise can secure its processes with specific control methods.

The defined controls should meet such requirements for example that all the data should be correct and stored so that no data can be lost and also accesses to the information systems should be controlled with authorization methods so that unauthorized access to data is prevented at all times. All changes to company data in information systems are logged and therefore user authentication must be performed every time a user accesses the systems. Users are only allowed to perform such tasks and transactions that are in their line of duty and position in the company and this is called the Separation of duties and possibilities such as creating and approving the same orders are denied with correctly designed authorizations. Also the data should be accessible at all times and the inputted data must always be allocated to the the correct time period and values and transaction are accurately calculated. Control types can be preventive where possibility of risk occurrence is eliminated before a process is started or detective where existing errors are searched by reviewing and analyzing change documents and logs. Example of a preventative control can be for example the requirement to input a unique ID and password everytime a user logs in to the system or separation of duties with authorizations. Detective control may be for example monthly reviewing and reconciliation of financial reports.

The Authorizations of the SAP systems provide efficient features to implement the internal controls. They allow the control of transactions so that users are allowed only to access and execute such transactions that they are authorized for and belongs to their duties. For example system administrators are not allowed to perform the same actions than business users.

In order for the controls to be efficient and up to date specific monitoring needs to be carried out periodically to identify that the risks are assigned to proper control methods all the time. Additionally also internal auditing is necessary for the control system to function and the external auditing should be carried out periodically to confirm that the enterprise complies with the SOX requirements. (IBM Business Consulting Services 2003, 105-124.)

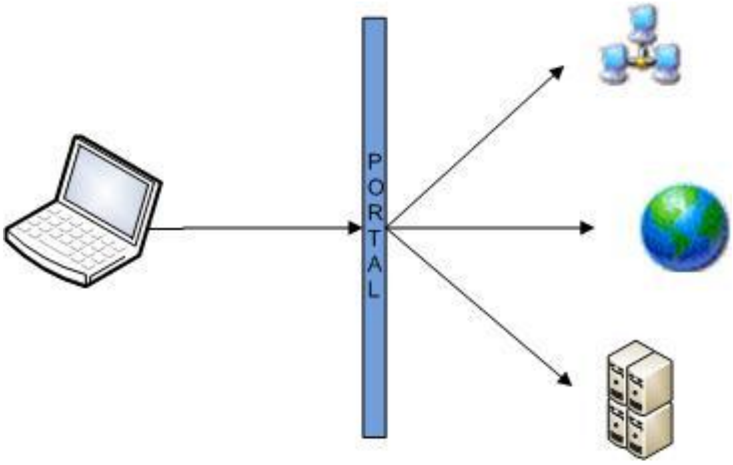
2.2.2 Controlling the authorization process

While working with authorizations I have discovered some general controls that are used to comply with the demands of SOX act. For example it is very important that a company establishes working procedures and processes that provide methods of access right control. It is very important that a process is followed when a new user account is needed for example the manager of the specific user needs to approve and validate that the account need is valid. Also when any user logs into the system a proper authentication method needs to be performed such as checking the username and password combination from a valid source. All changes to roles need to be controlled so that the control of what specific authorizations each role provides is maintained. Roles or combination of roles should have specific responsible persons that provide overwatch of who uses them. In more detail this sort of ownership of roles or composite roles ensures that the separation of critical duties within the company is performed and no user is allowed to perform tasks that are not in their line of duty. Responsible persons also provide validation to changes before they are allowed to be taken in to use. Also all the changes and providing of authorizations need to be properly documented so that eventually they can be easily audited.

2.3 SAP Enterprise portal

SAP portal’s main idea is to offer a single point of access to applications and needed information in their daily tasks. This includes such services as back end applications, self-service applications, company intranet and internet services. As companies secure intranet and Internet are accessed in the same interface the importance of application and data security grows. The portal allows users to access the full functionality of the SAP system via internet browser. Overall access to the SAP is then made easier as no application installations are needed. SAP Enterprise portal authorizations are are also role-based and then is similar to the SAP system. Therefore the main authorizations are maintained in the user master data and the portal system reads the authorization data straight from the backend system. (IBM Business Consulting Services 2003, 225.)

ABAP based systems are the back end systems where user data exists. Authorizations are created by assigning created roles to users. Roles will have defined objects to allow access to data and applications. The user administrator performs all tasks that are relevant to user management and role assignments. In the portal, all user management functions related to users and groups are provided by the user management engine (UME). Portal based systems are created to allow users simple access to company data in the web browser as illustrated in picture 3.



Picture 3: Idea of a portal

2.3.1 Portal components

Different components and their interaction are needed to provide the full functionality of the portal and its idea to allow users to access company’s internal applications. Web server is used to provide HTML-code to the browser and in SAP Enterprise portal an Internet Information Server is used to generate SAP R/3 transactions to HTML. An Application Server provides the communication between the portal and the application and can convert protocols and can manage status of the session. A runtime environment for example J2EE is used when the portal needs to acces programs that are developed in Java programming language. User information can be saved in a component called a directory service which can save all information about the user’s identity and the information that is used between different systems. In addition a SQL-database is used to save all configuration specific data such as the personalized user settings in the portal. (IBM Business Consulting Services 2003, 227-228.)

2.3.2 Interaction between the back end system and the Portal

The Portal supports all functionalities of the backend SAP R/3 system including the business processes and security policies. Therefore the Portal allows users to access all needed applications via internet browser which then eliminates the need for additional installation of software. The interaction between the portal and SAP R/3 can be handled in different ways for example Internet Transaction Server is used to convert SAP transactions to HTML-code. Authorization of the user is then handled by checking that the username and password are correct and then the assigned access rights are compared to the requested access in the portal and a decision is then made whether to user is allowed to proceed. (IBM Business Consulting Services 2003, 229.)

2.3.3 User authentication

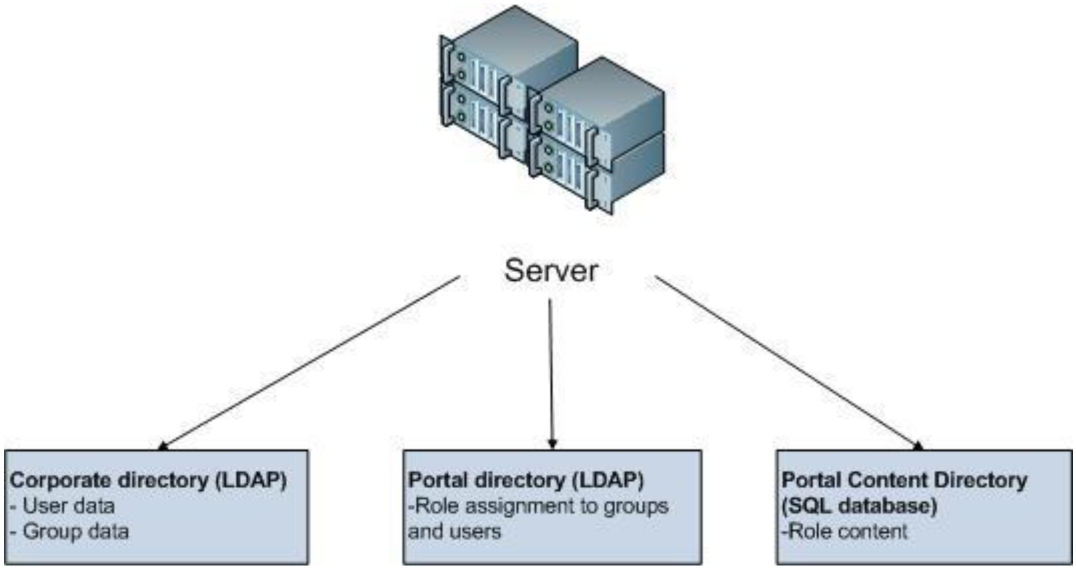
Users are assigned with a unique user ID to assure the authenticity of each user. When user tries to access the system the user ID is checked to identify the person and the password is checked to authenticate the access and finally the system verifies if user is allowed to access or not. Other ways to authenticate users instead of a password are using smart cards or physically by fingerprint or biometric data. Portal supports the combination of username and password, SAP Passport and third party products.

The most usual way to authenticate users is using the combination of username and password. The usernames can be mapped from different systems to allow access from the portal but also a direct logon method can be used when the portal sends the logon information to the accessed system which will then respond back with information if user is allowed access or not. A much more secure but also much more complex way to authenticate user’s password is the use of certificates. Certificates can contain crypted keys as well as information about the user and the certificate itself. Certificates are digitally signed and can be used in any system that supports the technology. SAP Enterprise Portal certificates are included in the SSL (Secure Socket layer) handshake where the user and the portal exchange certificates that hold cryptographic keys in the authentication process. Although the complexity of establishing an own infrastructure to manage the certificates it also allows a lot more safer execution of the authentication since no confidential information is saved on the server and therefore SSL is used as a standard in the internet. In addition to these methods also one time passwords with an own authentication can be used as well as Single Sign-On systems that allow access to multiple systems with one logon. (IBM Business Consulting Services 2003, 232-234.)

2.3.4 User administration in the Portal

Administration of each user can be either maintained separately for each system or centralized in one directory. If an enterprise uses several SAP Systems where the same user master records need to be maintained a common way to handle user administration is the usage of Central User Administration (CUA). All user information is centrally stored in CUA. This information can then be synchronized to individual SAP systems which reduce costs and allows faster modification as user data maintenance is only performed once. The CUA is an individual SAP system which is used to store the user information and the data is distributed automatically to connected child systems.

LDAP (Light weight Directory Access Protocol) is a standard used to access these central directories with TCP/IP protocol. To allow fast server response times there can be many LDAP directories distributed in several remote servers that are synchronized together. CUA is capable to store user information to different SAP systems that are called child systems. This allows the administration of user specific data in both CUA and the child system and the data is then simply synchronized between the systems. This cuts down costs as user maintenance is not needed in every system separately and also the user information is always accurate as the data is synchronized. This also removes the possibility of such users still active in a single system that do not work in the company anymore and also allows faster access right management for new users. In addition a Portal directory and a Portal Content Directory is used, where the Portal directory saves user settings for the portal and the content directory holds personalization data in an SQL database. (IBM Business Consulting Services 2003, 234-236.)


Server
Corporate directory (LDAP)
- User data
- Group data
Portal directory (LDAP)
-Role assignment to groups and users
Portal Content Directory (SQL database)
-Role content

Picture 4: Different directories used to store user information

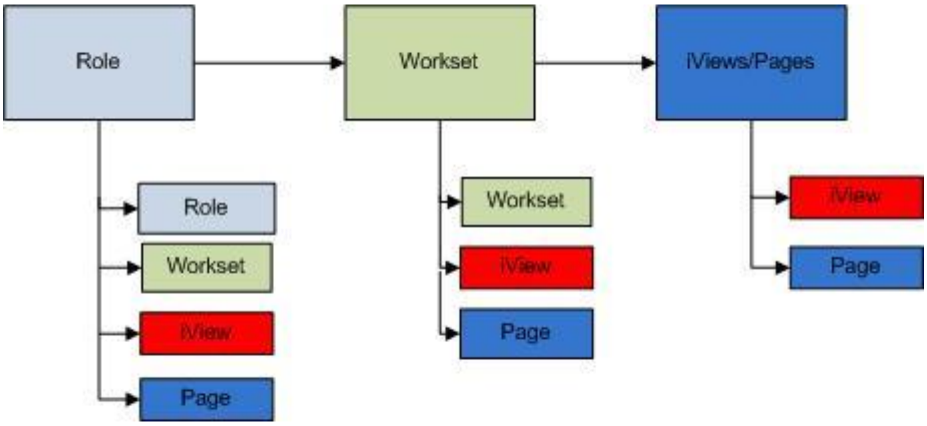
2.3.5 UME - User Management Engine

All user management for the Portal concerning users and groups are performed in the UME. UME is integrated in the J2EE Engine of the SAP Web Application Server Java. UME is capable to read and write user data from multiple different data sources. UME actions are used to allow different Java permissions for users and the actions are either assigned to UME or Portal roles. Basic UME action can be for example UME.Manage_All that is usually assigned to user administrators and allows such permissions as group management, role assignment and import and export of user data along with other permissions. UME web tool displays both UME roles and Portal roles and basically UME roles define authorizations for J2EE applications and Portal roles define the visible content inside the portal but can also have UME actions. UME roles are stored in the user management tables and the Portal roles are stored in the Portal Content Directory of the J2EE database. It is not recommended that UME roles are used alone as then users although having authorizations to the J2EE engine do not see any content in the Portal. (Portal; User administration)

2.3.6 Portal role

The access rights in the SAP Enterprise portal are controlled by role assignment which defines the information and applications the user can access. Role based authorizations allow the separation of role design and user administration which removes the need for individual design of authorizations for every user. An iView is defined to determine what specific access and content, from the back end application, is allowed to be accessed in the portal by the user. The actual detailed authorizations of transactions and allowed data are still defined in the back end system and the portal only retrieves the authorization information. This means that the concept declared in the SAP R/3 doesn’t need to be changed when an Enterprise Portal is taken into use. Roles are managed in the Portal Content Directory and the roles can be assigned to users as well as user group definitions.

Furthermore the portal roles are folders that can hold iviews, worksets and pages. The role structure then defines the actual navigation and layout of the visible Portal for the user that has the roles assigned. Worksets idea is to combine multiple iViews and pages together. This helps the design of common sets of allowed content in the Portal and is easily re-used in many different roles. In contrast to the role that defines the actual role of the user in a company the workset defines user specific activities. Worksets are not directly assigned to users as they need to be assigned via the Portal roles. (Portal; Roles and worksets)



Picture 5: Portal role hierarchy

2.3.7 iView

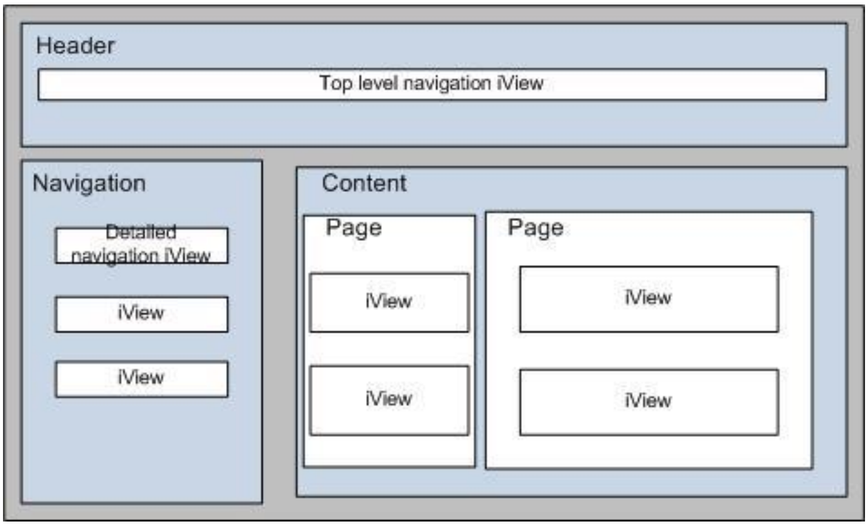
An iView can be any kind of content for example application such as database, an ERP system, intranet, email etc. or any sort of information. Combination of multiple different iViews provides the layout of the portal. An iView can be for example a report from an external source or a search dialog box that is displayed in a web page as a functional element. So the iView is not just a window to an external source of information or an application but offers the functionality of the element within the portal webpage. Administrators can provide customization based on the user's job role for example information that is relevant the specific user and furthermore users can personalize iViews themselves for example by subscribing to specific content for a newsfeed or a report for example. IView’s main idea is to provide useful information and services that adds value to the user’s workspace within the portal.

IViews also provide the portal navigation that is visible for the user. Top-level navigation is located in the header area of the page and can provide up to two levels of navigation which can be defined in the iView properties. Detailed navigation is provided in a hierarchy of links that shows all levels of navigation determined in the top-level in the navigation panel of the portal. (Portal; iViews)

2.3.8 Page

Portal pages additionally are a combination of iViews and other portal pages that together provide a layout of the portal. Pages are created in the Page wizard where a layout is defined to provide containers for iViews. Page editor is used to assign different iViews to the page and defining settings of the page. Users are allowed to change the layout of the page and also organize the iViews within the defined containers to further personalize the page. (Portal; Pages)

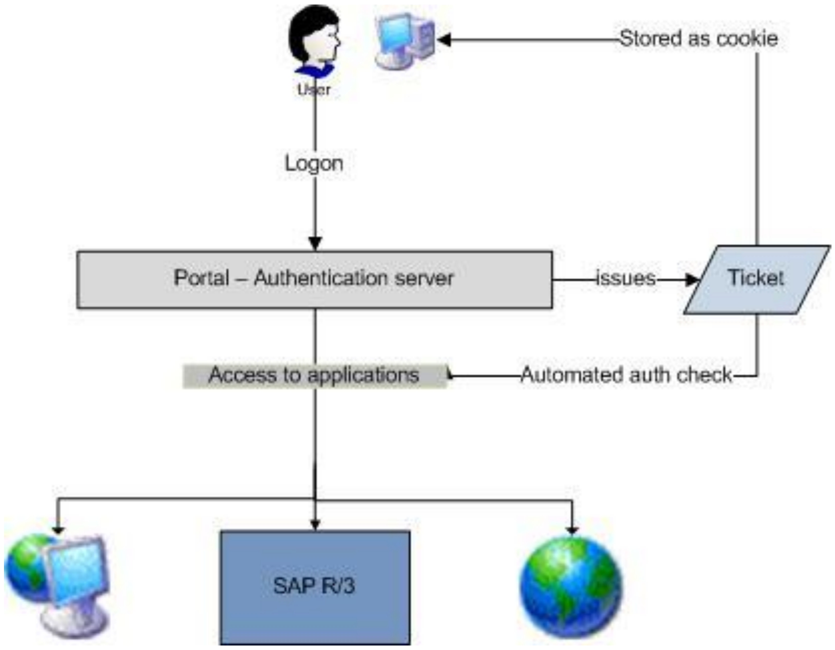
Once iViews and pages are created they are combined in the earlier mentioned worksets that can hold multiple pages and iViews in a folder hierarchy. The worksets are then specifications of the user’s job responsibilities and tasks that are combined in a portal role. Additionally a navigation iView can be defined for the role to determine the top level and detailed navigation.



Picture 6: Portal page structure

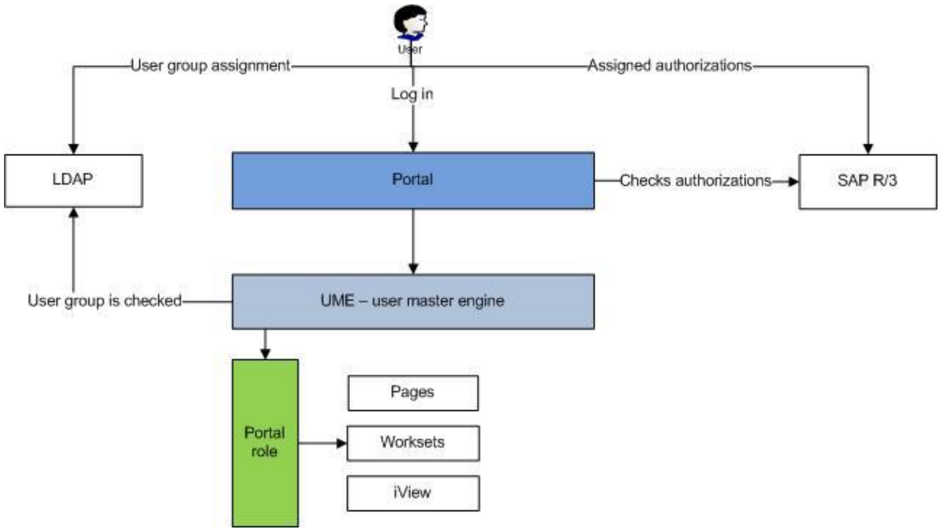
2.3.9 SSO – Single Sign On

A technology called SSO is used to allow users to access multiple different systems with a single logon. SSO allows more tightened security for users using multiple systems as there is no need to have multiple usernames and passwords anymore. An authentication server is the first point of access where the user logs in. The server will then verify the authenticity of the user and a ticket is then issued. This ticket is then used in the backround, when the user tries to access different applications, to allow access automatically. In this case the SAP Enterprise portal acts as an authentication server and like in any other web application the ticket is saved as a cookie to the user's computer. (IBM Business Consulting Services 2003, 239-240.)



Picture 7.1: Login procedure and logon ticket

Another way to authenticate users with SSO is to save the usernames and passwords directly to the LDAP directory. This will then also create a bigger security threat when compared to the ticket as the passwords and usernames have to be saved in the portal directory. User information can be stored and managed centrally in an Enterprise directory LDAP – Lightweight Directory access protocol. This directory can be used in Enterprise portal as well as in SAP component systems. (IBM Business Consulting Services 2003, 241-242.)



Picture 7.2: Login procedure and LDAP

3 IMPLEMENTATION OF AUTHORIZATIONS

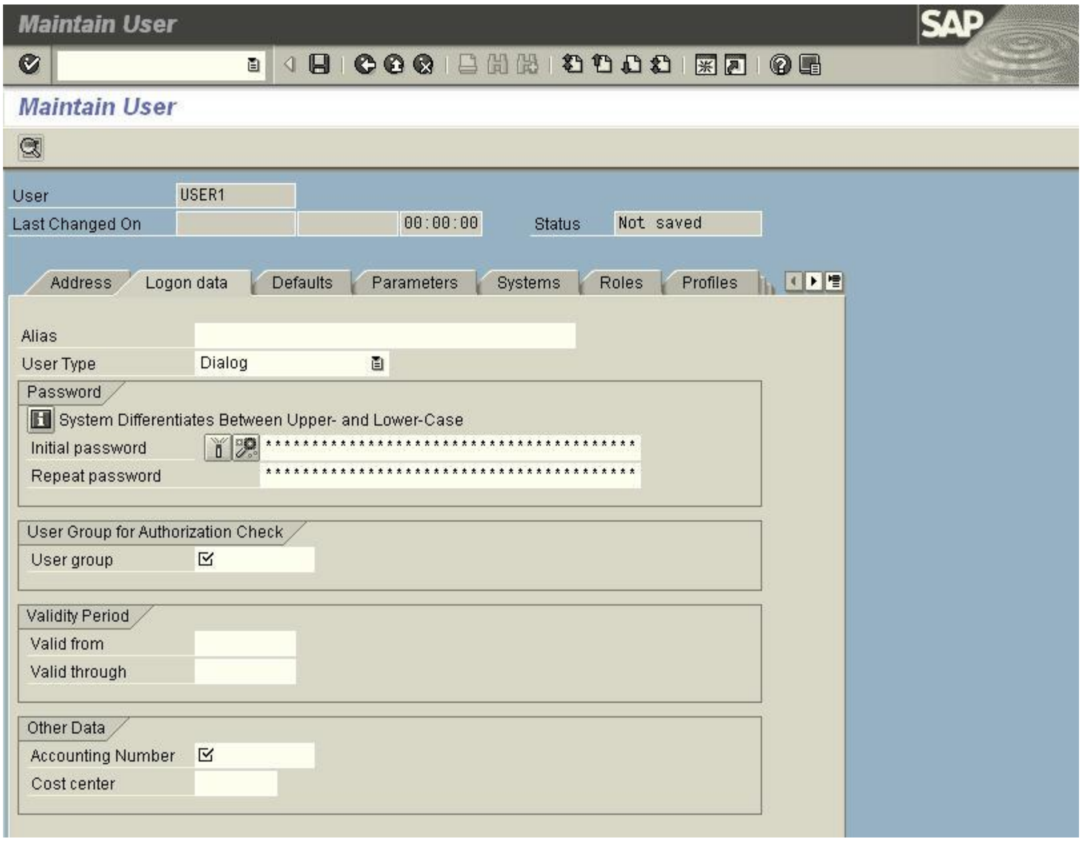
As we have now covered different areas of authorizations in SAP and the portal and we have learned what needs to be considered on the portal side, we can start implementing learned things. In this section of the thesis we will discover how the different components for authorization in the backend system and the portal are created and how they need to work together in order to provide working authorizations and we will also learn how working with authorizations changes when a portal is used alongside with the traditional back end system.

The following information and description of worksteps and knowledge is mainly gathered and learned while I have been working with the authorizations for an IT-department of a global enterprise. I have been following closely on projects where different SAP environments have taken use of the Enterprise Portal and studied documentation about how the portal solution effects the normal authorizations and how portal content is provided.

This chapter of the thesis is dedicated for implementing the authorization concept where the goal is to provide authorizations for a user in the portal to execute specific SAP R/3 transactions via the portal. Steps that need to be included are defining the users and the authorizations in the backend system. Also the system landscape needs to be identified and the way information is exchanged between the systems for example how the user is authenticated during logon and how authorizations are checked when portal needs to display backend transactions and data. Definitions of roles need to be created to both SAP R/3 system and for the Portal and User Management Engine roles. The definition for authorizations of the user administrators is also created to define the difference and separation of duties with authorizations so that for example user administrators are allowed to create and assign roles but the actual end user is not. The whole purpose is not to provide a complete solution for implementing SAP systems or the whole authorizations but to give an example of the basic worksteps needed for providing authorizations in an SAP environment. First step is to define all the tasks and users that are included in the project. Normally an enterprise would include a lot wider user scope, but in this case we are only defining the needed actions for the business user that needs the portal to display for data from the SAP back end system via the internet browser.

3.1.1 User maintenance

In order for the “business user” to gain access to the system a unique user master record is needed to hold all the personal data of the person and also to hold the assigned authorizations in forms of composite roles for example. The user master record is accessed everytime a user logs on to the system and the authorization data is read to the user buffer. In an SAP R/3 system the user master record is created and maintained behind transaction SU01. Users responsible for authorizations need to be authorized to use this transaction in order to create and maintain user data. The SU01 holds the user data in a tabbed structure. Address data holds personal data such as the username, first and last name and data for communication such as phone number, email and address data. Logon data is used to assign an initial password for the user alongside with a user group. During first logon to the system the user is prompt to change the initial password. Also a validity period can be defined for the user in the logon data. User defaults can be used to set optional information such as a specific logon language and a default printer and parameters tab can be used to save default values for specific fields. Roles tab is used to input the single and composite roles for the user. When a composite role is assigned to a user the single roles assigned to the composite role are automatically assigned also. Also the generated profiles from roles are automatically saved in the Profiles tab. additionally personalization tab is used to assign additional application parameters. We will create a user called “USER1” and save the needed information to the main systems user master record and the following image illustrates the SU01 transaction and the Logon data tab.



Maintain User

User USER1

Last Changed On 00:00:00 Status Not saved

Alias

User Type Dialog

Password

System Differentiates Between Upper- and Lower-Case

Initial password **

Repeat password **

User Group for Authorization Check

User group

Validity Period

Valid from

Valid through

Other Data

Accounting Number

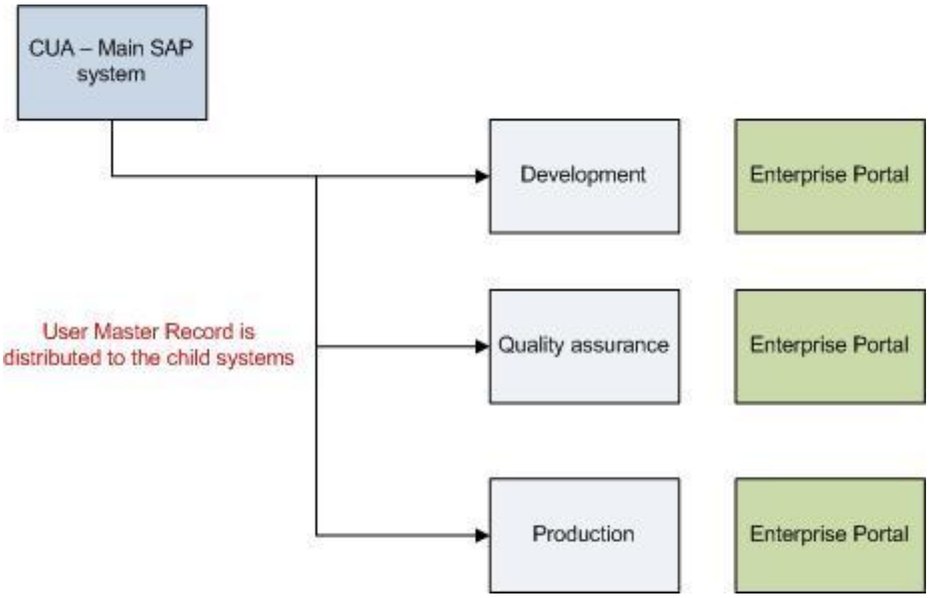
Cost center

Picture 8: Logon data tab behind transaction SU01

When CUA is implemented the user master record can be maintained in the main system and then distributed to the child systems. This also simplifies the user administration as user data needs to be modified and saved only in one place and such actions as locking and deletion of the user can also be performed in the main system. Authorizations are assigned in the user master record of the specific child system so roles are not assigned in the main system.

3.1.2 Systems

The landscape of the systems consist the SAP R/3 main system and the child system. Like mentioned the main system is used to create and maintain the user master record which is distributed to whatever child system desired. SAP recommends that a Three-system landscape is used for the clien/child systems. The Three-system landscape has a development system, a quality assurance system and a production system. The development system is used to create all changes to data. All changes are then released for transport to the quality assurance system which is used to test all changes. Once the changes are as intended they can finally be transported to the production system where the actual productive work is done. The production system is then the actual system where for example the reporting happens and the actual authorizations are assigned. In addition to the SAP back end systems the actual Portal system where the user accesses to read the reports or or whatever possible content that is needed. When user accesses the portal the authorizations are checked from the back-end system and if the user is allowed to access the requested transaction or business object the content is displayed in the browser.

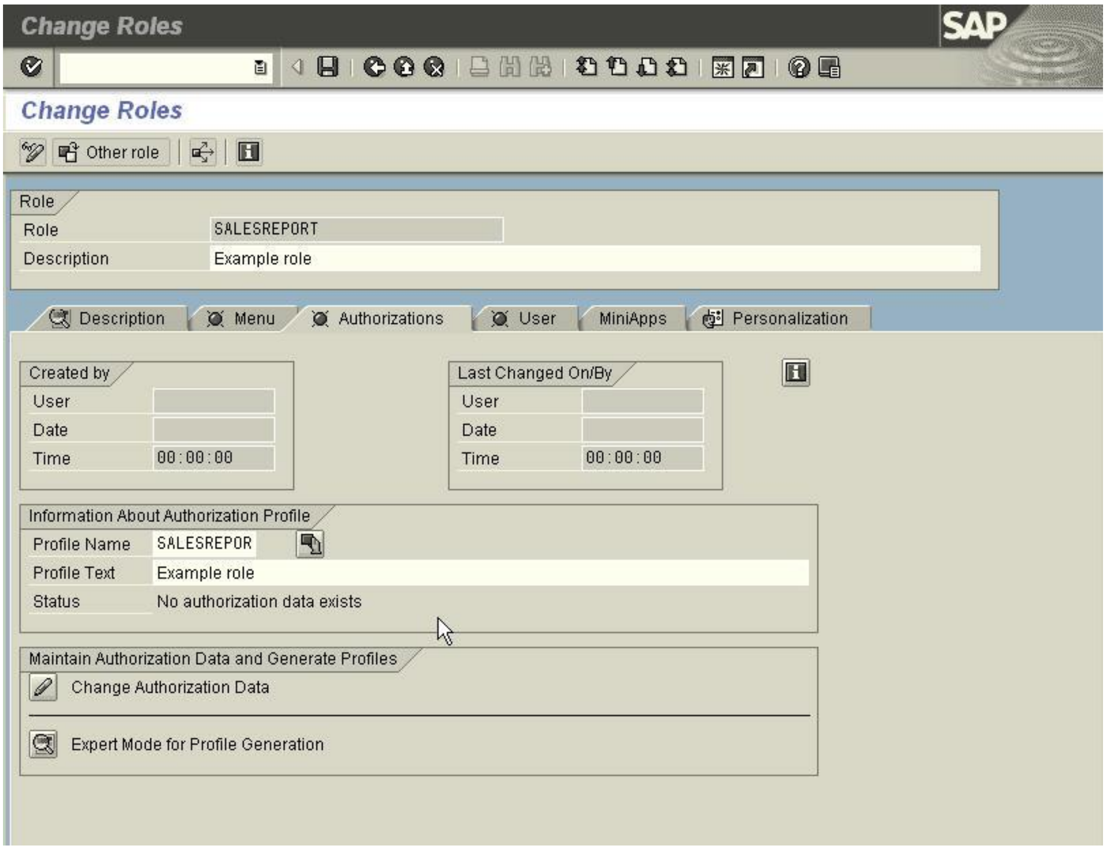


Picture 9: Three-system landscape

A System Landscape in the portal is used to map all the systems including back-end systems, external systems and portal systems to enable connections and access for data. A Portal Archive (PAR) file exists in the Portal Content Directory to save all the needed information for the connection.

3.1.3 PFCG – Profile generator and the creation of roles

Transaction called PFCG (Profile generator) is used to create single and composite roles in an SAP R/3 system and therefore the persons responsible for authorizations need also authorizations for this transaction. The single roles can be created by manually assigning transactions and authorizations objects or by using templates provided by SAP. The role is ultimately saved and the PFCG generates the profiles for the role menus that contain all the transactions provided in the role. Once all needed authorizations are created via single roles for a user in a specific job position the roles are grouped in a composite role to ease the assignment of needed authorizations per user. The PFCG interface is also a collection of tabs where the role information is inputted. The description tab displays information when the role has been created and additional description of the role. Menu tab display all the transactions that the role holds and also allows the assignment of the transactions. Authorizations tab contain the profile name and description and allows access to change the authorization data. Where all the authorizations objects are listed in a hierarchy and their field values can be accessed for modification. User tab displays all the users that have the specific role assigned.



Role

Role: SALESREPORT

Description: Example role

Created by

User:

Date:

Time: 00:00:00

Last Changed On/By

User:

Date:

Time: 00:00:00

Information About Authorization Profile

Profile Name: SALESREPOR

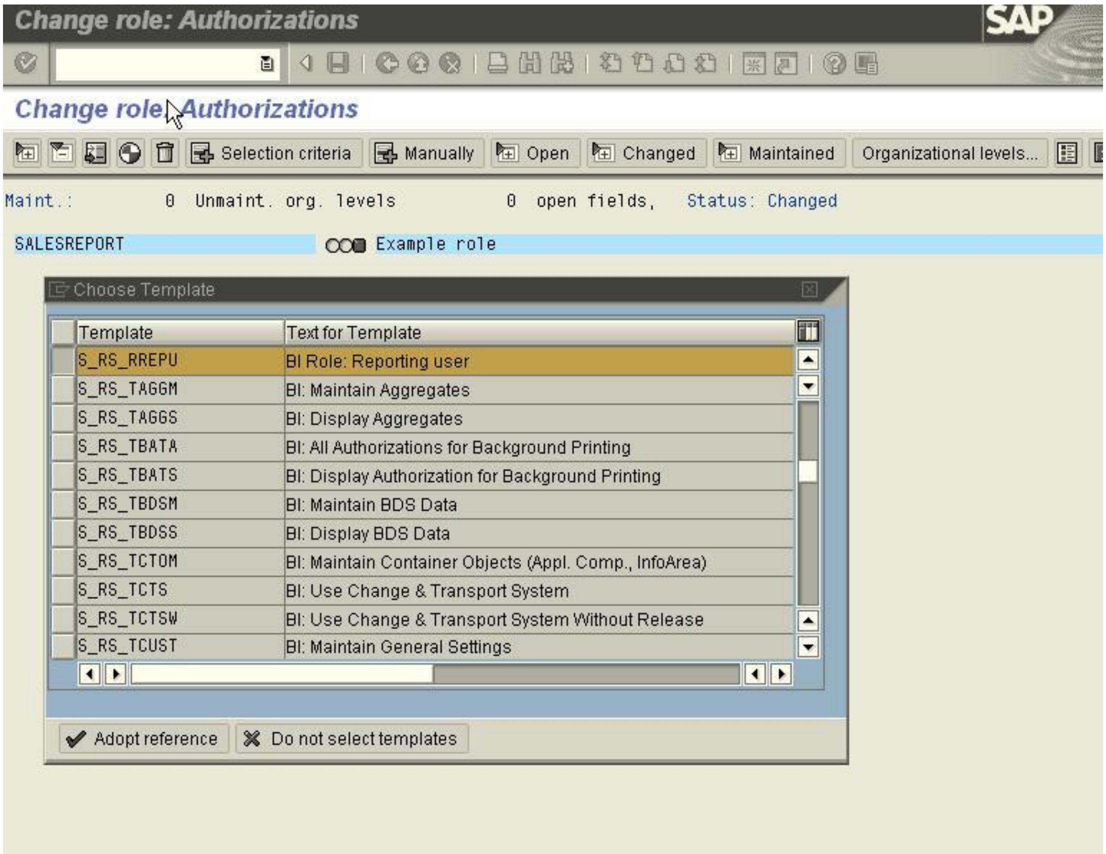
Profile Text: Example role

Status: No authorization data exists

Maintain Authorization Data and Generate Profiles

Picture 10: Authorizations tab in PFCG

We create a role called SALESREPORT in the PFCG to demonstrate the steps needed in creating the role and generating the profile. We also create a composite role called SALES_COMP where the single role is eventually assigned. The system does not distinguish between single role names and the composite role names so therefore it is recommended that a naming convention is adopted before the roles are created. In this case it does not matter as we are simply creating a few examples. The role name is inputted to the Role field and Create single role button is pressed. This action creates the role to the system and opens the view of the PFCG displayed before. Description for the role is inputted in the Description field and possible longer description in to the Long text box of the Description tab. After this the needed transaction are assigned in the role menu tab. In the Authorizations tab we will proceed to the modification of the authorizations data. SAP has templates for different authorizations and the when we access the Change authorization data the program automatically suggest if a template should be used. We choose a template just as an example in the following image.

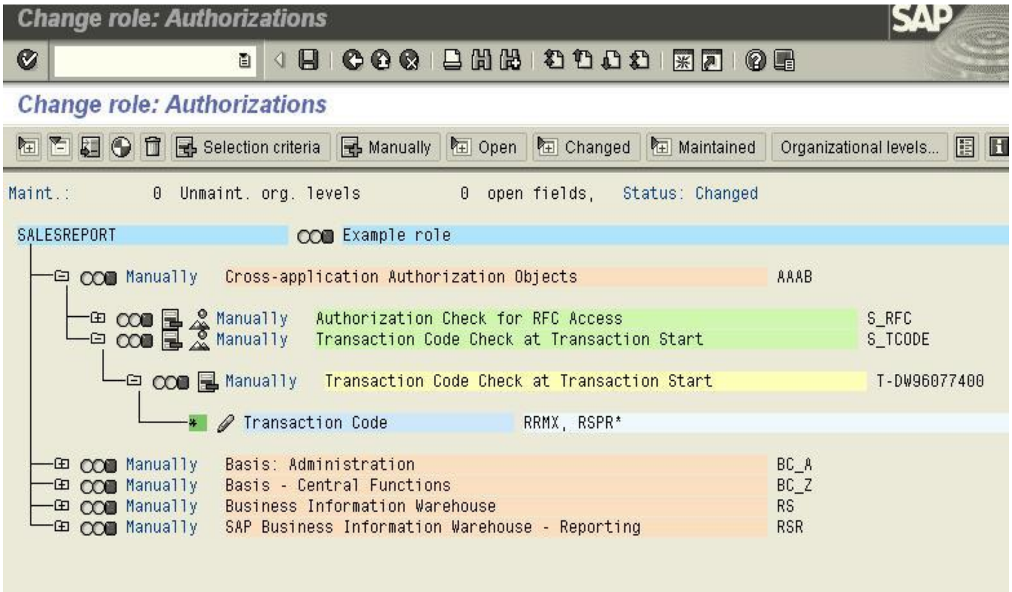


```
Maint.:          0 Unmaint. org. levels          0 open fields,   Status: Changed
SALESREPORT                        Example role
```

Template	Text for Template
S_RS_RREPU	BI Role: Reporting user
S_RS_TAGGM	BI: Maintain Aggregates
S_RS_TAGGS	BI: Display Aggregates
S_RS_TBATA	BI: All Authorizations for Background Printing
S_RS_TBATS	BI: Display Authorization for Background Printing
S_RS_TBDSM	BI: Maintain BDS Data
S_RS_TBDSS	BI: Display BDS Data
S_RS_TCTOM	BI: Maintain Container Objects (Appl. Comp., InfoArea)
S_RS_TCTS	BI: Use Change & Transport System
S_RS_TCTSW	BI: Use Change & Transport System Without Release
S_RS_TCUST	BI: Maintain General Settings

Picture 11: Template selection for a role

As an example we chose a template that is used for building authorizations for a reporting user in SAP NetWeaver Business Intelligence module. Although this specific template holds no signifigance in this thesis as we are merely touching the surface of authorizations and not building thorough solutions for an entrprise we can still have a look what kind authorization objects this specific template would assign to the role. The following image illustrates the authorizations objects in the role and the one expanded stores the values of specific transactions that are assigned in the role.



Change role: Authorizations

```
Maint.:        0  Unmaint. org. levels        0  open fields,   Status: Changed

SALESREPORT                  Example role
 ├─ Manually  Cross-application Authorization Objects                     AAAB
 │   ├─ Manually  Authorization Check for RFC Access                        S_RFC
 │   └─ Manually  Transaction Code Check at Transaction Start               S_TCODE
 │       └─ Manually  Transaction Code Check at Transaction Start            T-DW96077400
 │           └─ Transaction Code              RRMX, RSPR*
 ├─ Manually  Basis: Administration                                       BC_A
 ├─ Manually  Basis - Central Functions                                   BC_Z
 ├─ Manually  Business Information Warehouse                              RS
 └─ Manually  SAP Business Information Warehouse - Reporting              RSR
```

Picture 12: A view of Authorization objects in a role

Once the needed settings are applied to the objects the role is generated and saved. After this the role is assigned to the composite role which can be assigned to the end users user master record.

3.1.4 Portal role creation

The portal role creation with iViews, worksets and pages are mainly done by the content administrator of the Portal but it is important from the user administration point of view to understand how the content is created.

Like explained earlier in the theory part of the thesis a portal role consists of other portal content and is structured as a folder hierarchy to hold all the content. The content is stored in the Portal content directory. Portal role development is done in the Portal Content Studio. The studio has all the editing tools needed to create and administrate the portal content. The studio also allows administration of the Portal Catalog which provides access to all content in the Portal content directory and allows the organization of all content in hierarchy structure. The environment provides an efficient tool for editing the whole portal content including the roles although at the sametime creating a conflict in the separation of duties as the administrators have access to edit everything in the portal. Portal roles are created in the Role wizard of the Portal content studio and are stored in the Portal catalog in pre-created folder. The General properties of the roles that are defined are the Role name, a unique ID, ID prefix, language and the description of the role. For future reference we can name our role simply PORTAL_ROLE. After this the content hierarchy is created in the Role Editor and the actual role content of iViews, pages, worksets and other roles are added to the role. Additionally the role editor allows the modification and permissions setting of the role.

Worksets are created similarily than the roles and they do have their own Workset wizard. When the workset is created the same basic information needs to be saved than with roles also. The editor allows additionally the controlling of permission and the editing of the workset.

The portal permisisions are used to define user access to objects in the Portal Content Directory. It is possible to assign every portal object directly to users but the preferred way is doing it in controlled manner by using user groups and roles. By default the user rights are very limited and the super administrator role has authorizations for the whole portal functionality and the content objects. The editor is used to assign different permissions to the objects for example Administrator level rights are used to determine who is allowed to see content in the design-time. End user permissions are used to control what content is allowed to a portal user in the run-time. Role assigner permissions are used to determine the users who are allowed to perform role assignments. So the permissions assigned to the user determine what objects are visible and the permission level determines what actions users are allowed to perform to the objects. So the permissions are additional way to control the portal objects and does not effect the actual SAP authorizations in any way.

3.1.5 Creating an iView

IViews are created in the iView wizard based on for example templates, components or Web Dynpro applications. To create an iView that will retrieve data from the back end system a Java Connector Architecture standard is used to provide the support for the connection. It is possible to create two types of iViews, in the first option data is queried from the system and rendered in to a matrix and the second one which displays the GUI of the application directly inside the iView. It is possible to display different types of data from the back end system such as transactions, different kind of reports and SAP MiniApps. A representative connector that corresponds to the back-end system must exist in the portal in addition the Portal Catalog has system templates that provide the properties needed to access the system.

To create an iView to a back-end transaction a transaction template is used. The connection is either handled by a connector or with the Internet Transaction Server. Basic properties including the System alias, the actual transaction code and SAP GuiType are saved to the iView properties. System's alias is additionally defined in the Portal content directory and refers to the actual system where the transaction is executed. GuiTypes can be of three different types WebGui, JavaGui and WinGui. For example the WebGui uses the Internet Transaction Server to generate the desired content into HTML and then displayed in the browser. Once the iView is created it can be assigned straight to the created role or into a workset or a page.

3.1.6 Creating a page and a workset

Pages are also created by copying existing pages or by using a Page Wizard. Similarily also basic information needs to be set when the page is created including name, ID, language, prefix and description. A template and a layout also need to be chosen for the page after which the page creation is done. After this the content is added to the page in the Editor for example the iView that displays the back-end transaction. Normally more than one iView and a page is needed to serve the end-users needs and worksets are used to bundle iViews before they are directly assigned to a role. Workset has its own wizard also in the Portal Content Studio and they are also saved in the Portal Catalog with same basic properties needed for other content as well. After workset is created the Editor is used to create a folder hierarchy in to the workset where finally the page can be added.

With the workset created with needed content it can be added to the PORTAL_ROLE and in this case as well a folder hierarchy is defined in the role. Content can be either added as a copy or as a delta link where the added object refers to the original source of the object. When the source is modified the changes are made also to the target objects and the target objects can also be changed individually but the changes will not be copied to the source object. The role is now ready for use and can be further used with the authorizations for the end-user.

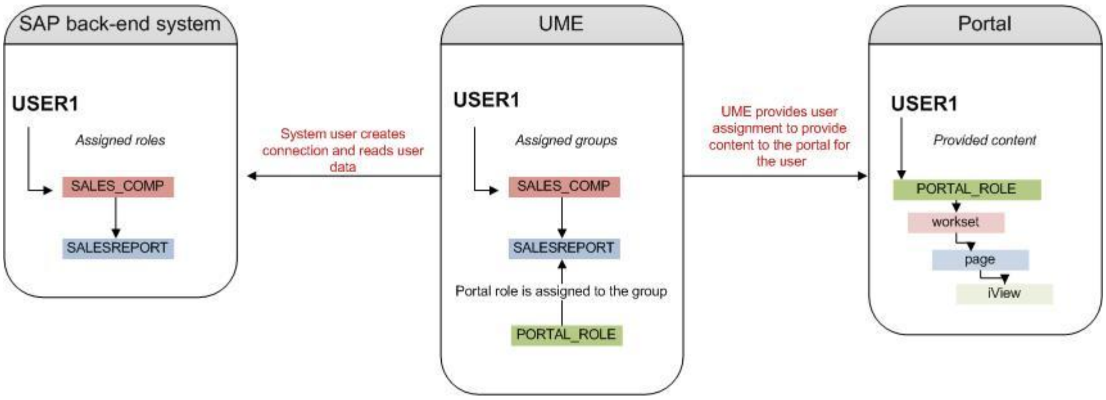
3.1.7 User mapping

Single Sign-On is used to map the back end ID with the portal ID. This can be done by mapping the portal ID with the back end ID and password of the back end system or by using the logon tickets. Needed prerequisites are that SAP NetWeaver Application Server preferably needs to support strong encryption of ID and password, user mapping type defined, logon method, user mapping fields in the the system and system alias defined. A reference system needs to be defined when user mapping for SSO is done with logon tickets to the back-end system. User mapping data can be maintained either by using an Administrator Tool or by allowing the user to map its own user data.

3.1.8 User Administration in the UME

Now that the role role is created it can be used for user assignment in User Management Engine which is used for all user management tasks concerning users and groups in the portal. To be allowed to assign portal roles to users and groups the user administrator needs to have role assigner permissions for the role that needs to be assigned. UME roles instead are not controlled by the role assigner permission but are authorized for the user administrator via UME.Manage_Roles action. This though creates a conflict when trying to comply with the separation of duties as the UME.Manage_Roles action allows the user administrator to assign also the Administrator role and that way gain all the administrator functions to the portal as well.

UME data sources need to be configured when UME is taken in to use. These data sources provide the user management data for the UME and there can be multiple different and already existing sources that are used at the same time. A configuration file defines the settings for the sources for example user data that is saved to the LDAP directory. UME can use three different types of data sources which include Database of the AS Java, Directory service such as the LDAP and User management of the AS ABAP. To use the user management of the application server ABAP as a data source provides an efficient way to bring the back-end users to the UME and also importantly the roles assigned to users are visible as groups in the UME. Like in our example where user needs to be able to use the portal as an additional feature to the back-end system this usage of the back end as a data source simplifies the user management task in the UME. As an example the roles assigned to the user in the back end system appear and are assigned as groups to the user in UME and additionally the portal roles and UME roles can be assigned to these groups and that way provide the portal role functions and content directly to the user. To create the connection a user of type System needs to be used in the UME. A default user named SAPJSF is created in a combined installation of SAP Application Server ABAP and the AS Java Installation to the UME and it is provided with a role called SAP_JSF_COMMUNICATION_RO that provides read-only access to the back end system’s user data. So simply this feature reads the user data and assigned roles from the back end system to the UME where roles are displayed as groups that are assigned to the user and the portal role is the assigned to the group which then provides the portal content to the user and user. The following picture illustrates the use of the back end as a data source for the UME.



Picture 13: Overview of authorizations

Finally the user has back end authorizations in the back end system which are read to the the User Management Engine that is used to assign the actual portal role for the user. Furthermore the portal role provides needed content for the user in the portal that can be accessed via internet browser. Although a lot of administration work and content creation is needed to actually reach this point the idea how different parts of the authorizations are utilized in order to provide user with needed access rights are now described.

4 SUMMARY

Now we have covered basic steps that are needed to handle authorizations in an SAP based environment. We have discovered how user master record is maintained and distributed from system to system to make user account management easier and how roles are built and combined in composite roles. Furthermore we have learned the basis of a Portal solution as a supporting application for the back end systems and how the content is created with components such as iViews, pages and worksets combined in a portal role. Also the concept of User Management Engine and its key part in the whole process of providing the ability to read user data from a data source and create user assignment for the roles created in the portal.

This thesis has provided knowledge in key parts needed for authorizations and does not try to provide a thorough guidebook how to build a complete authorization concept. But rather to give an idea what different components need to be considered when SAP systems are taken in to use and that authorizations play a key part in designing secure systems which in many cases and generally is not recognized as an important area. Therefore many projects in big enterprises suffer loss of money and time since authorizations are recognized only in latter parts of application projects and not clearly implemented from the beginning.

What comes to solutions like the portal it is easy to recognize the efficiency it brings to normal work routines as there is no need to have heavy application installations anymore and therefore systems can be accessed basically from anywhere without being tied to a specific workstation. Alhtough the providing of authorizations is different but in no means more difficult it creates more difficulties when trying to cope with the internal controls and more specifically in the separation of duties. As normally roles should be crated by people responsible for authorizations it can seem that in the portal side the role is more of a content component than an authorization. Still the portal components are assigned with different permissions and acts as a provider for authorizations and therefore it is not that clear who should create the roles but a working solution could be for example that the pages and iViews are created by content administrators and the worksets and roles by authorization administrators. The UME administration should be in all cases a responsibility for the authorization admins but possesses risks in the role assigning rights as they do not restrict the possibility to assign UME and portal roles to the assignors as well and that way authorization admins can gain rights for components out of their responsibilities. Therefore the application should deny the possibility of one assigning roles to themselves.

The defining of internal controls based the demands of the SOX legislation is no means a simple task but a task that is crucial for the whole business and therefore can not be avoided. Therefore SAP authorizations are ideal to provide thorough control and security for business objects and are easy to maintain and assign ownership and responsibilities specific content controlled with roles. Therefore role based access rights are an easy way to assign ownership for specific roles so that persons are directly controlling who accesses and to which content. So that way an approval process for obtaining access rights is ideal and then a dedicated person needs to approve access rights for specific composite role and that way providing an extra human control. Composite roles provide a great solution to design access rights for a job role and a good way is to set a control that denies the possibility to provide multiple composite roles. Therefore restricting the possibility for one user to fully control a business process and that way implements the idea of duty separation.

To summarize the importance of authorizations is crucial but in no ways the only important thing and therefore IT responsible persons need to co-operate tightly throughout the lifecycle of applications. It is important for system administrators to recognize how access rights are built for the systems and content administrators how users can gain access rights to specific content.

To further study the authorizations of an Enterprise Portal and SAP solutions I would recommend first of all a thorough study of the whole application landscape and therefore it is very important that the people who are in responsible for authorizations are actively included in application projects. To specify areas within the portal I would recommend that the use of different directories such as LDAP that can save and provide user data should be studied. Also the distribution of role information can be performed either from the portal to the SAP R/3 system and that is one method that could also be used when implementing the portal solution. SAP provides new solutions all the time to different areas of business applications and many times the methods of authorization differ from each other and therefore it is very much recommended that an IT-professional responsible for authorizations studies new solutions and applications all the time.

LIST OF REFERENCES

IBM Business Consulting Services 2003, SAP Authorization System, SAP Press

Internet Transaction Server, SAP Documentation, [referred to 15.3.2010]
http://help.sap.com/saphelp_nw04s/helpdata/en/1e/82daf0ee9911d3a6510000e835363f/frameset.htm

Portal; iViews, SAP NetWeaver 2004 SPS23, [referred to 3.3.2010]
http://help.sap.com/saphelp_nw04/helpdata/en/df/bedca2076511d7b84500047582c9f7/frameset.htm

Portal; Portal Pages, SAP NetWeaver 2004 SPS23, [20.2.2010]
http://help.sap.com/saphelp_nw04/helpdata/en/ac/c29d3f53055a7be10000000a11405a/frameset.htm

Portal; Roles and worksets, SAP NetWeaver 2004 SPS23, [16.2.2010]
http://help.sap.com/saphelp_nw04/helpdata/en/4f/bceaffeb8c114ebef8255b63079c7c/frameset.htm

Portal; User administration, SAP NetWeaver 2004 SPS23, [15.2.2010]
http://help.sap.com/saphelp_nw04/helpdata/en/59/bf2287b3cb5e48af94f99929ad15b9/frameset.htm

SAP, official website, [referred to 01.10.2009]
http://www.sap.com/about/index.epx
http://www36.sap.com/about/newsroom/press.epx?pressID=2694