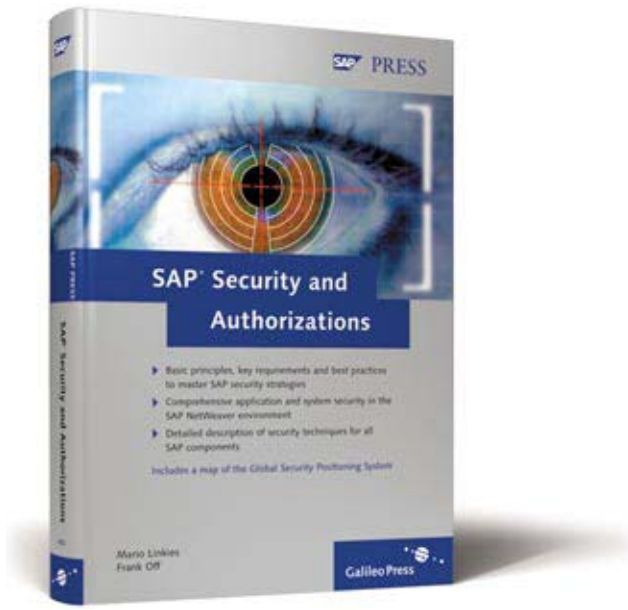
Mario Linkies, Frank Off

SAP® Security and Authorizations



SAP PRESS

Contents

Foreword by Prof. Wolfgang Lassmann

The increasing global networking of computers, reach of national and international business processes over the Internet, and complexity of information systems magnify the risk potential of negligent actions or intentional attacks on information systems. Unauthorized, anonymous attackers with an Internet connection can enter remote systems from any location and cause significant material or economic damage.

SAP, Microsoft, and other well-known companies have recently begun initiatives to improve overall IT security, such as "Deutschland sicher im Netz" in Germany and the "SAP Global Security Alliance." These initiatives help both customers and solution providers collaborate on the design and implementation of the simplest possible solutions for the complex world of IT security.

It is the task of academic and research institutions related to IT to highlight the complicated relationships and risks of attacks on system security and to suggest effective solutions for defense against them.

Mario Linkies and Frank Off have skillfully dedicated themselves to this task in this book. As experienced specialists in the area of IT security at the SAP consulting organization, they possess not only valuable and up-to-date practical knowledge, but also the required theoretical background to understand the essential context.

This book provides a manageable introduction to the broad topic of IT security. The authors have succeeded very well in joining externally oriented technological security management (security reporting) with internally oriented business risk management (risk reporting). Integrated solutions, attention to risks, and a holistic approach are all important aspects of IT security.

This book encourages a critical review of the security solutions that companies have used to date and an examination of them in light of new requirements. Step by step, readers move from risk analysis to effective methods of control and, ultimately, to IT security that meets legal requirements.

This book illustrates the relationships among SAP solutions and other IT components with the required communications and security solutions, the overall theme being the global security positioning system (GSPS). The GSPS points out the options available for using a simulation tool to optimize an IT landscape comprised of SAP and other industry solutions.

I am sure that this book makes a significant contribution to important work in the area of security and risk management in the IT industry. The authors are to be thanked for their efforts.

April 2006
Prof. Wolfgang Lassmann
Professor of Business IT and Operations Research
at Martin Luther University, Halle-Wittenberg, Germany

Foreword by Dr. Sachar Paulus

From the vantage point of security management, the central observation of the past few months is that security and compliance are increasingly converging. Until recently, the fulfillment of legal requirements in IT (except in a few industries) was a topic that primarily interested boards of directors, because compliance was limited to supervisory authorities in stock markets and correct accounting. IT security experts paid more attention to infrastructure topics.

Until 2002, the interest groups were split, with accountants and internal auditors on one side, and IT security experts on the other side. The latter dealt with the network security, email systems with firewalls, anti-virus management, and password management; the former dealt with authorization in business applications.

Although both groups have the same objective (everything should take place correctly), each uses a different language. Security experts speak of activities and threats; auditors speak of controls and risks.

The convergence of both areas is due to two factors:

- The collapse of Enron and the resulting legal initiative of the Sarbanes-Oxley Act (SOX) have significantly increased the liability for controls in IT systems and specified procedures for dealing with risk. IT security has often taken many of the required steps, but not when necessary to comply with auditors.
- The opening of business systems to customers and partners over the Internet became an urgent necessity. All of a sudden, personnel in IT security and auditors had to speak to each other. Such conversations weren't necessary in the past, because auditors looked at the inner workings of a company and IT security experts were responsible for the surroundings. But today there is no more inside and outside. Now, each individual process must be protected properly, and that requires collaboration between those responsible for the infrastructure and those responsible for applications.

At SAP, a global organization with more than 33,000 employees in 60 locations, we now find ourselves at such a juncture. We have a global security organization and a global risk management organization; local units often give both roles to one employee. We have risk reporting, and we have security reporting. Security risks show up in risk reporting, while legal guidelines for security requirements show up in security reporting. Cooperation between both methods and their subsequent integration are always being driven ahead at the technical and process levels. It is only a matter of time before cooperation and integration are implemented organizationally.

Many SAP customers have already taken this step and set up central departments called Security & Controls or Chief Information Security Office. These departments are responsible for the implementation of legal guidelines like SOX, the German data protection law, FDA CFR Part 11, and California Civil Act SB 1386, and for technical, organizational, and personnel activities and controls. The separation of risk management and security solutions is no longer visible in these companies.

Yet despite all the competency on the market, finding concentrated success factors is still rare: practical knowledge about controls for specific technologies, a uniform language, and best practices. Specialists at the interfaces of business and technology are required to bundle this knowledge and then format and spread it methodologically so that proper controls can be effectively implemented throughout the industry. SAP has a special role to play here. SAP is active at the crossroads of business processes and technology more than any other software company. Its objective is to make the most of technological advances in innovative business processes. That's why SAP also has a special responsibility for modeling controls for these new types of business processes:

- The solutions offered by SAP must support integrated control options up front and include them as part of the processes. The use of new technology, like service-oriented architecture (SOA) will probably not work with traditional methods and requires integrative solutions and methods.
- SAP, its partners, and specialists close to SAP are best able to develop and spread the knowledge required to define proper controls, to establish it at national and international levels in companies, and thus use trustworthy business processes productively.

This book is an important step toward recognizing compliance and security requirements in future architectures and illustrating the required solutions. For the first time, the security aspects of SAP software are examined with regard to compliance and risk; the necessity of such aspects is also evaluated. Above all, the book looks at new SAP solutions that already show the first characteristics of SOA. As the director of the Risk Management & IT Security global focus group of the SAP consulting organizations, to which Dr. Frank Off also belongs, Mario Linkies has the practical experience of bringing SAP solutions to clients around the world—in a manner that conforms to legal requirements—and a sufficient familiarity with new concepts to influence the design of new products based on his experience. Mario Linkies and Frank Off are therefore the ideal authors for this broad subject area.

I hope that this book offers you a good introduction to the topics of risk and control management, compliance, and IT security. I hope it simplifies your work in operating SAP solutions securely and in conformity with legal requirements. Moreover, I hope that you obtain food for thought and ideas from this book, and that you make the right investments in IT security to be able to lower operating costs.

April 2006
Dr. Sachar Paulus
Chief Security Officer
SAP AG

1 Introduction

We live in an insecure world. Markets, finances, company assets, people, work, health, culture, and values: everything seems threatened. Some of these threats are real; others influence many developments in our lives. Security is a basic human need. And that's true in one's personal and professional life. Risks are a part of life. They offer opportunities, but they must remain calculable. That's why transparency is required. There are various ways to minimize risks and reach your required level of security.

The control and reduction of risks will be a primary focus of IT in the coming years. Growing functionality, changing technology, the opening of internal IT systems, and increasing national and international regulations like Sarbanes-Oxley (SOX) and Basel II necessarily produce new requirements for secure processes, systems, and users. Globalization links national and international business partners via B2B, I2I, and B2G scenarios. Employees are equipped to use new and more effective means of communications and applications. Customers and consumers increasingly use the Internet and mobile devices to access information, make reservations, or place orders. Dramatic economic and technological changes are reflected in business and market processes. But these changes are accompanied by new risks that affect, greatly influence, and disturb markets, processes, systems, organizations, employees, partners, and customers. These developments and the interaction of business partners, employees, and customers can be protected only with appropriate security strategies and measures. This book highlights the essential elements of security measures and controls.

1.1 Background

In the last few years, SAP has made a quantum leap. Its offerings of functionality have been expanded, along with its implementation of new technologies, applications, and systems. An essential step in this leap is the move from the previously delimited architecture based on the ABAP/4 programming language to the new SAP NetWeaver architecture with components like SAP Enterprise Portal, SAP Exchange Infrastructure, J2EE, and a mobile infrastructure. On the one hand, the new technologies and enhanced functionalities improve options for integrating partner companies and customers. On the other hand, they require attention to and reduction of the risks that the new developments pose.

The financial collapse of large companies like Enron and the activities of managers and auditing companies at the beginning of the new millennium have profoundly shaken investors' and shareholders' trust in publicly traded companies in particular. These developments led to new laws and the expansion of national controlling

standards like the Sarbanes-Oxley Act in the United States for publicly traded companies, and Basel II for the financial industry. The objective of such laws is to establish stronger controls and improved security measures within companies and organizations to protect investors, companies, employees, and consumers. One way to implement the laws for national control, which include fines for the managers responsible, is the use of consistent security of IT-supported processes, business transactions, and financial data extracted from IT security measures.

Furthermore, many of the existing organizations that have implemented SAP products have a large backlog of measures needed to establish effective authorizations and secure, optimized administrative processes. Because practically no methodological standards for authorizations and role structures exist, companies use an almost endless variety of solutions related to technical IT security. Authorization administrators are somewhat overwhelmed, and processes often don't meet actual requirements for secure user administration and management.

This book is based on the international consulting and teaching experience of the authors and their close collaboration with SAP and partner companies in the area of risk and security. It provides an overview of SAP NetWeaver security, in general, and an introduction to the components of a secure implementation of SAP products. The authors do not profess to have written everything about security that you need to know, but they do follow a consulting methodology when describing concepts, problems, procedures, and examples. The information in this book will be beneficial to company management, financial auditors and internal accountants, Sarbanes-Oxley teams, information owners, data protection officers, authorization administrators, leaders of SAP implementation projects, security officers, as well as employees, service providers, and consultants who are interested in security. Readers will get a beginner's guide to evaluating risks, creating control options, security measure design, and the appropriate procedure to set up supporting practices and processes.

The objectives of the book are to contribute to the improved security of existing SAP systems and processes, to help companies include new technologies and enhanced functionality in the consideration of security measures, and to provide assistance in working through legal requirements in the areas of risk and control management. Individual IT security topics may no longer be looked at in isolation. They must be understood as part of a comprehensive, strategic, and continuous whole to establish security throughout a company and thus for business partners and shareholders.

This book is intended to help, provide support, offer new ideas, indicate best-practice solutions, and offer a view into the complex but important world of IT

security so that companies are able to meet growing requirements with efficient methods, solutions, and strategies.

1.2 Contents

The following overview highlights the content of each chapter of this book.

Part 1

Chapter 2 gives an overview of risk and control management. It explains terms like company assets, risk and control types, and potential risks, and covers methods like risk analysis and control consulting.

Chapter 3 provides basics on security strategy, proven procedures, implementation project and system audit experiences, new methods and principles, SAP security solutions, solutions from security companies, and examples of best practices.

Chapter 4 covers some important legal regulations and requirements that influence IT security and its characteristics.

Chapter 5 describes the country-specific and international security standards that can serve as guidelines for security projects.

Chapter 6 describes the technical and conceptual basics of security solutions for active inclusion in companywide control measures.

Part 2

Chapter 7 provides a basic introduction to the topic of SAP NetWeaver security. It also provides a map of the *global security positioning system* (GSPS) and helps you navigate through it, explains the basic principles of SAP NetWeaver technology, and discusses proven and new security methods and technologies.

Chapters 8–29 cover the essential components of SAP NetWeaver along with risks and control measures. These chapters explain potential risks based on examples and the concepts of application and system security tailored for individual examples. This section provides an overview based on expert knowledge, without becoming enmeshed in technical details.

1.3 How to Read This Book

This book has a modular structure, which should provide value to experienced and inexperienced readers, project leaders and decision-makers in organizations, internal and external employees, and consultants. This book offers an introduc-

tion to IT security and aims to provide a comprehensive overview of the complex world of securing IT-supported processes and connected systems. The chapters build on each other, and most of them follow the same structure.

Explanatory sections and content on the basics, examples, and best-practice methods supplement that material. Best-practice methods are solutions that were used very successfully in the past or that reflect the newest developments in security consulting. They indicate the places where security strategies can be optimized with little effort and quick success.

1.4 Acknowledgements

The authors wrote this book in their free time, that is, in addition to their many responsibilities in national and international consulting and teaching. Therefore, this book would not have been possible without the support they received from their SAP group colleagues, subject-matter experts, security consultants, collaboration with well-known consulting and auditing firms, and the help and encouragement they got from family, friends, and professionals in Germany, South Africa, and Canada. Freda Li (Toronto) created the GSPS map. The authors would like to sincerely thank all of these people for their support.

19 SAP Enterprise Portal

This chapter explains IT security concepts for SAP Enterprise Portal in the Global Security Positioning System (GSPS) area of server security. The integrative portal concept is discussed in detail.

19.1 Introduction and Functions

Like SAP Web AS, *SAP Enterprise Portal* (SAP EP) plays a critical role in the SAP NetWeaver product strategy. Via a central access point, SAP EP provides important applications and information (for example, documents) to individual employees. In an Internet scenario, business partners can also be directed to various Internet applications of the enterprise via this central access point. To start their applications, employees and business partners only need a web browser to access SAP EP. They no longer need to start every application separately, for example, using SAP GUI. SAP EP controls the entire access to these applications. This is referred to as *people integration*, which is illustrated in Figure 19.1.

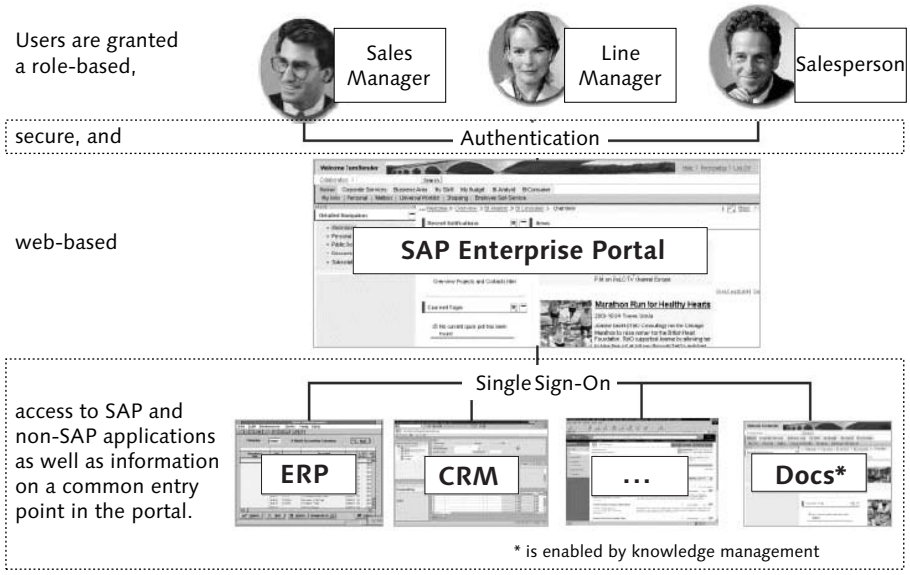


Figure 19.1 People Integration via SAP Enterprise Portal

The authorizations for the applications are controlled using portal roles. Applications are either accessed after an enforced user authentication or anonymously.

Another benefit of SAP EP is the possibility to easily implement a Single Sign-On mechanism for the associated backend applications. Users only need to log on once to SAP EP. SAP EP then takes over any further authentication to the backend applications. In addition to SAP applications, non-SAP applications can also be integrated in SAP EP. Even links to other external resources can be integrated. Additionally, users can customize their content, or they can organize the portal content, like documents, for managing their own know-how. This makes it possible to integrate a knowledge management functionality in the portal.

19.1.1 Technical architecture

SAP EP is based on SAP Web AS J2EE. It is an SAP Application Server that combines with other software components for knowledge management, the Unification Server, and the Connector Framework, to form the SAP Enterprise Portal architecture.

The SAP EP architecture is illustrated in Figure 19.2. Its essential components are:

- **Portal server**
  The portal server contains the portal's runtime environment, the *portal runtime* (PRT), including the application information that is partially returned by the backend applications (for example, via XML) or other portal content, and which is prepared accordingly for the frontend (web browser) in the Page Builder. The various content is provided to the users in iViews. An iView is the smallest unit for dividing and structuring a portal page.

  Portal services comprise the services for managing the iView content. User management (definition of authorizations and roles) via the *User Management Engine* (UME) is significant as well. Another service manages the connections of the individual iViews to the backend applications via the Connector Framework.

  Other important services include those that provide the navigation service for the entire portal content, the caching service, the portal content handling service, the URL generation service (for example, via SAP Internet Transaction Server), and the Web service. The latter can be used to access the portal via Web services. In turn, it is also possible to call Web services. The *Portal Content Directory* (PCD) is used to manage the content, that is, all objects (for example, iViews, roles, content, applications, backend applications). PCD sets the portal roles and their accesses to the individual objects and defines the services that can be called.

- **Knowledge management**
  Knowledge management is an additional component that contains content management, that is, portal content management using administration tools

(for creating iViews, layouts, documents, etc.), and the TREX search and classification engine. TREX is the SAP search engine that creates an index across the entire portal content and can be used to search the portal content for keywords or logically related search terms. Users can then store the found documents and information in the portal for their personal knowledge management.

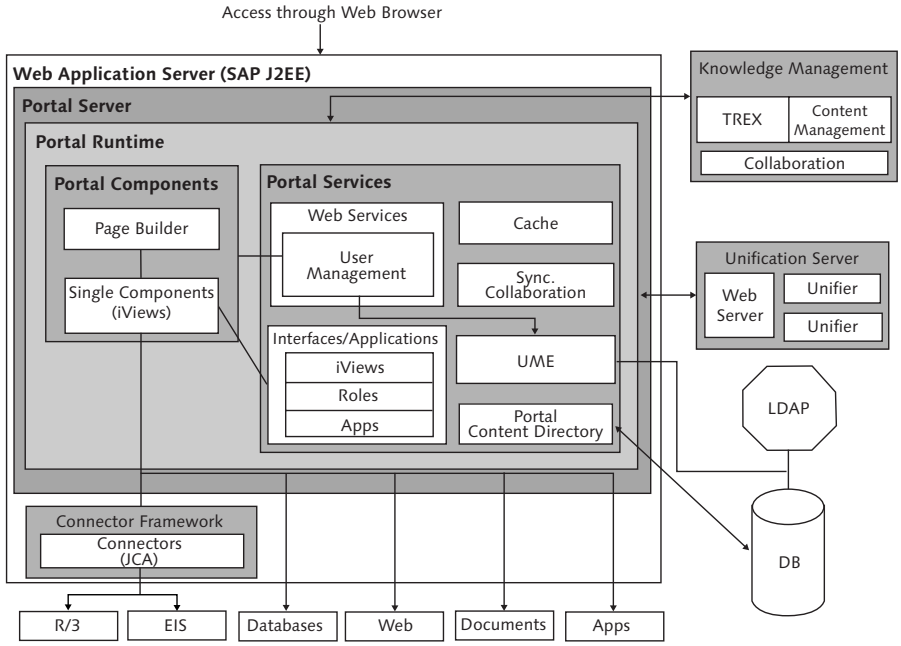


Figure 19.2 Logical and Technical Architecture of SAP EP

- **Unification Server**

  At the business object level, the Unification Server provides a *Drag&Relate functionality*. Using this functionality, the user can start a query across several applications and data sources. For example, the user can simply drag a name to an author query and will then receive replies for that name from all applications and data sources attached to the portal that are grouped in one view. All further existing information about a given object can be grouped in this way.

- **Connector Framework**

  The Connector Framework is based on the standardized *Java Connection Architecture* (JCA). This framework can be used to connect the applications running in the portal to other backend applications. Connectors for this purpose are already available (e.g., for R/3 backend applications, JDBC, etc.). Connectors can also be called via Web services and can be used to connect iViews to the

backend applications. The connectors provide an integration form that is independent of the respective backend application so that the programmer can focus entirely on developing the business logic.

19.1.2 Description of the User Management Engine

In the portal environment, it is crucial to have a basic understanding of the *User Management Engine* (UME), because this architecture service controls all management of users and their authorizations in SAP Enterprise Portal. More sophisticated knowledge of the UME is also important, because many of the technical controls explained are implemented using UME.

Figure 19.3 presents an overview of all architecture services provided by the UME. The central layer provides the *application programming interfaces* based on Java that are required by the SAP EP applications (e.g., Java-based iViews) to perform, for example, the authentication of a user or to maintain the related master data.

These programming interfaces are the following:

- **User API**
  Using the User API, a portal application can call authentication services for existing users and also validate their authorization.
- **User Account API**
  The User Account API enables the portal application to create new users, to maintain their master data, and to assign their portal roles, among other things. The User Account API is therefore implemented for management services and, unlike the User API, is not used at runtime.
- **Group API**
  The Group API can be used to create group definitions. Even at runtime, you can query if a user belongs to a specific group.
- **Role API**
  The Role API serves for managing the portal roles. It can also be used to assign the portal roles to the users.

The *Persistence Manager* controls the access to user data via the programming interfaces described above. The Persistence Manager performs the task of managing the available storage systems. As persistence storage, the portal database, an external LDAP directory, or SAP Web AS ABAP can be implemented.

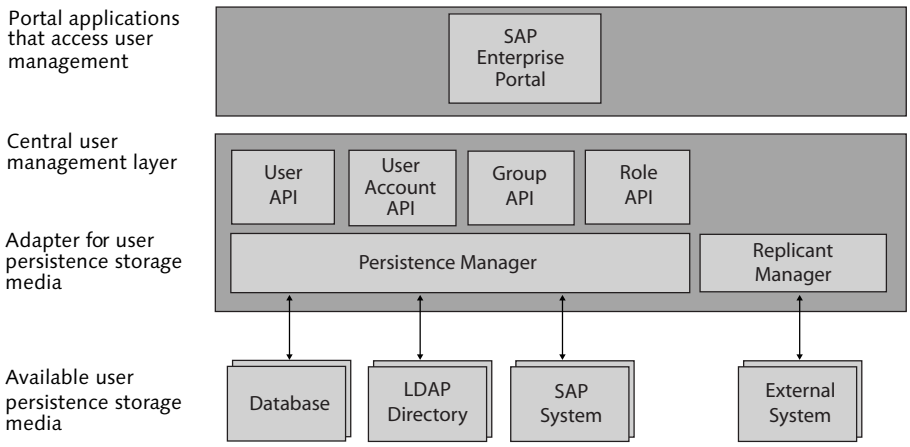


Figure 19.3 User Management Engine

The following formats can be used for the database:

- Oracle 9.2 or above
- Microsoft SQL Server 2000 or above
- IBM DB2/UDB

Possible LDAP directories are:

- Novell eDirectory
- Sun ONE Directory Server
- Microsoft Active Directory Server
- Siemens DirX

The following SAP system is required:

- SAP Web AS 6.20 or above

The Persistence Manager can manage several LDAP directories at a time. You therefore have the option to distribute users among the various storage systems connected to UME, which is particularly important when implementing SAP EP in Internet scenarios. For example, external users can be made persistent in the portal database, and internal users can be made persistent in an LDAP directory. It is also possible to make this division according to user attributes. For example, the assignment of the portal role to the user can be stored in the portal database, and the corresponding master data can be stored in the LDAP directory.

This distribution is controlled via an XML file, the *data source configuration file*, which can be set using the config tool. It is recommended to use one of the UME data source configuration files delivered by SAP. A customized file can be defined only if none of the specified files meets the requirements. The name of the data source configuration file is defined in the following UME property entry:

```
ume.persistence.data_source_configuration=
  dataSourceConfiguration_new.xml
```

The property is `ume.persistence.data_source_configuration`, which in this case is set to the file *dataSourceConfiguration_new.xml*.

Listing 19.1 shows an example of an XML file where regular users are stored in an LDAP directory (CORP_LDAP) and service users are stored in the portal database (PRIVATE_DATASOURCE).

```
<dataSource id="PRIVATE_DATASOURCE"
            className="com.sap.security.core.persistence.
              datasource.imp.DataBasePersistence"
            isReadonly="false"
            isPrimary="true">
    <homeFor>
        <principals>
            <principal type="USER">
<!--
COMMENT: If you set the triple attribute values ($service-
User$,SERVICEUSER_ATTRIBUTE,IS_SERVICEUSER) in a substructure
for the principals (not yet authorized user) of the type "USER"
in your name range, this rule is applied, and the service users
are stored in the PRIVATE_DATASOURCE portal database.
-->
                <nameSpace name="$serviceUser$">
                    <attribute name="SERVICEUSER_ATTRIBUTE">
                        <values>
                            <value>IS_SERVICEUSER</value>
                        </values>
                    </attribute>
                </nameSpace>
            </principal>
        </principals>
    </homeFor>
    <notHomeFor>
```

```
    </notHomeFor>
    ...
</dataSource>

<dataSource id="CORP_LDAP"
            className="com.sap.security.core.persistence.
              datasource.imp.LDAPPersistence"
            isReadonly="false"
            isPrimary="true">
    <homeFor>
        <principals>
            <principal type="USER">
<!--
COMMENT: If no substructure for specific principals of the type
"USER" is defined, except for the "notHomeFor" section, this rule
is applied to all other users. This means that all users except
for those with the service user attribute are stored in the CORP_
LDAP LDAP directory.
-->
            </principal>
        </principals>
    </homeFor>
    <notHomeFor>
        <principals>
            <principal type="USER">
<!--
COMMENT: As explained above, this rule applies if a substructure
exists for principals of the type "USER" and the Serviceuser
attribute.
-->
                <nameSpace name="$serviceUser$">
                    <attribute name="SERVICEUSER_ATTRIBUTE">
                        <values>
                            <value>IS_SERVICEUSER</value>
                        </values>
                    </attribute>
                </nameSpace>
            </principal>
        </principals>
```

```
    </notHomeFor>
    ...
</dataSource>
```

Listing 19.1 Example of the dataSourceConfiguration_new.xml File

The *Replication Manager* is responsible for providing a replication service via XML with additional external applications. Therefore legacy SAP systems like SAP R/3 4.6D up to SAP Web AS 6.10 can be supported, for example.

19.2 Risks and Controls

In this section, we will use a simplified version of the proposed risk analysis methodology described in Chapter 2 to identify the main security risks and the necessary controls (see Table 19.1). The controls are then discussed in more detail in the following sections and illustrated using examples.

No.	Classification	Description
1.	**Risk potential**	Authorization concept missing or faulty. Due to an inadequate assignment of rights, users gain access to information and applications in SAP Enterprise Portal for which they have no authorization.
	Impact	Due to their authorizations, users are able to view or even change confidential business documents. This enables them to perform fraudulent acts or other activities that jeopardize the business.
	Risk without control(s)	Extremely high
	Control(s)	Portal roles are predefined and assigned the corresponding authorizations. Portal roles enable users to access only specific applications and information.
	Risk with control(s)	Negligible
	Section	19.3.1
2.	**Risk potential**	No information ownership principle. Owners of business processes cannot determine or approve the assignment of portal roles that enable other employees to access their information and applications.

Table 19.1 Risks and Controls for SAP Enterprise Portal

No.	Classification	Description
	Impact	Central administrators assign portal roles and the associated authorizations for business process information without the approval of the business process owner. Because of this, authorization accumulations can occur, or the assigned authorizations can no longer be validated due to a lack of transparency. Users therefore gain access to information for which they are not authorized.
	Risk without control(s)	Extremely high
	Control(s)	A segregation of functions when assigning portal roles is achieved using the delegated administration by involving the information owner (usually the owner of the business process).
	Risk with control(s)	Negligible
	Section	19.3.2
3.	**Risk potential**	No holistic authorization concept between SAP EP and the backend. Users have incongruent roles in the portal and the corresponding backend applications, and therefore have either too little or too much authorization.
	Impact	Due to excessive authorization, users are able to access information or applications for which they are not authorized. Therefore, they have the possibility to manipulate information and to perform fraudulent activities. Additionally, it is likely that they cannot perform their tasks due to insufficient authorization and are therefore not productive.
	Risk without control(s)	High
	Control(s)	Portal roles are synchronized and reconciled with the respective backend applications. For this purpose, portal roles can be downloaded into the bakkend applications, or the roles can be uploaded to the portal. However, this only applies if the bakkend applications are SAP systems.
	Risk with control(s)	Negligible
	Section	19.3.3
4.	**Risk potential**	No approval process for portal content. There is no approval process when uploading and implementing new portal content if SAP EP is used in an Internet scenario.
	Impact	In an Internet scenario, incorrect portal content is published, which damages the organization's external presentation and reputation. Eventually, this may result in a loss of sales.

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Risk without control(s)	High
	Control(s)	An appropriate workflow needs to be established that ensures that portal content is checked before it is published.
	Risk with control(s)	Negligible
	Section	19.3.4
5.	**Risk potential**	No central user persistence storage location. Master data is stored in several different user persistence storage locations. In addition to this, there is no unified enterprise-wide employee identifier. Therefore, the master data storage concept contains redundancy, and the data is inconsistent.
	Impact	Inconsistent user master data causes a large amount of redundancy, not to mention a lack of transparency. Therefore, when changes need to be made (for example, if an employee leaves the enterprise), user accounts are not managed in an appropriate manner. The result may be the existence of user accounts with excessive authorizations, which could be exploited by other unauthorized users. There are also the additional administrative costs of maintaining redundant user accounts.
	Risk without control(s)	Extremely high
	Control(s)	Connect SAP Enterprise Portal to a central LDAP directory that contains the master data of all users in one central location. Alternatively, SAP EP can also be connected to an existing SAP backend system that is then used as the main user persistence storage location.
	Risk with control(s)	Negligible
	Section	19.4.1
6.	**Risk potential**	Passwords that are too numerous and too simple. Every backend application has its own password. Users need to memorize these different passwords, so they often choose simple or even structured passwords, like names of months. In the extreme case, passwords are jotted down somewhere near the desktop.
	Impact	An unauthorized user can easily take on another identity and gain more application rights to effect unauthorized and fraudulent transactions.
	Risk without control(s)	Extremely high

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Control(s)	Using SAP EP, a Single Sign-On mechanism is established based on SAP logon tickets. The user then only has one user name and one password for all applications connected to SAP Enterprise Portal. Additionally, there needs to be a regulation that passwords are not to be written down on notes close to the desktop.
	Risk with control(s)	Normal
	Section	19.4.2
7.	**Risk potential**	Passwords that are too numerous and too simple. Every backend application has its own password. Users need to memorize these different passwords, so they often choose simple or even structured passwords, like names of months. In the extreme case, passwords are jotted down somewhere near the desktop.
	Impact	An unauthorized internal user can easily take on another identity and gain more application rights to effect unauthorized and fraudulent transactions.
	Risk without control(s)	Extremely high
	Control(s)	Using SAP EP, a Single Sign-On mechanism is established based on an external authentication mechanism (Windows authentication) for the Windows system. Users then only need to log on to their Windows accounts on their desktops to access all applications connected to SAP EP.
	Risk with control(s)	Negligible
	Section	19.4.3
8.	**Risk potential**	Passwords that are too numerous and too simple. Every backend application has its own password. Users need to memorize these different passwords so they often choose simple or even structured passwords, like names of months. In the extreme case, passwords are jotted down somewhere near the desktop.
	Impact	An unauthorized internal user can easily take on another identity and gain more application rights to effect unauthorized and fraudulent transactions.
	Risk without control(s)	Extremely high
	Control(s)	Using SAP EP, a Single Sign-On mechanism is established based on person-related digital certificates for the individual users. Users are then always authenticated to the portal and its associated applications using their certificates.

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Risk with control(s)	Negligible
	Section	19.4.4
9.	**Risk potential**	Misconfigured anonymous access. The portal is misconfigured for anonymous access so that anonymous users can access confidential information.
	Impact	Anonymous users can view or manipulate information for which they are not authorized. Therefore, confidential information is released to the public, which can damage the company's reputation and even result in financial losses.
	Risk without control(s)	Extremely high
	Control(s)	Correct configuration of the portal for anonymous users.
	Risk with control(s)	Negligible
	Section	19.4.5
10.	**Risk potential**	Misconfigured portal. SAP EP has been misconfigured for the initial configuration.
	Impact	Due to a misconfiguration of SAP Enterprise Portal, a directory browsing of SAP EP might be enabled, for example. Unauthorized content, like exploits, can then be uploaded to SAP Enterprise Portal. Additionally, it might be possible to gain administrative rights.
	Risk without control(s)	Extremely high
	Control(s)	Adhere to SAP Note 606733, deactivating services that are not required.
	Risk with control(s)	Negligible
	Section	19.4.6
11.	**Risk potential**	Circumventing authentication and authorization mechanisms of SAP EP. SAP EP services can be accessed directly, circumventing authentication and authorization, by calling the appropriate service URL.
	Impact	By circumventing the authentication and authorization mechanism of SAP EP, confidential information can be viewed or manipulated.
	Risk without control(s)	Extremely high

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Control(s)	Set up security zones for SAP EP content so that it cannot be called directly by entering the URL.
	Risk with control(s)	Negligible
	Section	19.4.7
12.	**Risk potential**	No network strategy. At the network level, there is no sufficient security for the portal due to the fact that the network is not divided into trustworthy and untrustworthy areas using firewalls.
	Impact	If a firewall configuration is not used, the security of SAP Enterprise Portal at the network level is inadequate, and any weak points that there may be in the system can be exploited at the operating system level. This can allow system attackers to obtain administrator authorizations. The portal can therefore be compromised. The final result may be unauthorized manipulation of data or unauthorized execution of financial transactions.
	Risk without control(s)	Extremely high
	Control(s)	Secure the portal by securing the network. Divide the network segments into less protected areas and trustworthy zones. Do this by appropriately configuring and setting up network-based firewalls.
	Risk with control(s)	Negligible
	Section	19.4.8
13.	**Risk potential**	External attacks on the application. On the application side, the entries transferred from the client at the application level (e.g., URL parameters, form field entries, etc.), are not sufficiently checked. The following attacks can therefore be successful at application level: Stealth commanding: changing transfer parameters in order to obtain a different application status or to modify price information Cookie poisoning and token analysis: enables the hacker to carry out session hijacking Buffer overflow: enables a denial-of-service attack Cross-site scripting: enables the hacker to divert the user to a compromised site
	Impact	Because of inadequate checking of input parameters the application is compromised, and therefore unauthorized users can obtain advanced permissions at the application level. This also means that backend applications might be attacked and that data theft or modifications can take place.

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Risk without control(s)	Extremely high
	Control(s)	Transfer parameters and input fields have to be checked for plausibility and correctness on the server side. It is also recommended that you introduce an application-level firewall. This is particularly relevant for self-developed applications that are to be integrated into the portal.
	Risk with control(s)	Negligible
	Section	19.4.9
14.	**Risk potential**	Unencrypted access. The connection between the frontend (browser) and portal server is unencrypted. Further internal communication channels are unencrypted as well.
	Impact	If a Single Sign-On configuration was implemented in SAP EP by using SAP logon tickets, the session of another user can be copied by "sniffing" and adopting the cookie. Additionally, a *man-in-the-middle attack* is possible, where important business information is accessed by unauthorized persons and can be manipulated by them. Financial losses can be very high for the organization.
	Risk without control(s)	Extremely high
	Control(s)	The communication between frontend and SAP EP and other communication channels is encrypted via SSL.
	Risk with control(s)	Negligible
	Section	19.4.10
15.	**Risk potential**	No virus scan when uploading documents. When uploading documents or other attachments from the Internet to SAP EP, the attachments are not scanned for potential computer viruses or other exploits.
	Impact	An unidentified virus can spread through SAP EP to other systems of the organization and potentially compromise all IT systems of the organization. This can result in substantial damage to the organization due to downtime and recovery of the IT systems. There might also be legal consequences for the organization if the portal turns out to be a "cesspool of viruses."
	Risk without control(s)	Extremely high

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

No.	Classification	Description
	Control(s)	Implement an antivirus scan when uploading attachments to the document via knowledge management. The attachment will then be discarded if it contains potential viruses and will not be posted on the portal server. This scenario is particularly relevant for recruiting portals where attached résumé documents need to be scanned for existing computer viruses or macros.
	Risk with control(s)	Negligible
	Section	19.4.11

Table 19.1 Risks and Controls for SAP Enterprise Portal (cont.)

19.3 Application Security

19.3.1 Structure and Design of Portal Roles

Structure of Portal Roles

The structure of SAP portal roles is very different from ABAP-based roles that are traditionally used in most applications (e.g., FI, CO, MM, etc.) in the SAP environment. The main difference is that ABAP-based roles specifically define the access to transactions and also the authorization range of a role via authorization fields. For example, a role specifies that a user may start the "Create material" transaction and create materials for a specific company code. See Section 9.3 for more details on this matter.

Portal roles do not specify the access to individual transactions in an SAP system, but the access to individual objects that are available in a portal. Basically, these are the following objects:

- **iViews**
  An iView is an extract from the complete page of a portal. It can either present pure information or access to a specific functionality. An iView can also store the call of a backend application and link it directly to the start of a specific transaction in an SAP system. This is the main purpose of an iView. An iView is the smallest unit in SAP EP.
- **Worksets**
  A workset groups various iViews in a logical navigation structure according to the respective business aspect. This means that all iViews concerning "Controlling" are grouped in one workset. Therefore, a workset is a navigation structure below the portal role.

- **Pages**
  A portal page specifies the visual arrangement of different iViews; it defines the layout. A page can consist of one single iView. It can also be assigned to a workset.

The navigation structure at the highest level is the portal role. It comprises worksets that can, in turn, contain pages and iViews. This structure is shown in Figure 19.4.

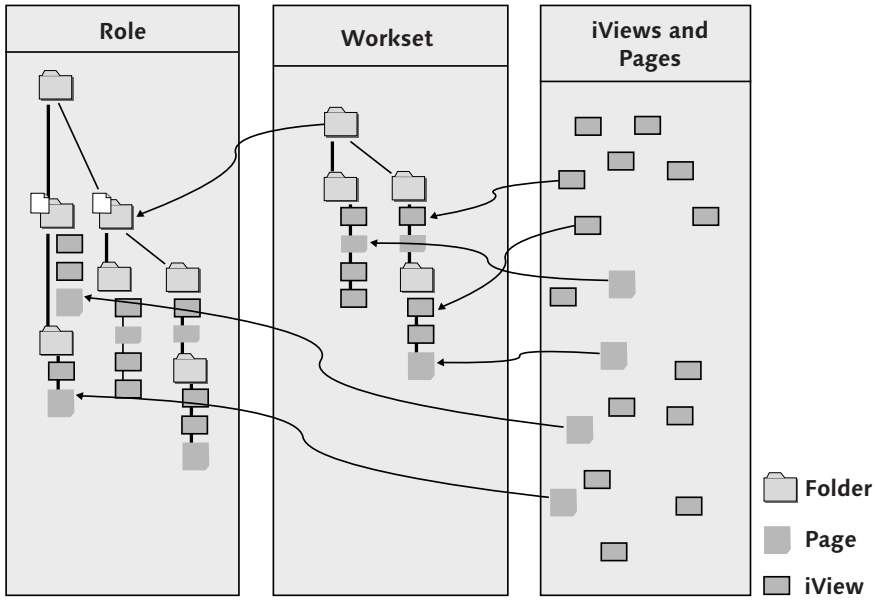


Figure 19.4 Portal Role Defines Navigation Structure in SAP Enterprise Portal

The example in Figure 19.5 shows the **Corporate Home** workset, which exists in the **Administrator** role. The first level of the navigation structure—in this case, the **Corporate Home** workset—always goes to the top portal navigation row of the mandatory and predefined top-level iView. The second level, **About Us** in this example, always defines the second portal navigation row of the predefined top-level iView. The third level goes to the detailed navigation iView. In this example, the pages **About Us** and **Corporate Index** are on the third level and contain more iViews.

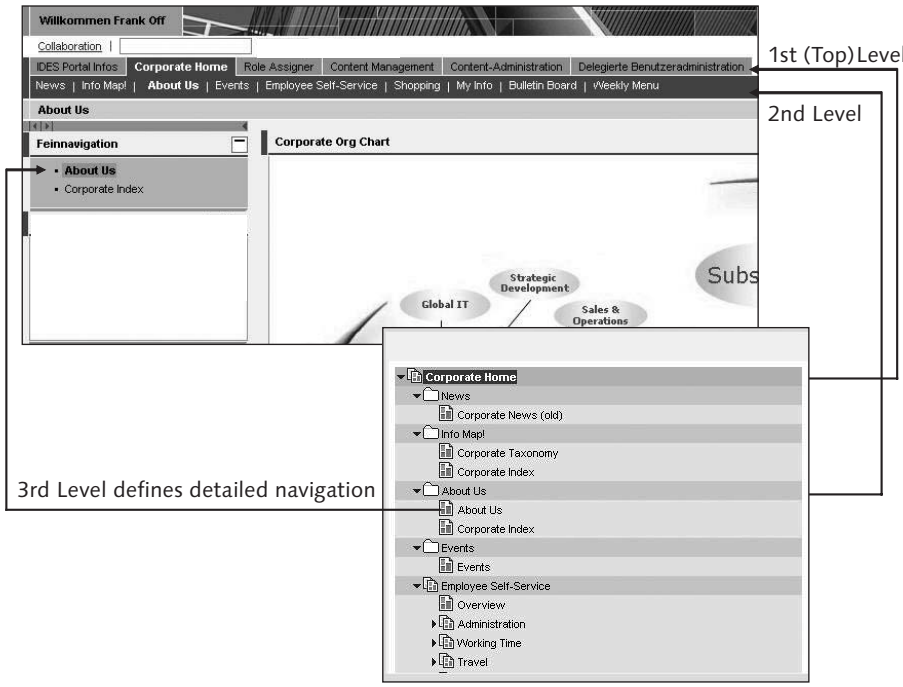


Figure 19.5 The Portal Role During Runtime ("Corporate Home" Workset)

In summary, portal roles can be described as follows:

- A portal role defines a collective folder for several worksets, pages, and iViews that are to be accessed by the role.
- Portal roles are grouped according to the individual job roles of the positions existing in the enterprise.
- A portal role defines the technical navigation structure of a user in SAP Enterprise Portal. The entire navigation structure of a user is defined by the sum of all portal roles assigned to it.
- Portal roles can be directly assigned to individual users or user groups.

Technically, the roles are administered in the *Portal Content Directory* (PCD) that is located in the **Content Administration** workset. Using the Role Editor, the roles can be defined in a dedicated directory within a content area. Figure 19.6 shows the **Standard User with Hometab** sample portal role. This portal role contains the **Home** workset, which includes various iViews like the **Outlook Web Access** and **Universal Worklist** application calls. The **Home** workset also contains other worksets, such as **Shopping** and **Employee Self-Service,** which are shown on the second top-level navigation when the role is executed.

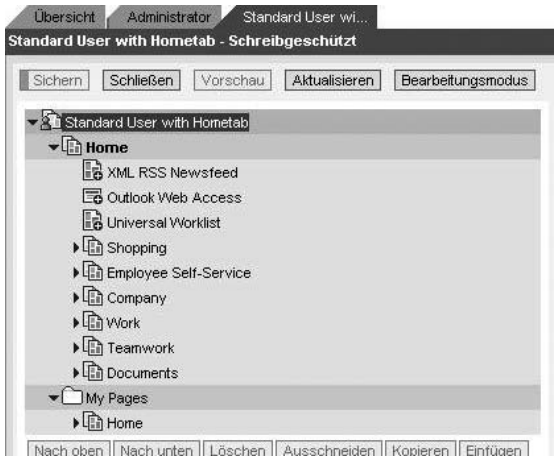


Figure 19.6 Sample Portal Role ("Standard User with Hometab")

These objects can be administered using the Role Editor, and the hierarchy of the worksets, pages, and so on can be changed. For example, if more iViews or pages are to be added to the role, you need to navigate to this object in the PCD and right-click to select **Add to Role**. You can then insert the new object as a delta link or as a copy. The delta link has the advantage that changes to the original object, for example, the added iView, are propagated to the portal role; the object properties can be inherited accordingly. If you want to prevent this, you can also dissolve inheritances. The Role Editor can also be used to edit Access Control Lists (ACLs) and other properties. Additionally, you can define worksets of the second level as an entry point so that they are displayed in the first row of the top-level navigation.

Authorizations for Portal Roles

An important difference between ABAP roles and portal roles is that in the portal, no authorizations are defined for the backend application itself. This must still be done within the backend applications (for example, mySAP ERP).

In the portal, however, access to the individual objects (portal roles, worksets, pages, iViews) is defined via ACLs. There are three authorizations for the objects:

- **Administrator**
  This authorization controls the administration of the portal objects at administration time.
- **End User**
  This authorization controls the call of an object at runtime if the object is executed in the runtime environment of SAP EP. This does not apply, for example,

if the iView starts a transaction on a backend application, because in this case, only a redirect takes place.

- **Role Assigner**
  This authorization controls the right to assign a portal role to another user. It therefore only exists for objects of the portal role type and for PCD directories that pass the authorizations on to the objects contained therein.

For the ACL administrator, there are six authorization levels for administering the objects, which are listed in Table 19.2.

	Description		
ACL definition	**Create**	**Delete**	**Edit**
None	The directory of the objects and the objects themselves are not visible in the PCD. This setting only makes sense for pure runtime roles for which the end-user right must be activated.	The directory of the objects and the objects themselves are not visible in the PCD.	The directory of the objects and the objects themselves are not visible in the PCD.
Read	The directory of the objects and the objects themselves are visible in the PCD. New objects can be created as an instance of an existing object, as a delta link.	The directory of the objects and the objects themselves are visible in the PCD. Objects cannot be deleted.	The directory of the objects and the objects themselves are visible in the PCD. Objects cannot be edited.
Write	This ACL selection only applies to directories in the PCD and not to objects. A role that has write authorization for a directory can create new objects in that directory.	This ACL selection only applies to directories in the PCD and not to objects. Objects cannot be deleted, but directories can.	This ACL selection only applies to directories in the PCD and not to objects. Objects cannot be edited.
Read/write	The directory of the objects and the objects themselves are visible in the PCD. New objects can be created as an instance of an existing object, as a delta link.	The directory of the objects and the objects themselves are visible in the PCD. Only the newly created inferior objects of an existing superior object can be deleted.	The directory of the objects and the objects themselves are visible in the PCD. Only object properties and delta links[1] can be edited.

Table 19.2 ACL Definition "Administrator" for the Design Phase of Portal Objects

1 New objects that are created on the basis of template objects are only derived from the original. This derivation is referred to as a delta link.

	Description		
ACL definition	**Create**	**Delete**	**Edit**
Full access	The directory of the objects and the objects themselves are visible in the PCD. New objects can be created as an instance of an existing object, as a delta link.	The directory of the objects and the objects themselves are visible in the PCD. All objects can be deleted.	The directory of the objects and the objects themselves are visible in the PCD. Only object properties and delta links can be edited.
Owner	The directory of the objects and the objects themselves are visible in the PCD. New objects can be created at any time.	The directory of the objects and the objects themselves are visible in the PDC. All objects can be deleted.	The directory of the objects and the objects themselves are visible in the PCD. All object properties, including authorizations, can be edited.

Table 19.2 ACL Definition "Administrator" for the Design Phase of Portal Objects (cont.)

At runtime, only the **End User** ACL is checked. It can take on two values: possible or not possible. At runtime, when the user is logged on to the portal, the portal object contained in the portal role can be displayed accordingly. For customizing the layout, the user can only use those objects that have an authorization specified in the **End User** ACL. Direct access to the portal object via the web browser URL is possible only if the **End User** ACL has been set for the security zone as well (see Section 19.4). However, the iView execution restriction using the ACL only works if the called application is executed in the runtime environment of SAP EP and if it is therefore a Java application. For iViews only starting a backend application, this access protection does not work. For this purpose, the authorizations in the backend application must be set properly.

The **Role Assigner** ACL only exists for the portal role object or can only be defined for PCD directories that pass their authorizations on to the portal roles contained therein via inheritance. The **Role Assigner** ACL can also take on only two values: set or not set. A role possessing this ACL is authorized to assign this role to other users. This means that delegated user management is feasible.

Figure 19.7 summarizes the relationship of portal roles, their assignment to users or user groups, and the (still necessary) specification of authorizations in the backend applications (SAP Web AS ABAP authorizations).

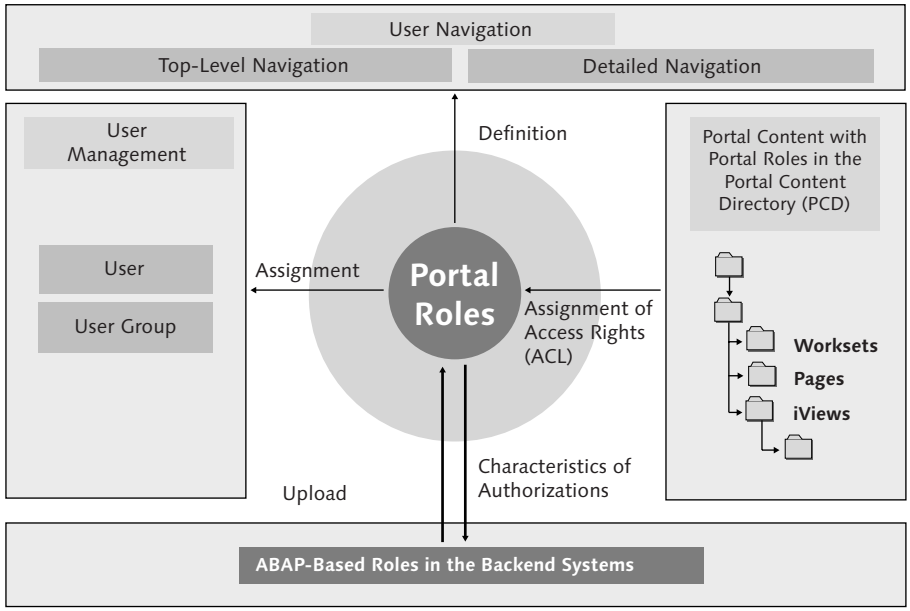


Figure 19.7 Relationship Between Portal Roles and Authorizations in the Backend Applications

In the *Portal Content Directory* (PCD), the portal roles are defined with the existing navigation structures via the workset, page, and iView portal objects. For access control, there are three Access Control Lists for every object for the design phase and for runtime. Within the backend applications, the authorizations are still specified if an iView calls a backend application, for example, from mySAP ERP. You have the option to upload roles from the backend applications and vice versa. The sum of all portal roles assigned to a user defines the user's complete navigation structure.

19.3.2 Delegated User Administration for Portal Roles by Involving the Information Owners

SAP Enterprise Portal is delivered with standard roles that enable delegation, or better distribution, of tasks. Task distribution can be observed in the areas of system, content, and user administration. For this purpose, SAP provides the **Superadministrator**, **Content Administrator**, **System Administrator**, and **User Administrator** standard portal roles. Table 19.3 provides an overview of these portal roles.

Portal role	Description
Superadministrator	This portal role is assigned to the initial "SAP*" user and enables the following: ▶ Full access, including all rights for all objects in the Portal Content Directory ▶ Full access to all tools of the content, system, and user administrators
Content Administrator	This portal role enables access to the following portal tools and content: ▶ Content administration (maintenance of portal content), including the option to define portal roles, worksets, pages, and iViews ▶ Editors for maintaining portal content, such as the Permissions Editor (maintenance of authorizations, ACLs) and Property Editor (maintenance of object properties) ▶ All directories of the PCD if the ACLs have been defined accordingly
System Administrator	This portal role enables access to the following portal tools and content: ▶ System administration, such as system configurator, transports, authorizations, monitoring, support, and portal display ▶ All directories of the PCD if the ACLs have been defined accordingly
User Administrator	This portal role enables access to the following portal tools and content: ▶ All user management tools for creating new users, assigning roles to the users, administering the *user mapping* (mapping of the portal user name to potentially deviating user IDs in backend applications), user replication with external directories, group administration, and more

Table 19.3 Standard Administration Roles

Standard administration roles can be fine-tuned using authorization control and can therefore be adapted to specific requirements. The significant segregation of functions for defining and assigning portal roles can be achieved in this way.

In terms of the information ownership principle that has been introduced for the management of ABAP roles and ABAP users already, the portal environment provides the option of delegated user administration. It can be set up so that there is still one ultimately responsible user administrator who has the authorization to perform all user management, but who is supported by delegated user administrators.

These delegated user administrators can be specified so that they are only authorized to issue the assignment of users from one subsidiary or department to a portal role. The delegated user administrators need to belong to the same subsidiary or department.

The following technical steps must be carried out to establish delegated user administration for the portal:

1. Define the necessary subsidiaries or departments to which the users can belong. This is done in the config tool for the J2EE Engine underlying the portal. For this purpose, the following entry must be added to the `sapum.properties` property (for example, with the sales, marketing, and development departments):

   ```
   ume.tpd.companies=Sales,Marketing,Development
   ```

   Alternatively, you can import a list of subsidiaries and departments from a partner directory on a backend system into the portal. This option is not discussed here in detail because it depends on the type of directory and on the backend system itself.
2. Set the `Check ACL` parameter for the `com.sap.portal.roleAssignment` iView to **True**.
3. Determine one or several delegated user administrators per company, department, and so on. The user administrator in charge does this by assigning the following portal role to these administrators: **Delegated User Admin**, which can be found in the following PCD directory: *pcd:portal_content/administrator/user_admin/delegated_user_admin_role*.
4. Assign the portal users to a company, department, and so on using the `Org_ID` attribute. This can be done by the user administrator in charge. The following possibilities are available:
   - Use the user administration tool in the portal
   - Use the import function in the portal for inviting users from a directory or a file, and so forth. In this case, the `Org_ID` needs to be defined.

As soon as these steps have been completed, the delegated user administrator can create new users for the respective subsidiary or department and assign portal roles for which the **Role Assigner** authorization has been set.

The delegated user administration can be associated with the self-registration of users with the portal. If a user is to be admitted during the self-registration as a proper portal user by the user administrator responsible for a specific subsidiary, the following parameter must be defined for the portal in the config tool:

```
ume.logon.selfreg=TRUE
ume.admin.selfreg_company=TRUE
```

Additionally, all admissible subsidiaries or departments must be defined. If this is the case, the delegated user administrator receives a notification about the admittance of the user if the user specified his or her company during the registration process. If this is not the case, the self-registered user retains his or her guest status.

Please note that the term "company" can also be interpreted so that this concept is built according to your own organizational structure, and the responsibility of approval can be delegated to the individual departments. Unfortunately, true information ownership is not feasible because the administration of portal roles cannot yet be assigned to the individual subsidiaries or departments.

19.3.3 Synchronization of Portal Roles with the ABAP Roles of SAP Backend Applications

Portal roles and ABAP roles in the SAP backend applications can be synchronized. For this purpose, SAP EP allows you to upload ABAP roles or to import portal roles into the backend applications. However, only the relevant transactions and MiniApps can be uploaded, but not the actual ABAP authorizations that are defined in the authorization objects and profiles. Still, these options are very important, particularly in an SAP application environment, because SAP EP is becoming increasingly important as a central component, but it must be synchronized with the backend applications. For this reason, both possibilities should be considered.

Uploading ABAP Roles in SAP Enterprise Portal

In the first step, let's look at how ABAP roles are uploaded from the SAP backend applications. The following conversion rules are applied:

- Simple ABAP roles are migrated as portal roles (or as worksets) to the portal. Simple ABAP roles are stored in the Portal Content Directory as portal roles or worksets using the corresponding menu path.
- Composite ABAP roles are created either as portal roles or as worksets in the PCD using the corresponding menu path. The simple ABAP roles contained in the composite role are migrated as well. The menus of the simple ABAP roles are integrated in the main menu of the migrated composite role.
- MiniApps are migrated as iViews.
- In addition to the migration of ABAP roles, all services containing simple roles and composite roles (e.g., transactions, MiniApps, URLs) are migrated as well. This means that all transactions, MiniApps, URLs, and so on that were contained

in the "old" ABAP role are available as portal content objects after migration and can be assigned to more portal roles. The transactions contained in the ABAP roles are automatically migrated to iViews that include the transaction call via the default SAP GUI (either SAP GUI for Windows, SAP GUI for Java, or SAP GUI for HTML). These are stored in the PCD under the *Migrated Content* path.

- Even the existing assignment of roles to the users in the backend applications can be migrated. However, this only works if the users exist under the same user ID in both the portal and the backend application.
- The authorizations existing in the backend applications due to authorization objects and profiles are not migrated. Eventually, this means that the authorizations for the backend applications cannot be specified via SAP EP. Therefore, this specification of authorizations must remain within the respective backend applications.
- Derived ABAP roles are not migrated, because they do not differ from the template ABAP roles with regard to their functions, and authorizations are not migrated.

Figure 19.8 summarizes the migration of an ABAP role to a portal role during the upload process.

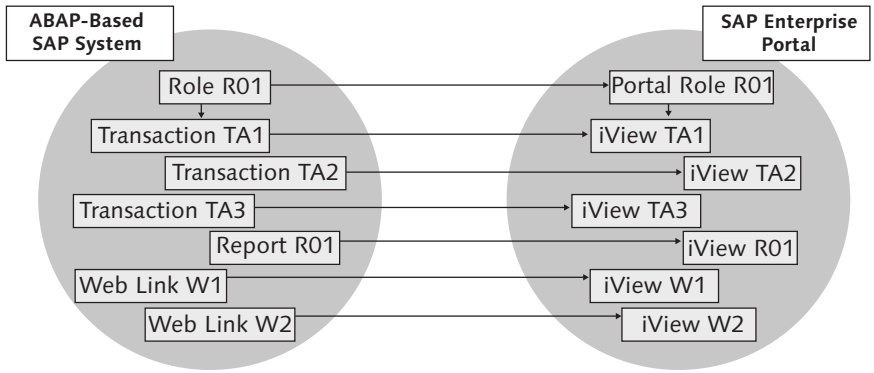


Figure 19.8 Migration of ABAP Roles to SAP EP

However, the following restrictions or notes need to be considered for this functionality:

- Simple ABAP roles and composite roles do not have pages that define the layout of the arrangement of the migrated iViews. These pages must be created (e.g., using templates) and assigned to the migrated portal roles. However, this is not mandatory but simply improves the layout.

- The role hierarchy and navigation structure must be adapted. The role menus of the migrated ABAP roles correspond to the menus of an ABAP-based SAP backend application that normally has a deep navigation structure with many hierarchical levels. Therefore, removing superfluous navigation levels is recommended.
- The top navigation level needs to be validated as well because it often contains 10 or more entries. A one-to-one migration would mean that in the portal, the first navigation row in the top-level iView (in the portal header) would be overloaded.
- Often you need to consider whether it is more advantageous to migrate ABAP roles to worksets and not directly to portal roles, which, in turn, can be combined more easily to design self-developed portal roles.
- It is also often recommendable to only migrate single services, like a transaction, for example, instead of a complete (often complex) role. Transactions, and thus iViews, can therefore be grouped in a simpler and more structured way to form new portal roles.

Here is a short description of the uploading procedure:

1. The functionality for uploading the ABAP roles from a backend application can be found in SAP EP under the following menu path: **System Administration · Transport · Upload Roles**
2. In this menu, you need to select a backend application. After selection, a list of available ABAP roles that can be uploaded is displayed. After completing this selection, you can choose the following options in the next screen:
   - **Upload user mapping**
     If this option is set, the assignment of the ABAP roles to the users is also uploaded apart from the ABAP roles themselves. This option only works if the user IDs in the portal and in the backend application are identical. This can be achieved by selecting the ABAP backend application as the user persistence storage location for the portal.
   - **Upload included services**
     If this option is set, not only the role structure is uploaded, but also the transactions, URLs, and so on contained therein. These are created as new objects in the PCD.
   - **Select first folder level as entry point**
     If this option is set, all top navigation levels of an ABAP role structure are specified in the portal role as entry points in the portal main navigation row. However, you need to be careful because the top portal navigation row can quickly be overloaded. This option should therefore not be set.

- **Convert roles to worksets**
  If this option is set, ABAP roles are not directly converted to portal roles, but rather to worksets. These worksets can then be further processed at a later stage and grouped to form a customized portal role.

3. After selecting these options, you can start the procedure via the **Upload** button. After uploading, the migrated portal roles can be further processed in the PCD like any other portal role. The roles are stored in the following PCD directory: **Portal Content · Migrated Content · SAP Component System · Roles · Systems** (system ID plus client of the SAP backend application). The name of the portal role contains the role description of the SAP backend application.

After the upload of the ABAP roles has been completed, the roles can be supplemented with existing predefined SAP business packages. If the uploaded ABAP roles are integrated as delta links into the existing portal roles of the business packages, these are renewed automatically when the ABAP roles are uploaded again at a later stage. This enables consistent portal role maintenance between SAP EP and backend applications.

Possibility of Distributing Portal Roles in the SAP Backend Applications

In addition to uploading existing ABAP roles to SAP EP, you also have the option of distributing portal roles to the associated SAP backend applications. When distributing portal roles to the backend applications, the following must be considered:

- During the distribution, only those iViews that contain transactions, MiniApps, and non-transactional services are taken into account. All other objects, such as documents or links, are not distributed. Non-transactional services include iViews that call backend applications using BAPIs and that can display the results of these backend applications in SAP EP.
- Additionally, the assignments of users to portal roles are optionally distributed to the backend applications as well. In contrast to the uploading functionality, however, only those users that do not exist in the backend applications are newly created. Still, you should take care that the user IDs in SAP EP and in the backend application are the same. If this is not the case, the SAP EP user mapping functionality must be used. Additionally, the user assignment to roles must be adjusted manually using Transaction WP3R.

The role distribution to the backend applications is illustrated once more in Figure 19.9. In this example, Transactions T1, T2, and T6, which are called in the "System 1" backend application via the appropriate iViews, are distributed to the backend

application as the ABAP role **A_1**. Using Transaction WP3R, this ABAP role can then be processed, and the authorization objects can be specified accordingly. This ABAP role **A_1** can also be copied to ABAP role **A_2**. This role can then be defined with different authorization values. The assignment of ABAP roles to the users can also be performed using Transaction WP3R. The same applies to Transactions T3, T4, T5, or, respectively, to iViews C, D, and E.

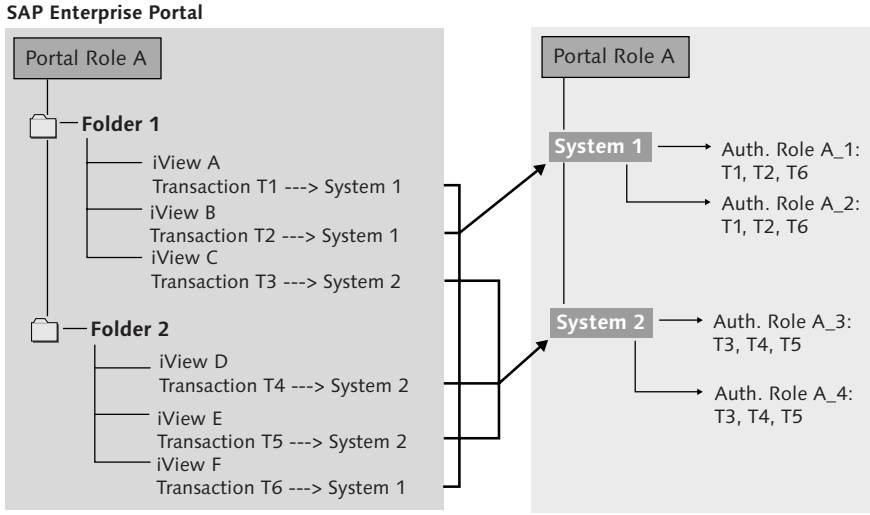


Figure 19.9 Distribution of iViews to the Corresponding SAP Backend Applications

As mentioned above, the ABAP roles can be implemented in the ABAP authorizations using Transaction WP3R after the portal roles have been distributed to the backend applications. Transaction PFCG cannot be used for this purpose.

These maintenance steps should be regarded in more detail:

1. In the first step, the desired portal roles need to be distributed to the corresponding backend applications. For this purpose, you need to navigate to the application **System Administration · Permissions · SAP Authorizations** in SAP EP. There you will find the portal roles that can be distributed. The roles to be distributed are simply selected.
2. In the next step, you need to select the target system to which the roles are to be distributed. As shown in Figure 19.9, only those iViews or transactions, respectively, are distributed from the portal role to the relevant backend application that can be executed there.
3. In the next step, the portal roles with the appropriate name are distributed to the backend application.

4. In the backend system, the authorizations for the ported portal roles can now be maintained using Transaction WP3R. At first, the migrated portal roles themselves need to be maintained. In the initial screen, you need to select the first option, **Maintain authorization roles,** with the corresponding ported portal role.
5. In the next step, the authorizations can be specified as shown in Figure 19.10.

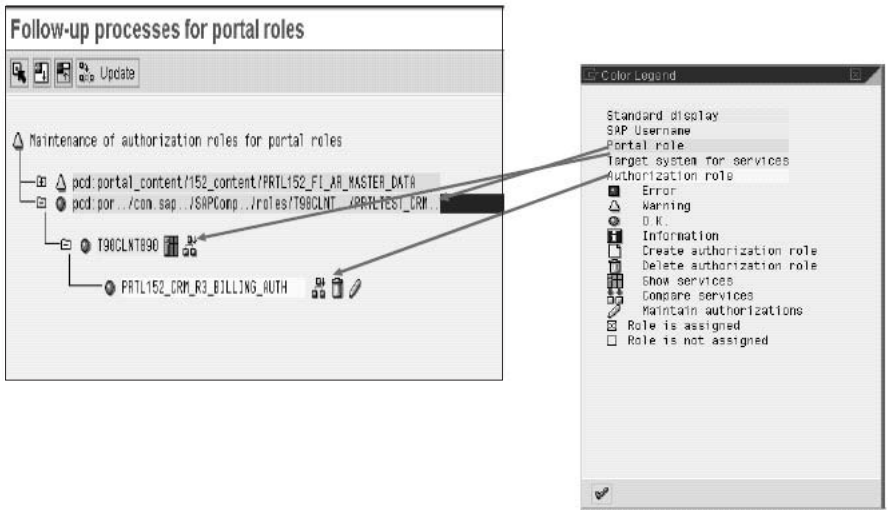


Figure 19.10 Maintenance of Authorizations of Distributed Portal Roles Using Transaction WP3R

6. To be able to assign the distributed ABAP roles to the users, this assignment must once again be distributed in the portal. For this purpose, navigate to **System Administration · Permissions · SAP Authorizations** and go to the **Transfer User Assignment** tab. For portal roles that have already been distributed, you can distribute the respective assignment of users to the backend applications as well.
7. After distributing the users to the backend applications, the second option in Transaction WP3R, **Assign authorization roles to users,** needs to be selected. With this option, the distributed portal roles can be assigned to the selected user.

Selection of the Primary System: SAP EP or Backend Applications

For synchronizing the business roles between SAP EP and the backend applications, you must select a primary system. In this regard, you should consider the following aspects:

- If SAP EP is exclusively used for managing documents or other company-internal content, and if the portal roles for calling the backend applications are rather simple, you should use SAP EP as the primary role design system. However, make sure that the ABAP authorization structure does not need to be specified in a very complex manner with many company codes, plants, and so on, because in that case, the maintenance effort using Transaction WP3R would be very high.
- If the access to backend applications is managed primarily by using SAP EP, you should use the backend applications as primary systems. The roles should be built and managed there and transferred to SAP EP via the uploading functionality.

Assuming that we have a common business scenario, where SAP EP is primarily used as a standard entry platform for the backend applications, we recommend that you continue to use the respective backend applications as primary systems for managing the roles. This solution is much better, because the information ownership principle demanded by the Sarbanes-Oxley Act (SOX) can be implemented best by using currently existing external tools, especially SecurInfo for SAP.

19.3.4 Change Management Process for New Portal Content

For SAP EP, several tools, such as the GUI Machine or the Portal Development Kit, can be used to create new content and store it in the PCD. This content might also be created directly in the PCD using the *iView Wizard*. In any case, however, you need to ensure that an appropriate change management process is implemented, as it is required for changes to traditional SAP systems as well.

For this purpose, SAP EP also provides a transport management system that can be used to transport packages from portal objects. Therefore, a three-system landscape with a development (DEV), quality assurance (QA), and production system (PROD) should exist in SAP EP. The development of the new content must take place on the development system and must then be tested on the quality assurance system by key users of strategic business units. On approval, the new content can then be imported into the production environment.

The following principles and best practices should be considered during portal content change management:

- Changes to objects on the development system should always be made to the originals and not to copies, because existing changes would otherwise be overwritten again during a succeeding transport.

- The development system carries out a transport to a common transport directory, from where the quality assurance and production systems then import its changes.
- Transport packages for the developers must be created at an early stage so that they are able to gradually integrate their modified or newly created objects during the project.
- The developers of new portal content must be responsible for the content they created. They also must confirm when they have placed their content in the provided transport packages.
- The business process owners must be involved in the approval of the new portal content. They must check this content to make sure it functions properly and is textually correct. Additionally, they must give their final approval for import to the production system.
- When finalizing the transport packages, dependencies among objects must be considered. This is important if inheritances are to be transported as well. For this purpose, a multi-package approach should be chosen where the object content, portal structures, and applications are separately exported and imported.

  The following transport packages should be created:

  - **Content transport package**
    This package contains iViews and pages with dependent objects.
  - **Structure transport package**
    This package contains pages, worksets, and portal roles without dependent objects.
  - **Application transport package**
    This package contains new application elements (PAR files) that include new portal components and services.
- When importing multi-packages, application packages need to be imported first, then the structure packages, and finally the content transport packages.

The transport manager is available in SAP EP under the following path: **System Administration · Transport**. Here you will find the **Export** and **Import** functions. In export mode, the objects can be selected in the PCD that are to be added to a defined transport package. For this purpose, right-click the appropriate object and select **Add to transport package**.

The transport mechanism is only available to the content administrator to whom the **Content Administrator** portal role was assigned. This role is a standard role delivered by SAP.

Index

D

E

F

S