SAP CRM AUTHORIZATIONS

Concepts and examples
**About the Author:**

Davy Pelssers his background includes Applied Economics, which he studied at the University L.U.C. in Diepenbeek, Belgium.

His experience with SAP began right after he started working as SAP Consultant for his first company in the year 2000.

During his career he has worked for CSC Belgium ([www.csc.com](http://www.csc.com)) and Cernum ([www.cernum.com](http://www.cernum.com)) in the role of SAP Consultant.

Working with SAP, he has worked in different modules and areas such as:
- SAP Authorizations
- SAP BW (Business Warehouse)
- SAP CRM (Customer Relationship Management)
- SAP IS-U (Industry Solution for Utility Companies)

As of April 2006 he started his own legal company DASAP Consulting BVBA in Belgium, where he now is working as a freelancer ([www.dasap.be](http://www.dasap.be)).

The past 6 years he is focusing on the SAP CRM module.

Contact details:
Davy Pelssers
Email: davy.pelssers@contactoffice.net

**ATTENTION:**

All the money you spent by donating will 100% be transferred for medical or educational purposes in those countries that are far worse off then the readers of this book probably are. In most cases everyone in contact with SAP (and therefore being a potential reader) is either working as consultant, or working internally at a large national or international company. This implies that most of you have a decent and nice job and might be willing to donate a small amount of money for a good cause.

On my personal website [www.dasap.be](http://www.dasap.be) you will be able to make a contribution. I will also further update the knowledge base section. Please visit the section about “Charity Projects”.

© 2007  Contact Author:  davy.pelssers@contactoffice.net
1. Introduction

2. SAP Authorization Concept
   2.1. Authorization Components and their Relationships
   2.2. The Profile Generator (PFCG)
      2.2.1. Installing the Profile Generator
      2.2.2. Creation of a new Role
      2.2.3. Single Role versus Composite Role (collective role)
      2.2.4. Master role and Derived Role
      2.2.5. Assigning Users
      2.2.6. Transporting Roles
   2.3. Organizing Authorization Administration
      2.3.1. Creating administrator roles
      2.3.2. List of available templates
      2.3.3. Authorization Objects checked in role maintenance
      2.3.4. Relevant SAP Tables for Authorizations and Roles
      2.3.5. System Settings-profile parameters
      2.3.6. Protective measures for Special profiles SAP_ALL & SAP_NEW
   2.4. Authorization Checks
      2.4.1. Checking at program level with AUTHORITY-CHECK
      2.4.2. Starting SAP Transactions
      2.4.3. Starting Report Classes
      2.4.4. Calling RFC Function Modules
      2.4.5. Checking assignment of Authorization Groups to Tables
   2.5. Analyzing Authorization Checks
      2.5.1. System Trace
      2.5.2. Authorization error Analysis
   3. Testing the roles
   4. User Maintenance
      4.1. Creation of a User in the CRM system
         4.1.1. Display user information
         4.1.2. Initial Data load for Users and Authorizations
      4.2. Creation of a User in the SAP Enterprise Portal
      4.3. Creation of an Employee in the CRM system
      4.4. Maintaining the Organizational Model
   5. CRM specific Authorizations
      5.1. Marketing and Campaign Management
         5.1.1. Role for creating marketing plan and campaign
         5.1.2. Restrictions made based on person responsible
         5.1.3. Restrictions made based on Authorization Group
         5.1.4. Restrictions made based on the Campaign Type
         5.1.5. Set Restrictions for assigning Attribute Sets and Attributes
      5.2. Business Partner Security
         5.2.1. Functional insight into Account and Contact Management
         5.2.2. General role SAP_CRM_BUSINES_PARTNER

© 2007  Contact Author: davy.pelssers@contactoffice.net
5.2.3. Restrictions for certain input fields based on Authorization Type ............. 146
5.2.4. Restrictions for certain field groups ......................................................... 149
5.2.5. Restrictions based on Authorization Group ............................................. 152
5.2.6. Restrictions for maintaining certain Business Partner Roles .................. 154
5.2.7. Perform authorization checks for sales area related data for business partners. ................................................................. 160
5.2.8. Restriction of business partner role in the BP transaction ..................... 160
5.3. Product Security ......................................................................................... 162
  5.3.1. Relevant SAP Authorization objects ....................................................... 162
  5.3.2. Product maintenance ............................................................................. 163
  5.3.3. Product Proposals .................................................................................. 168
5.4. Authorization check in Business Transactions .......................................... 169
  5.4.1. Relationship Business Transactions, Types and Categories ................... 169
  5.4.2. Process flow authorization check ........................................................... 182
  5.4.3. Examples of the authorization assignment .............................................. 185
  5.4.5 Authorization Check at Field Level ......................................................... 188
  5.4.6. Business add-in for authorization check in business transactions ........ 191
5.5. Authorizations in E-commerce (Internet Sales) ........................................... 191
  5.5.1. Customizing settings for Internet Sales .................................................... 191
  5.5.2. User Administration .............................................................................. 195
5.6. Interaction Center Winclient ....................................................................... 210
  5.6.1. Technical System Landscape ................................................................. 210
  5.6.2. User Administration and authentication .................................................. 211
  5.6.3. Users Overview ...................................................................................... 211
  5.6.4. Data synchronization between CRM system and other systems ........... 212
  5.6.5. Authorizations ....................................................................................... 212
5.7. CRM IC Webclient ...................................................................................... 213
  5.7.1. Customizing of the IC Webclient ............................................................ 214
  5.7.2. Assignment of the IC Webclient Profile .................................................. 216
  5.7.3. How to launch the IC Webclient .............................................................. 218
  5.7.4. Useful Parameters .................................................................................. 219
  5.7.5. Useful information about the IC Webclient ............................................. 220
5.8. ACE (Access Control Engine) ..................................................................... 222
  5.8.1. Introduction ............................................................................................ 222
6. BW specific authorizations (TO BE ELABORATED) ....................................... 223
7. Frequently Asked Questions .......................................................................... 223
8. Tips and Tricks ............................................................................................... 224
9. Relevant OSS notes regarding SAP Authorizations ....................................... 225
  9.1. SAP CRM related ...................................................................................... 225
APPENDIX .......................................................................................................... 227
© 2007 by Pelssers Davy. All rights reserved.

No part of this e-book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system without written permission of the author.

SAP, R/3, SAP CRM, SAP BW, ABAP/4 are either registered trademarks or trademarks of SAP Aktiengesellschaft, Systems, Applications and Products in Data Processing, Neurottstrasse 16, 69190 Walldorf, Germany. SAP AG is not the publisher of this book and is not responsible for it under any aspect of press law.

Information contained in this book has been obtained by doing a lot of research on help.sap.com, following the most common standard SAP Courses, by reading SAP Press books, but most important by combining the authors’ functional knowledge of R/3, SAP CRM, SAP BW and his understanding of the SAP Authorization concept.

The publisher does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information. Readers should be particularly aware of the fact that the product SAP is a continuously changing entity. Some facts may have changed since the writing of the e-book.

The book is a private initiative of the author and is started as a personal SAP CRM security bible in order to keep all relevant experience he obtained during his SAP consultant career into one central document. Due to the lack of a good specific SAP CRM security guide, SAP Course or centralized information about this topic at the time of writing, the author decided to make this book publicly available for sale. The choice of e-book instead of hardcopy is due to the fact that the author is continuously working on this topic, and all updates will be included from time to time.

The price any reader would pay for this e-book is for the effort the author has put into centralizing all relevant information into one document, but will be 100% donated to a good cause. This can be functional know-how, technical knowledge and step-by-step examples of the usage of available authorization objects in the different SAP Modules.

The book is not intended to replace any SAP course and the author strongly advises to attend the basic courses for every SAP Module such as SAP CRM and SAP BW. Furthermore it is also advised to follow the specific SAP Authorization related courses such as:
A) BW365: Business Information Warehouse - Authorizations  
B) ADM940: SAP Authorization Concept  
C) HR940: Authorizations in HR

Foreword

This guide has been written to elaborate the SAP Authorization concept and to give concrete system examples to understand the design and implementation.

Today a lot of large national and international companies are using SAP as an ERP system to automate their business processes. They often use the well-known R/3 modules such as SD, FI/CO, MM and so on, but also new technologies such as Business Warehouse (BW) and Customer Relationship Management (CRM) and SAP Enterprise Portal.

Business processes are defined and elaborated in those systems by Customizing and developments. Now the way people work with these systems or should be able to work with is being defined by implementing the authorization concept.

In the first chapters I will try to give a solid overview of the general authorization concept, which in fact is valid not only for R/3, but also for other SAP modules such as SAP CRM and BW.

Next I will try to elaborate some concrete examples within the domain of SAP CRM, since this is the module I am working on, on a day-to-day basis.

Because I try to share knowledge within my company but also with fellow SAP CRM colleagues and authorization specialists, I decided to write this manual.
1. Introduction

Those people that already obtained the book should know that it is not finished yet. When I find the time in between projects I will try to concentrate on some specific topics such as ACE (Access Control Engine). Furthermore I will elaborate an example for usage of every Authorisation object in SAP CRM, since this is the module I work in on a day-to-day basis.

2. SAP Authorization Concept

The SAP Authorization concept allows you to define what people can do in the SAP System, but more importantly what they are NOT allowed to do. When doing their day to day job, people are performing actions in the system such as creating sales orders, creating/changing master data (products, business partners), or entering leads/opportunities in the CRM system.

Of course some information should not be accessed by everyone, or at least not be changeable.

Examples:
- Employees should not be able to change their salary records.
- Only certain employees are responsible for creating sales orders in the system
- Account Managers should only be able to change master data information for their own business partners (sales prospects/customers).

The SAP authorization concept protects transactions and programs in SAP systems from unauthorized access. On the basis of the authorization concept, the administrator assigns authorizations to the users that determine which actions a user can perform in the SAP System, after he or she has logged on to the system by entering his/her username and password.
Most components concerning authorizations can be found in the SAP menu:

2.1. Authorization Components and their Relationships

A user will have one or more roles assigned to his user master record (maintenance can be done via the transaction code SU01). These roles can be single roles or composite roles. Furthermore the user also can have authorization profiles assigned to the user master record (a generated authorization profile via the profile generator, or a manual created authorization profile or standard SAP authorization profile such as SAP_ALL.)
A role usually contains one or more transactions. Every transaction contains a number of authorization objects that are being checked to see if the user has the right authorization to perform a specific action in the system. An authorization object in its turn can contain one or more authorization fields.

Figure 2.0: Authorization components and their relationships
Explanation of the Graphic:

- **User Master Record**: These enable the user to log onto the SAP system and allow access to the functions and objects in it within the limits of the authorization profiles specified in the role.

Changes only take effect when the user next logs on to the system. Users who are logged on when the changes take place are not affected in their current session.

- **Single Role**: Is created with the profile generator and allows the automatic generation of an authorization profile. The role contains the authorization data and the logon menu for the user.

- **Composite Role**: Consists of any number of single roles.

- **Generated authorization profile**: Is generated in role maintenance from the role data.

- **Authorization object**: An authorization object groups up to ten authorization fields that are related by AND. An authorization object allows complex tests of an Authorization for multiple conditions. Authorizations allow users to execute actions within the system. For an authorization check to be successful, all field values of the authorization object must be appropriately maintained in the user master (the SY_SUBRC must equal 0 during the authority check).

Authorization objects are divided into authorization classes for comprehensibility. An object class is a logical combination of authorization objects and corresponds for example, to an application (financial accounting, human resources, and so on).

![Figure 2.1: Screenshot of authorizations in the Profile Generator](image_url)
2.2. The Profile Generator (PFCG)

In the CRM system (release 4.0) you start the Profile generator in the SAP Menu via the path:
Architecture and Technology → System Administration → User Maintenance → Role Administration → Roles

Or directly by using the transaction code “/npfcg” in the command field.

![SAP Easy Access Extended Interface]

You can use the Profile Generator to manage roles and authorization data. You can automatically create the authorization profiles with this tool.

![Role Maintenance]

Figure 2.3: Screenshot of the profile generator screen

**Remark:** depending on the release of your system (being R/3, BW or CRM) the access to the profile generator might be different, so the easiest way is to use the Transaction code PFCG immediately.
2.2.1. Installing the Profile Generator

You must first configure the system so that you can use the role maintenance function and the Profile Generator. To do this, perform the following steps:

1. Set the profile parameter **auth/no_check_in_some_cases** to the value **Y**.

**Profile parameters** can be displayed/changed via the transaction code RZ11.

**Display Profile Parameter Attributes**

<table>
<thead>
<tr>
<th>Param Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth/no_check_in_some_cases</td>
<td>Activation of the Profile Generator</td>
</tr>
</tbody>
</table>

You could also look at the full overview of the configured parameters in transaction code TU02 or report RSPARAM (called in transaction code SA38).

**Parameter Changes in SAPSYSTEM cernum04 00**

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>CCI cernum04</th>
</tr>
</thead>
<tbody>
<tr>
<td>04.01.2006 16:36:53</td>
<td>cernum04</td>
</tr>
</tbody>
</table>

**List of Active Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert/cache/size_MB</td>
<td>6</td>
</tr>
<tr>
<td>alert/param_file</td>
<td>G:\usr\sap\CC1\CWEBG00\Log\ALPARAMS.DAT</td>
</tr>
<tr>
<td>auth/authorization_trace</td>
<td>4</td>
</tr>
<tr>
<td>auth/new_buffering</td>
<td>4</td>
</tr>
<tr>
<td><strong>auth/no_check_in_some_cases</strong></td>
<td><strong>Y</strong></td>
</tr>
<tr>
<td>auth/object_disabling_active</td>
<td><strong>Y</strong></td>
</tr>
<tr>
<td>auth/rfc_authority_check</td>
<td>1</td>
</tr>
</tbody>
</table>
2. Execute transaction SU25.

Transaction SU25 copies the proposals for check indicators and authorization field values delivered by SAP to the customer tables USOBX_C and USOBT_C, which you can then change by using the transaction code SU24. You can then use the role maintenance functions and the Profile Generator to manage the authorization information for your users.

Profile Generator: Upgrade and First Installation

Installing and upgrading the Profile Generator

<table>
<thead>
<tr>
<th>Actions to be performed</th>
<th>Date</th>
<th>Time</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Profile Generator</td>
<td>23.05.2003</td>
<td>11:56:08</td>
<td>DDIC</td>
</tr>
</tbody>
</table>

Post-processing the settings after upgrading to a higher Release

<table>
<thead>
<tr>
<th>Actions to be performed</th>
<th>Date</th>
<th>Time</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>2A. Preparation: Compare with SAP values</td>
<td>17.07.2002</td>
<td>17:48:09</td>
<td>DDIC</td>
</tr>
</tbody>
</table>

2B. Compare transactions
2C. Roles to be checked
2D. Display changed transaction codes

Transport connection

3. Transport the customer tables

Adjusting the authorization check (optional)

4. Check indicator (Transaction SU24)

5. Deactivate authorization object globally

Create roles from manually-created profiles

6. Copy data from old profiles

You can set the tables to the check indicators described below. It is important to note that the check of a specific authorization object during the processing of a transaction cannot be simply forced by simply maintaining the object in tables USOBT_C and USOBX_C.
Instead, the check indicators in table USOBX_C only define how the system responds to the authorization checks that are contained in the ABAP coding of the respective transaction.

<table>
<thead>
<tr>
<th>Check Indicator</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>Not maintained</td>
<td>No indicator has been set. The check is always performed. The object is not proposed in the Profile Generator.</td>
</tr>
<tr>
<td>N</td>
<td>No check</td>
<td>The check is not active. The object is not processed in the Profile Generator.</td>
</tr>
<tr>
<td>C</td>
<td>Check</td>
<td>The check is always performed. The object is not proposed in the Profile Generator.</td>
</tr>
<tr>
<td>CM</td>
<td>Check/Maintain</td>
<td>The check is always performed. The object is proposed for maintenance in the Profile Generator.</td>
</tr>
</tbody>
</table>

Example of Check Indicators for Transaction BP in the CRM system:

<table>
<thead>
<tr>
<th>Check Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>Business Partner: Authorization Types</td>
</tr>
<tr>
<td>N</td>
<td>Business Partner: Field Groups</td>
</tr>
<tr>
<td>C</td>
<td>Business Partner: Authorization Groups</td>
</tr>
<tr>
<td>CM</td>
<td>Business Partner: BP Roles</td>
</tr>
<tr>
<td></td>
<td>Business Partner: Relationship Categories</td>
</tr>
<tr>
<td></td>
<td>Business Partner: Field Groups</td>
</tr>
<tr>
<td></td>
<td>Payment Cards</td>
</tr>
<tr>
<td></td>
<td>Data Cleansing</td>
</tr>
<tr>
<td></td>
<td>Status Management, Set/Delete User Status</td>
</tr>
<tr>
<td></td>
<td>Banks: General Maintenance Authorization</td>
</tr>
<tr>
<td></td>
<td>Personnel Planning</td>
</tr>
<tr>
<td></td>
<td>System Authorizations</td>
</tr>
<tr>
<td></td>
<td>ALV Standard Layout</td>
</tr>
<tr>
<td></td>
<td>Authorization for Document Set</td>
</tr>
<tr>
<td></td>
<td>Background Processing: Background Administrator</td>
</tr>
<tr>
<td></td>
<td>Background Processing: Operations on Background Job</td>
</tr>
<tr>
<td></td>
<td>Administration Functions in the Change and Transport System</td>
</tr>
<tr>
<td></td>
<td>Authorization for file access</td>
</tr>
<tr>
<td></td>
<td>ABAP Workbench</td>
</tr>
<tr>
<td></td>
<td>QM Documentation Maintenance Authorization</td>
</tr>
<tr>
<td></td>
<td>Authorization for SU1 activities</td>
</tr>
<tr>
<td></td>
<td>SAPoffice: Authorization for an Activity with Documents</td>
</tr>
<tr>
<td></td>
<td>SAPoffice: Office User Attribute</td>
</tr>
<tr>
<td></td>
<td>Authorization Object for Sending</td>
</tr>
<tr>
<td></td>
<td>IMS: New authorizations for projects</td>
</tr>
<tr>
<td></td>
<td>Authorization Check for RFC Access</td>
</tr>
<tr>
<td></td>
<td>Spoof: Device authorizations</td>
</tr>
<tr>
<td></td>
<td>Cross-Client Table Maintenance</td>
</tr>
<tr>
<td></td>
<td>Table Maintenance (via standard tools such as SM30)</td>
</tr>
<tr>
<td></td>
<td>Transaction Code Check at Transaction Start</td>
</tr>
<tr>
<td></td>
<td>Translation environment authorization object</td>
</tr>
<tr>
<td></td>
<td>Transport Organizer</td>
</tr>
<tr>
<td></td>
<td>User Master Maintenance: User Groups</td>
</tr>
<tr>
<td></td>
<td>ArchiveLink: Authorizations for access to documents</td>
</tr>
</tbody>
</table>
With the transaction SU24, you can check/change the authorization objects that are relevant for a specific transaction.

First of all, this allows you to check upon the relevant authorization objects that are checked/checked-Maintained within a transaction. If an authorization object is checked/maintained, this means that relevant SAP-fields (like BUKRS for company code) can be maintained/restricted in the profile Generator when adding this transaction into a role.

Let’s take an example:
Suppose we would like to see what authorization objects are relevant for the transaction “BP”.

You launch the transaction SU24, and enter the transaction.

The other option: “edit check indicator in all transactions” is used to see in what transactions a certain authorization object is used and which status it has for that transaction (Checked; Check/Maintain…).
For example, you could give in the auth. Object K_ORDER and press execute. This returns a list with all Transaction Codes where the authorization object is relevant for the transaction.

Now, to continue, when we press execute for the above screen, we would get the following:
Here you see three buttons:

1) Display Value list

Here you only see the relevant authorization objects with the status (check indicator) and the object description.
You also see the fields (if status is check/maintain) that you are able to restrict upon in the profile generator: e.g. example below authorization object B_BUPA_RLT for Transaction code BP.

<table>
<thead>
<tr>
<th>EF</th>
<th>Check/maintain</th>
<th>B_BUPA_RLT</th>
<th>Business Partner: BP Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>FID</td>
<td>Val Trn</td>
<td>Value to</td>
<td></td>
</tr>
<tr>
<td>ACTVT</td>
<td>01</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLTVF</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When pressing the button ![Check indicator](image), you get a list similar to the display value list; so with the authorization objects, the status and the description.

**Display Check Indicator for BP**

<table>
<thead>
<tr>
<th>N CI CM Check ID</th>
<th>Object</th>
<th>Object name</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Business Partner: Authorization Types</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_GRP</td>
<td>Business Partner: Field Groups</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Business Partner: BP Roles</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Business Partner Relationships: Relationship Categories</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Business Partner Relationships: Skill Groups</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Payment Cards</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Data Cleansing</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>Status Management: Set/Delete User Status</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>FMX_MIB</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>PLM6</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>OMLL</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>ALV</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>BSG_WK</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
<tr>
<td><img src="image" alt="Check indicator" /></td>
<td>B_BUPA_RLT</td>
<td>SE81</td>
</tr>
</tbody>
</table>
| ![Check indicator](image) | B_BUPA_RLT | SE81 | Authorization Object for Work C...
Here you create a new request, give it an appropriate name: e.g. Change authorization checks for Tcode BP.

The Request number generated by the system is the following:

Press ok.

Now you are in change mode and can either change the status of existing authorization objects in the transaction or add a new authorization object into the transaction. This you can do by pressing the button Auth. Object with the plus sign. This launches a pop-up where you enter the name of the authorization object.
Press ok.
You now see that the authorization object is in the list for this transaction and can change the status if you want.

Example below: for financial report (with tcode /PEU/FI_E0006_3) the authorization object Z_ACCRUAL was added.

In this case the status is on Check/Maintain.

After you have made the necessary changes into the transaction you save.

Now, you can immediately check (in development where you made the change) this change of the transaction by adding this transaction into a role via the profile generator. You will see that the authorization object is automatically taken up into the tab “Authorizations” where you can set restrictions for the relevant fields within this auth. Object.

Remarks:
1) Changes that you made for a transaction, after testing for restrictions on this transaction need to be transported to QA and the Production system. This is necessary if you create a role with this transaction and want to transport the role to production, so that change for the transaction you made is also available in the other clients.

1) If you would change a transaction that is already used in other roles, this could affect the authorizations within that role, so always check what the effect is, because it might be possible that the tab “authorizations” in the role where the transaction was in before becomes red now.
2) In our example we used an authorization object that was standard SAP. It is also possible to have a completely new Authorization object created (with own development class) and where the code (program) behind is changed to add a check. (This will be done by the ABAP-team).

Once they have created the new authorization object in development, you can either add this authorization object to the role (manually) or into the relevant transaction. Either way, it needs to be in one of the two options. Where you will add the authorization object is up to you. But the person, who needs to have authorization, needs to have this allocated to his user profile. This is either done by allocating the role to his user-profile (with the changed transaction) or by adding the auth. Object manually into the role.

3) When your test results turn out to be all right, then you need to pay attention with the order of transports:

In development you already can create the role with:
- The changed transaction in it
- Or with the auth. Object manually added into the role

If you changed the transaction, then you will have a transport request for this transaction change, which will update the table: USOBT_C.

In the case where you changed the transaction itself, first transport the change of the transaction that you made by using the transaction SU24 and the transport for the creation of the new authorization object. (A person of the ABAP-team normally made this request).
Next you transport the roles you created with either the auth. Object manually added, or with the changed transaction in it.

Once the roles are in production, you best do the user-allocation first and as last you transport the change in code that was made by the ABAP-team.

From that moment on the user should be able to use the transaction(s) with the relevant restrictions you wanted to make.
2.2.2. Creation of a new Role

Naming conventions:

The roles that are standard delivered by SAP correspond to the working environment of certain users. As these roles are only templates; that is, examples of work centers, you must still adjust these roles to the requirements of your users.

Standard SAP roles start with “SAP_”. The predefined roles are delivered as templates. Do not change the delivered standard roles (SAP_*), but rather only the copies of these roles.

For your own roles, instead of using the SAP namespace, use the customer namespace. This means that the prefix is “Y_” or “Z_”. Since you cannot tell from the names of the delivered roles whether they are single or composite roles, you should create a naming convention for your roles so that you can differentiate between single and composite roles.

Types of roles:
First of all you should know that there exist different types of roles. The different types and purpose I will explain are the following:

- Single role
- Composite role
- Master Role
- Derived Role

As soon as you start the Profile Generator, when creating a new role, you should make a choice between creating a Single role or a Composite role.

2.2.3. Single Role versus Composite Role (collective role)
You could look at it like this:

A single role usually is made to define all necessary transactions and/or reports used to perform a certain specific task such as master data maintenance or product maintenance.
Let’s take a specific example for the module CRM. In a company you have 20 employees using the CRM system.

Persons with functions like:
- marketing manager
- marketing assistant
- Master data administrator
- Call center agent
- ….

You have created for example several single roles such as:

Z_MARKETING_PLAN (create/change marketing plans)
Z_MARKETING_CAMPAIGN (create/change marketing campaigns)
Z_BP_DISP (display business partners)
Z_BP_ALL (create/change/display business partners)
Z_PROD_DISP (display all products)
Z_PROD_ALL (create/change products)
Z_LEADS (create/change/display leads)
Z_OPPORTUNITIES (create/change/display opportunities)

Now you can imagine that the Role Z_MARKETING_PLAN only should be assigned to the marketing manager and not to his assistant for example.

Furthermore, you will also see that one person (with a certain function) will need to have more than one single role assigned to his user master record, since the marketing manager will also need to be able to display products and business partners.

Therefore you will make a COMPOSITE role per function in your company, where you assign the different single roles needed to perform the processes in the system needed to do his job.

The advantage is that you do not need to assign every time every single role to a new person when for example someone leaves the company and a new marketing manager is hired. In that case you just create a new User in the system and assign the composite role.

**Procedure for creating a Composite Role:**

1) Start the profile generator and enter the technical name of your composite role.
Role Maintenance

To create the composite role, you press the button “Comp. Role”.

You will get the following screen:

Change Roles

2) On the tab ‘Roles’ enter the different single roles that should be contained in the composite role that make up all the necessary functions and authorizations that the marketing manager will need to perform his processes and actions in the system.

3) Last you assign the composite role to one or more people that share the same function as marketing responsible.
2.2.4. Master role and Derived Role

For a single role you should also now that there is the definition of a Master role and a Derived role.

Example:

You have implemented the R/3 SD module in an international Organization. Operations happen in the same way for all countries. So the processes as they are customized and setup are the same, but of course in one country people should only be allowed to create sales orders for a certain company code.

This means you need to use authorizations to limit on organizational elements. What you can do in such a case is create a general template role where you define what activities/transactions can be used, but do not set any limitations on organizational level. Next, you create for each country a derived role, where you put the right authorizations in place.

Creation of the Master Role (template Role)

The role we wanted to create was the Master Role for a local Sales Administration Operator. This was done as follows:
So you type in the name of the master role to be created and press the *Create Button*. In the following screen, you type in the description and press the save button.

In this starting screen, you see a number of tabs: Description, Menu, Authorizations, User etc.

These are important and will be explained further on.

Go to the tab “Menu” where you will enter the transactions that need to be assigned to the master role.
When you press the "Transaction button", you get the following pop-up screen, where you enter manually the Transaction codes. By pressing enter, the description for this transaction appears on the right side of the transaction-code. When you have finished entering your list of transactions, press the button ‘Assign Transactions’.

By using the Transaction button, you add transactions in this role.

When you press the “Transaction button”, you get the following pop-up screen, where you enter manually the Transaction codes. By pressing enter, the description for this transaction appears on the right side of the transaction-code. When you have finished entering your list of transactions, press the button ‘Assign Transactions’.
Now that you have entered the necessary transactions in the master role, you go to the tab ‘Authorizations’, where you enter the profile name and the profile text.

Press the Save button. 
Now you will maintain the authorization data for this role! Press the “change authorization data” button.

This will probably bring up a popup, where the relevant organization levels for the transactions you entered in the role, are already predefined by the system. When no Organization level is relevant for the transaction(s) you entered, then off course you don’t get this pop-up.
In the master role, in the case where you will create derived roles, you usually give full authorization. This can be done by manually entering a * or by pressing the button “Full authorization”.

Then press save.

You automatically return in the screen, where the relevant authorization objects for the entered transactions are in the screen.

In this case, since the role was already created (saved and generated) all the bolls have a green light. But when you create a new role, they have a yellow/red color and need to be maintained. This involves clicking everything open and press for each object on the * so that it becomes green. But at this moment, you also can decide whether you want to limit
authorizations for an activity, or some other field of an authorization object that can be maintained. This can be done by clicking on the change button (✍).

**Note:** A red color means that you have not specified an Organization level yet. To do this, you press the “organization levels” button, where you can maintain them.

![changed, maintained, organizational levels]

Once you have made all the traffic lights green (with or without setting restrictions on fields that are checked upon in the authorization objects, you can save the role and generate it.

![red button]

When you have done all these things, go back in the Description tab where you fill in the organization levels, other localization objects and other specific remarks concerning this role (for example manually entered authorization objects (SAP or own developments), etc.

In the derived roles you will do the same, but there you will have the restrictions on the organization levels in the long text, so when viewing the role, you immediately can see for which fields there are restrictions set.

**Creation of a Derived Role**

In this example I show you an example of how one or more derived Roles can be created. In the master role you already put in the relevant and necessary transactions. So maintenance concerning transactions **ALWAYS** happens in the master role (Delete/add transactions).

Start the transaction PFCG (profile generator) where you put in the name for the derived role.

![role maintenance]

Press the Create button.

© 2007 Contact Author: davy.pelssers@contactoffice.net
Fill in the description and press save.

<table>
<thead>
<tr>
<th>Role</th>
<th>/PEU/PEH_SD_L_OPS_01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>01001: PEH SAD Local Sales Administration Operator_01</td>
</tr>
</tbody>
</table>

Next you put the name of the master role in the field “Derive from Role”.

<table>
<thead>
<tr>
<th>Transaction inheritance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derive from role</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

You get a pop-up asking if you want to derive all characteristics from the Master role, where you answer yes.

Then, you can look in the tab “Menu” where you’ll see that the transactions from within the master role are also taken over in the derived role.

Go further into the tab ‘Authorizations’ where you now can change the Organization levels, and other restrictions for fields that are included in the authorization objects. (Make again sure that all the traffic lights are green.)

As you can see below, we set the restriction on Company code and Sales Organization. By doing so, the system automatically puts these values in the relevant fields in the authorization objects below.

<table>
<thead>
<tr>
<th>Define Organizational Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain the role org level values:</td>
</tr>
<tr>
<td>Org level</td>
</tr>
<tr>
<td>Company code</td>
</tr>
<tr>
<td>Controlling area</td>
</tr>
<tr>
<td>Division</td>
</tr>
<tr>
<td>Sales organization</td>
</tr>
<tr>
<td>Shipping point</td>
</tr>
<tr>
<td>Distribution channel</td>
</tr>
<tr>
<td>Plant</td>
</tr>
</tbody>
</table>
2.2.5. Assigning Users

To assign users to a certain role (being single role or a composite role) you open the role in the profile generator and select the tab ‘User’. The status display on the tab page tells you whether users have already been assigned to the role.

- Red: No users are assigned
- Green: At least one user is assigned
- Yellow: Although users are assigned, user master comparison is not current. For composite roles, the status display refers only to the assignment of users.
Procedure:

1) Enter as many user IDs as desired in the list.
   Enter the user IDs directly or from the possible entries help. You can make multiple selections with the ‘Selection’ pushbutton, such as all users in a user group.

2) Perform a user comparison if necessary.
   The generated profile is not entered in the user master record until the users have been compared. Changes to the users assigned the roles and the generation of an authorization profile also requires a comparison.

3) The default validity date when entering a new User ID into the role assignment is the following:
   From: Date of today
   To: 31.12.9999
   If you want to restrict this validity date, just enter the dates according to your wishes. If you want to limit the validity period, you must periodically schedule the report transaction PFUD daily to update the user master records. Is must also be scheduled if you use the organizational management.
Never enter generated authorization profiles directly into user master records, as these are deleted if the corresponding role is not contained in the user master record.

For **user comparison** you have the following options:

1) Choose the “User comparison” button on the ‘User’ tab page. The users are then compared for the selected role you created. The status for that role will next change into green after the comparison is finished successfully.
2) Choose Utilities→Settings→ Automatic comparison at save. When you save the role, a user comparison is performed automatically.
3) Wait until the user comparison is made with the program “PFCG_TIME_DEPENDENCY”. Set the indicator HR-OrgComparison indicator on the selection screen of the report.

You should schedule the report PFCG_TIME_DEPENDENCY periodically (preferably daily) as a background job. This ensures that user authorizations are regularly updated. The program performs a complete user master comparison for all roles. The authorizations are updated in the user master records. The authorization profiles of user assignments which have become invalid are removed from the user master record. The authorization profiles of valid user assignments to the role are entered.

**ABAP Editor: Initial Screen**

You can launch this report via the transaction code SE38 or SA38.
2.2.6. Transporting Roles

To transport a role you have created, launch the profile generator and enter the name of the role you want to transport.

To transport the role, press the ‘transport’ button.

In this case I choose a composite role and get the following screen:

The system asks you if you also want to transport the single roles of this composite role, and if you want to transport the generated profiles of the single role. Select both entries!

⚠️ You should not change the authorization profiles of the role after you have included the role in a transport request. If you need to change the profiles or generate them for the first time, transport the entire role again afterwards!

In the following dialog box, specify whether the user assignment and the personalization data should also be transported!

Next you need to enter a transport request. (You can check the transport request afterwards with transaction SE10).
2.3. Organizing Authorization Administration

The authorization system allows you great flexibility in organizing and authoring the maintenance of user master records and roles:

1) If your company is a small or medium sized company, you can have all maintenance of user master records and authorization components executed by a single person or super user.
2) Depending on the size of your company you should think about distributing responsibilities between more teams responsible each for another purpose. On the one hand you have one team/person responsible for the maintenance of user master records and assigning the appropriate roles. On the other hand you have the second team responsible for the authorization administration, meaning the creation of new roles and authorization profiles.

Since you can precisely restrict authorizations for user and authorization maintenance, the administrators do not have to be privileged users in your organization. You can assign user and authorization maintenance to ordinary users.

2.3.1. Creating administrator roles

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Permissible Tasks</th>
<th>Impermissible Tasks</th>
<th>Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Admin</td>
<td>Create/change user master records</td>
<td>Change role data</td>
<td>SAP_ADM_US</td>
</tr>
<tr>
<td></td>
<td>Assigning roles to users</td>
<td>Changing or generating profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assigning profiles beginning with “T” to users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Displaying authorizations and profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the User Information system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization Data</td>
<td>Creating/changing roles</td>
<td>Changing users</td>
<td>SAP_ADM_AU</td>
</tr>
<tr>
<td>Admin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Changing authorization data and transaction selection in roles</td>
<td>Generating Profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the User Information System</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Authorization Profile Admin

<table>
<thead>
<tr>
<th>Displaying roles and the associated data</th>
<th>Changing users</th>
<th>SAP_ADM_PR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using tcode PFCG or SUPC to generate the authorizations and profiles that begin with “T” for roles that have authorization data</td>
<td>Changing role data</td>
<td></td>
</tr>
<tr>
<td>Checking roles for the existence of authorization data (tcode SUPC)</td>
<td>Generating authorization profiles with authorization objects that begin with S_USER</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performing a user master comparison (tcode PFUD, performing a profile comparison of the user master comparison)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using the User Information System</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Creation of a User Administrator Role**

1) Launch the profile generator (PFCG)

![Role Maintenance](image)

On the initial screen, fill out the technical name of your role: Z_USERADMIN and press the “create single role” button.
2) Fill out the Description Field and extra info

When selecting another Tab to maintain, you get a popup asking you to save the role, so press ‘yes’.

3) On the Tab “Menu” you can create your own user menu if you want. You are able to take over certain parts from the standard SAP menu; from another role, or create a new user menu from scratch. Next, you can also add transactions, reports or other things to the role.

You can skip this for now.
4) On the tab “Authorizations” you will use the template SAP_ADM_US

Use a profile name that does NOT begin with ‘‘T’’, so that the authorization data administrator cannot change his or her own authorizations. Now press the button change authorization data.

Again you will receive a popup asking you to save the role (press yes).
After saving you get a list of templates that you can use to create your role. Since we want to create a User Administrator, choose the template SAP_ADM_US.

You will need to maintain all authorization fields of the available authorization objects. In this case, you can see that the ‘Plan version’ has a red status. Maintain it either by pressing the red ‘star *’ to give all authorization or by pressing the change button and select the right field value.
After every authorization object is correctly maintained, you can save and generate the role.

5) On the Tab ‘Users’ you can assign this role to an EXISTING user. You can also enter a valid-from and valid-to date if you want. Otherwise the system will automatically take the date of today until 31.12.9999.

After filling in one or more users that will perform the task of User Administrator, perform a ‘User Comparison’ in order that the role will be updated in their User Master Record.

Now the person with Username ZPERSONRESP will be able to do the user administration after the user comparison has finished.

2.3.2. List of available templates

<table>
<thead>
<tr>
<th>TEMPLATE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_ADM_AU</td>
<td>Administration: Authorization data administrator</td>
</tr>
<tr>
<td>SAP_ADM_PR</td>
<td>Administration: Authorization profile administrator</td>
</tr>
<tr>
<td>SAP_ADM_US</td>
<td>Administration: User administrator</td>
</tr>
<tr>
<td>SAP_ALL</td>
<td>Complete authorization with all authorization objects</td>
</tr>
<tr>
<td>SAP_PRINT</td>
<td>Print Authorization</td>
</tr>
<tr>
<td>SAP_USER_B</td>
<td>Basis authorizations for users</td>
</tr>
</tbody>
</table>

© 2007 Contact Author: davy.pelssers@contactoffice.net
### 2.3.3. Authorization Objects checked in role maintenance

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_USER_AUT</td>
<td>User master maintenance: authorizations</td>
</tr>
<tr>
<td>S_USER_GRP</td>
<td>User master maintenance: User groups</td>
</tr>
<tr>
<td>S_USER_PRO</td>
<td>User master maintenance: Authorization profiles</td>
</tr>
<tr>
<td>S_USER_AGR</td>
<td>Authorization system: Check for roles</td>
</tr>
<tr>
<td>S_USER_TCD</td>
<td>Authorization system: Transactions in roles</td>
</tr>
<tr>
<td>S_USER_VAL</td>
<td>Authorization system: Field values in roles</td>
</tr>
<tr>
<td>S_USER_SYS</td>
<td>User master maintenance: system for Central user Administration</td>
</tr>
<tr>
<td>S_USER_SAS</td>
<td>User master maintenance: System-specific assignments</td>
</tr>
<tr>
<td>S_USER_ADM</td>
<td>Administration functions for user and authorization administration</td>
</tr>
<tr>
<td>S_USER_OBJ</td>
<td>Authorization system: global deactivation of authorization objects</td>
</tr>
<tr>
<td>S_USER_WWW</td>
<td>User master maintenance: Internet Users</td>
</tr>
</tbody>
</table>

### 2.3.4. Relevant SAP Tables for Authorizations and Roles

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR_1016</td>
<td>Name of profile for activity group</td>
</tr>
<tr>
<td>AGR_1250</td>
<td>Authorization data for activity group</td>
</tr>
<tr>
<td>AGR_1251</td>
<td>Authorization data for activity group</td>
</tr>
<tr>
<td>AGR_1252</td>
<td>Organizational levels for authorizations</td>
</tr>
<tr>
<td>AGR_PROF</td>
<td>Profile name for activity group</td>
</tr>
<tr>
<td>AGR_SELECT</td>
<td>Assignment of activity groups to transaction codes</td>
</tr>
<tr>
<td>AGR_TCDTXT</td>
<td>Assignment of activity groups to transaction codes</td>
</tr>
<tr>
<td>AGR_TCODES</td>
<td>Assignment of activity groups to transaction codes</td>
</tr>
<tr>
<td>AGR_USERS</td>
<td>Assignment of activity groups to users</td>
</tr>
<tr>
<td>TOBJ</td>
<td>Objects</td>
</tr>
<tr>
<td>TOBJC</td>
<td>Classification of authorization objects</td>
</tr>
<tr>
<td>TOBJT</td>
<td>Texts for objects (for TOBJ)</td>
</tr>
<tr>
<td>TSTC</td>
<td>SAP Transaction Codes</td>
</tr>
<tr>
<td>TSTCA</td>
<td>Values for transaction code authorizations</td>
</tr>
<tr>
<td>TSTCP</td>
<td>Parameters for transactions</td>
</tr>
<tr>
<td>TSTCT</td>
<td>Transaction texts</td>
</tr>
<tr>
<td>USH04</td>
<td>Change history: authorizations</td>
</tr>
<tr>
<td>USH10</td>
<td>Change history: authorization profiles</td>
</tr>
<tr>
<td>USH12</td>
<td>Change history: authorization values</td>
</tr>
<tr>
<td>USKRI</td>
<td>Critical combinations of authorizations for transaction codes</td>
</tr>
</tbody>
</table>
2.3.5. System Settings-profile parameters

In order to configure system-wide settings in SAP, you have to maintain the profile parameters in the Computing Center Management System (CCMS).

You can do this via transaction code **RZ11**.

*Maintain Profile Parameters*

![Parameter Name]

Transaction **RZ10** provides more information on the different profile parameters.

Most of the relevant parameters begin with “auth” or “login” and can easily be found back.

Next to RZ10 you can also display a full overview of the configured parameters via transaction code TU02 or report RSPARAM (called via SA38).
**Note:**
Remember that changing profile parameters CAN have a serious impact on your system and therefore should best be restricted to change by a Basis Administrator. Also know that a change of profile parameters can only be visible after restarting the application server.

### 2.3.6. Protective measures for Special profiles SAP_ALL & SAP_NEW

**Authorization Profile SAP_ALL**

This composite profile contains all SAP authorizations, meaning that a user with this profile can perform all tasks in the SAP system. You should therefore not assign this authorization profile to any of your users. Try to maintain only one user with this profile and keep the password of this user secret! (Only to be used in emergencies).

**Authorization Profile SAP_NEW**

This composite profile contains a single profile for each release that contains the authorizations that the users require to be able to continue using the functions that they have used until now, but which are protected with new authorization checks. However, you should not leave this profile active for a long period of time.

SAP recommends that you perform the following steps:

1. After the upgrade, delete the SAP_NEW * profiles from the composite profile SAP_NEW for releases before the last revision of your authorization concept.
2. Assign the composite profile SAP_NE to all users. This means that they can continue to use the functions that they have used until now.
3. Distribute the authorizations contained in the SAP_NEW single profiles to the roles or profiles that you use productively and maintain the authorization values.
4. Delete the profile assignment for SAP_NEW and the SAP_NEW profile.

A long list of SAP_NEW profiles (for example, after multiple upgrades) indicates that it is time to revise and redefine your authorization concept.
2.4. Authorization Checks

To ensure that a user has the appropriate authorizations when he or she performs an action, users are subject to authorization checks.

The following actions are subject to authorization checks that are performed before the start of program or table maintenance and which the SAP applications cannot avoid:

- Starting SAP transactions (authorization object S_TCODE)
- Starting reports (authorization object S_PROGRAM)
- Calling RFC function modules (authorization object S_RFC)
- Table maintenance with generic tools (S_TABU_DIS)

2.4.1. Checking at program level with AUTHORITY-CHECK

Applications use the ABAP statement AUTHORITY-CHECK, which is inserted in the source code of the program, to check whether users have the appropriate authorization and whether these authorizations are suitably defined; that is, whether the user administrator has assigned the values required for the fields by the programmer. In this way, you can also protect transactions that are called indirectly by other programs. AUTHORITY-CHECK searches profiles specified in the user master record to see whether the user has authorization for the authorization object specified in the AUTHORITY-CHECK. If one of the authorizations found matches the required values, the check is successful.

One way of finding authority checks in the program code is to search the source text of the ABAP program for the string “AUTHORITY” in the ABAP Editor (transaction SE38). This search displays all the authorization checks within the respective program.
Coding Example:

```cobol
*&------------------------------------------------------------------------------*
*& REPORT  SAPBC400DDS_Authority_Check_2
*&-----------------------------------------------------------------------------*

REPORT  sapbc400dds_authority_check_2.

CONSTANTS actvt_display TYPE activ_auth VALUE '03'.

DATA: it_flight TYPE sbc400_t_sbc400focc,
      wa_flight LIKE LINE OF it_flight.

PARAMETERS pa_car TYPE s_carr_id.

* Check if user is authorized to read data of the specified carrier?

AUTHORITY-CHECK OBJECT 'S_CARRID'
  ID 'CARRID' FIELD pa_car
  ID 'ACTVT' FIELD actvt_display.

CASE sy-subrc.
  WHEN 0.  " user is authorized"
    SELECT carrid connid fldate seatsmax seatsocc FROM sflight
    INTO CORRESPONDING FIELDS OF wa_flight
    WHERE carrid = pa_car.

    wa_flight-percentage =
    100 * wa_flight-seatsocc / wa_flight-seatsmax.

    APPEND wa_flight TO it_flight.

  ENDSELECT.

  IF sy-subrc = 0.
    SORT it_flight BY percentage.
    LOOP AT it_flight INTO wa_flight.
      WRITE: / wa_flight-carrid COLOR COL_KEY,
        wa_flight-connid COLOR COL_KEY,
        wa_flight-fldate COLOR COL_KEY,
        wa_flight-seatsocc,
        wa_flight-seatsmax,
        wa_flight-percentage, '%'.
    ENDLOOP.
  ELSE.
    WRITE: 'No ', pa_car, 'flights found !'.
  ENDIF.

  WHEN OTHERS.  " user is not authorized"
    WRITE: '/Authority-Check Error'(001).

ENDCASE.
```

© 2007   Contact Author: davy.pelssers@contactoffice.net
You can see that a check is made on the authorization object “S_CARRID”. When executing this report the system will check the profiles assigned to the user and look if this authorization object is available. If not, the system will respond with a Sy-subrc <>0 and display the output message ‘User is not authorized’. If the authorization object is available via one of the profiles in the user master record, then the system will check if the field values for this authorization object correspond to the ones defined in the coding. If this is not the case, the Sy-subrc will also <>0.

If every check is ok; then the report will be executed as normal.

2.4.2. Starting SAP Transactions

When a user starts a transaction, the system performs the following checks:

- The system checks in table TSTC whether the transaction code is valid and whether the system administrator has locked the transaction.
- The system then checks whether the user has authorization to start the transaction.

The SAP system performs the authorization checks every time a user starts a transaction from the menu of by entering a command (directly entering the transaction code into the command field). Indirectly called transactions are not included in this authorization check.

- The authorization object S_TCODE (transaction start) contains the field TCD (transaction code). The user must have an authorization with a value for the selected transaction code.
- If an additional authorization is entered using transaction SE93 for the transaction to be started, the user also requires the suitable defined authorization object (TSTA, table TSTCA).

If you make a copy of a standard transaction such as “BP” (business partner maintenance), and display the information, you see the following:
You can enter an authorization object and authorization field values at this level, meaning that when starting this transaction this authorization object will be checked.

You can use existing authorization objects, but if a standard authorization object does not fulfill your needs, you can also enter a new authorization object that you have created via transaction SU21.

**Remark:** Transactions can also be blocked by using transaction SM01.
Creation of new authorization fields via SU20

List of Authorization Fields

<table>
<thead>
<tr>
<th>Authorization field</th>
<th>Data element</th>
<th>Check table for F4 help</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>/SAPCND/AP</td>
<td>/SAPCND/APPLICATION</td>
<td>/SAPCND/T001A</td>
<td>/SAPCND/CUSTOMIZING</td>
</tr>
<tr>
<td>/SAPCND/OGT</td>
<td>/SAPCND/COND_TABLE_ID</td>
<td>/SAPCND/T001</td>
<td>/SAPCND/CUSTOMIZING</td>
</tr>
<tr>
<td>/SAPCND/HTY</td>
<td>/SAPCND/COND_TYPE</td>
<td>/SAPCND/T001Y</td>
<td>/SAPCND/CUSTOMIZING</td>
</tr>
<tr>
<td>/SAPCND/UG</td>
<td>/SAPCND/USAGE</td>
<td>/SAPCND/TBM Y</td>
<td>/SAPCND/CUSTOMIZING</td>
</tr>
<tr>
<td>ABAPFORM</td>
<td>SYFORMNAME</td>
<td>SBM</td>
<td></td>
</tr>
<tr>
<td>ACTAREA</td>
<td>SRM窸窸窣窣</td>
<td>SRM_WF_PATH</td>
<td></td>
</tr>
<tr>
<td>ACTVT</td>
<td>ACTVT</td>
<td>TACT</td>
<td>SBM</td>
</tr>
<tr>
<td>ACT_GROUP</td>
<td>AGP_NAME</td>
<td>S_USERS</td>
<td></td>
</tr>
<tr>
<td>ACT_TYPE</td>
<td>DUNIT_NOTIFY_ACT</td>
<td>DUNIT_NOTIFY</td>
<td></td>
</tr>
<tr>
<td>ADDR</td>
<td>AO_PHONE</td>
<td>TS06</td>
<td>SZS</td>
</tr>
<tr>
<td>ADGROUP</td>
<td>AO_GROUP</td>
<td>TS007</td>
<td>SZS</td>
</tr>
<tr>
<td>ADGROUP_P</td>
<td>AO_GROUP_P</td>
<td>TS008</td>
<td>SZS</td>
</tr>
<tr>
<td>ADMIN_TYPE</td>
<td>CRM_00_00_ADMIN_TYPE</td>
<td>CRM_CRM</td>
<td></td>
</tr>
<tr>
<td>ADM_FUNG</td>
<td>M1_GLMADM_FUNG</td>
<td>M1_GLMADM</td>
<td>ME_CORE</td>
</tr>
<tr>
<td>AGFUN</td>
<td>CC_REFUN</td>
<td>CC</td>
<td></td>
</tr>
<tr>
<td>AGFUNK</td>
<td>KENST</td>
<td>CC</td>
<td></td>
</tr>
<tr>
<td>AF_CHEF_ASSIGN</td>
<td>CHAR1</td>
<td>S_CREATE_RESULT_MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>AF_CHEF_CREATE</td>
<td>CHAR1</td>
<td>S_CREATE_RESULT_MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>AF_CHEF_REGISTER</td>
<td>CHAR1</td>
<td>S_CREATE_RESULT_MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>AGFUNK</td>
<td>KENST</td>
<td>CC</td>
<td></td>
</tr>
</tbody>
</table>

Creation of new authorization object via SU21

List of Object Classes

<table>
<thead>
<tr>
<th>Obj.C1.</th>
<th>Short text</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAAA</td>
<td>Not assigned to a class</td>
</tr>
<tr>
<td>AAAB</td>
<td>Obsolete Authorization Objects</td>
</tr>
<tr>
<td>BBP</td>
<td>BBP Component</td>
</tr>
<tr>
<td>BC_A</td>
<td>Basis: Administration</td>
</tr>
<tr>
<td>BC_B</td>
<td>Basis: Development Environment</td>
</tr>
<tr>
<td>BC_2</td>
<td>Basis: Central Functions</td>
</tr>
<tr>
<td>BEA</td>
<td>Authorization Objects for Billing Engine</td>
</tr>
<tr>
<td>CLAS</td>
<td>Classification</td>
</tr>
<tr>
<td>CMS</td>
<td>Channel Management Solution</td>
</tr>
<tr>
<td>CRM</td>
<td>CRM Component</td>
</tr>
<tr>
<td>C_MW</td>
<td>CRM Middleware</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>ICM</td>
<td>CRM: Incentive and Commission Management</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Management</td>
</tr>
<tr>
<td>WFM</td>
<td>Work Force Management</td>
</tr>
</tbody>
</table>

© 2007   Contact Author: davy.pelssers@contactoffice.net
Select the correct Object class, and you get a list of all authorization object for this object class.

Example: for object class “CRM”.

<table>
<thead>
<tr>
<th>Object</th>
<th>Short text</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_PRP_BP</td>
<td>Authorisation Object for PPR Maintenance via BAPI</td>
</tr>
<tr>
<td>CRM_PRP_MT</td>
<td>Authorisation Object for PPR Maintenance via PRP API</td>
</tr>
<tr>
<td>CRM_MAP_TM</td>
<td>Authorisation object for CRM MKT Mapping Tool</td>
</tr>
<tr>
<td>COM_IL</td>
<td>Authorization Check for Relationships</td>
</tr>
<tr>
<td>CRM_CIC_DT</td>
<td>Authorization Object CRM , CIC - Check Overriding</td>
</tr>
<tr>
<td>CRM_CCHM_PS</td>
<td>Authorization Object CRM Channel Mngt. - Partner Self Serv.</td>
</tr>
<tr>
<td>CRM_CCHM_VL</td>
<td>Authorization Object CRM Channel Mngt. - View Restriction</td>
</tr>
<tr>
<td>CRM_ISO_US</td>
<td>Authorization Object CRM ISA - User Administration</td>
</tr>
<tr>
<td>CRM_MPL_AD</td>
<td>Authorization Object CRM Marketing - General Settings</td>
</tr>
<tr>
<td>CRM_ORDM</td>
<td>Authorization Object CRM Marketing Business Object Deal</td>
</tr>
<tr>
<td>CRM_ORDS</td>
<td>Authorization Object CRM Order - Allowed Organ. Units</td>
</tr>
</tbody>
</table>

You can create here your own authorization object within this object class.
The system checks whether the transaction code is assigned an authorization object. If so, a check is made that the user has authorization for this authorization object.

You can check this via Transaction code SU24.
2.4.3. Starting Report Classes

You can perform additional authorization checks by assigning reports to authorization classes (using report RSCSAUTH).

Consider the following:

- After you have assigned reports to authorization classes or have changed assignments, you may have to adjust objects in your authorization concept (such as roles (activity groups), profiles, or user master records).
- There are certain system reports that you cannot assign to any authorization class. These include:
  - RSRZZLG0
  - STARTMEN (as of SAP R/3 4.0)
- Reports that are called using SUBMIT in a customer exit at logon (such as SUSR0001, ZXUSRU01).
- Authorization assignments for reports are overwritten during an upgrade. After an upgrade, you must therefore restore your customer-specific report authorizations.

### 2.4.4. Calling RFC Function Modules

When RFC Function modules are called by an RFC client program or another system, an authorization check is performed for the authorization object S_RFC in the called system. This check uses the name of the function group to which the function module belongs. You can deactivate this check with parameter `auth/rfc_authority_check`.

### 2.4.5. Checking assignment of Authorization Groups to Tables

You can also assign authorization groups to tables to avoid users accessing tables using generic access tools (such as transaction SE11, SE16, SM31, OBA5 and so on). A user requires not only authorization to execute the tool, but must also have authorization to be permitted to access tables with the relevant group assignments. For this case, tables are delivered with predefined assignments to authorization groups. The assignments are defined in table TDDAT; the checked authorization object is S_TABU_DIS.

Remember that changing the assignment of tables is a modification of standard SAP; you are recommended to only modify those tables where the risk is very high. (i.e., that incorrect changes can result in inconsistent data or an unwanted system response for Customizing tables).

You can also use Transaction code SE54 to access this assignment.

---

### Generate Table Maintenance Dialog: Initial Table/View Screen

![Table Maintenance Dialog](image)

© 2007   Contact Author: davy.pelssers@contactoffice.net
If necessary you can also use authorization object S_TABU_CLI for cross-client table maintenance, in addition to authorization object S_TABU_DIS.

As of SAP release 4.6. You can also use the new authorization object S_TABU_LIN, which enables you to grant authorization for specific lines of a table. You can use this object to restrict access to certain data ranges and work areas within the table, for example, to specific plants, or company codes.

### 2.5. Analyzing Authorization Checks

If you do not know the required authorizations for a transaction, you can determine them in the following ways:

#### 2.5.1. System Trace

You can use the system trace function (transaction ST01) to record authorization checks in your own and in external sessions, if the trace and the transaction to be traced are running on the same application server. The trace records each authorization object that is tested, along with the object’s fields and the values tested.

![System Trace](image)

You will use this in certain cases to check authorization problems when you’re not using the standard SAP GUI. (Example, in the Bex analyzer, the IC Webclient, PCUI screens)
Suppose you are launching a BW report in the BEX analyzer. The consultant (who has SAP_ALL authorization) is able to launch this report without any problem, but the end-user which has certain Customer Defined roles, is having problems when launching the same report.

Since performing an SU53 authorization check is useless in such a case, you still can use the ST01 trace.

This trace is also useful in case you use PCUI screens or the IC Webclient.

→ **Procedure:**

Flag the ‘authorization check’ field and next, by pressing the button ‘general filters’ you can choose for which user you want to activate the trace!

Next, push the button “Trace on”.

Let the user who has the authorization problem perform the action(s) again in the system. After the user encountered the problem again, push the button “trace off” and press the “analysis button”.

On the next screen below, check/flag the ‘authorization check’ field and press the execute button.
In your result screen below, you can see that all checks were positive (dark green color) meaning that all authorization checks so far did not pose any problem. In case of a lack of authorization you will see another color, and a return code (RC = 0) different from “0”.

**Trace display**

<table>
<thead>
<tr>
<th>Client: 280</th>
<th>User: DAVYPP</th>
<th>Transaction</th>
<th>Trans ID: 4F459D6C198448866CD05512887381F</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Block of Dialog Step</td>
<td>Last Block in Dialog Step</td>
<td>Block Version: 088</td>
<td>No. of records: 10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>sec</th>
<th>Type</th>
<th>LastSec</th>
<th>Obj</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>59</td>
<td>28</td>
<td>059</td>
<td>KUTH</td>
<td>TCIEP</td>
</tr>
<tr>
<td>14</td>
<td>59</td>
<td>22</td>
<td>975</td>
<td>KUTH</td>
<td>TCIEP</td>
</tr>
<tr>
<td>14</td>
<td>59</td>
<td>22</td>
<td>450</td>
<td>KUTH</td>
<td>TCIEP</td>
</tr>
<tr>
<td>14</td>
<td>59</td>
<td>22</td>
<td>450</td>
<td>KUTH</td>
<td>TCIEP</td>
</tr>
<tr>
<td>14</td>
<td>59</td>
<td>28</td>
<td>980</td>
<td>KUTH</td>
<td>TCIEP</td>
</tr>
</tbody>
</table>

© 2007  Contact Author: davy_pelssers@contactoffice.net
2.5.2. Authorization error Analysis

You can use transaction SU53 to analyze an access-denied error in your system that just occurred. You can use transaction SU53 from any of your sessions, not just the one in which the error occurred. You cannot analyze an authorization error in another user’s logon session from your own session.

With this transaction you can check what authorizations are checked when a user is using a transaction and seems to be blocked because of authorization issues.

(Usually he gets the message: “you have no authorization …”.)

Although the user has a role (profile) allocated to his user-profile with the transaction in that role, he is blocked at a certain moment. This may be possible, because when performing a certain transaction, the first thing that is checked is whether you have authorization for the object “S_TCODE”. If so, and this will always be the case when you have added the transaction into the role, then he will be able to launch the transaction, but that’s all. If relevant transactions are used or authorization objects that are not standard in the transaction, but for which the user needs to have authorization, then you need to perform the transaction SU53 at the moment you are blocked to see what is checked on the one hand, and what the user has authorization for on the other hand.

This allows you to make the necessary changes to the role by manually adding the necessary authorization objects into that role with the limitations on the fields you want.

You can perform this SU53 by typing in /nsu53 in the screen where you were blocked for this transaction:

Example:

This means that the user has this transaction not within a role allocated to his user-profile.
### Display Authorization Data for User TESTAKN

<table>
<thead>
<tr>
<th>User</th>
<th>TESTAKN</th>
<th>System:</th>
<th>EE1</th>
<th>Client:</th>
<th>203</th>
</tr>
</thead>
</table>

The following authorization object was checked:

<table>
<thead>
<tr>
<th>Object</th>
<th>S_TCODE</th>
<th>Authorization Check for Transaction Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>AAAB</td>
<td>Cross-application Authorization Objects</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction code</td>
<td>VA01</td>
</tr>
</tbody>
</table>

Available authorizations for the object in the master record:

<table>
<thead>
<tr>
<th>Authorization</th>
<th>S_TCODE</th>
<th>Authorization Check for Transaction Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>T-E140003901</td>
<td>Exists in user buffer</td>
</tr>
<tr>
<td>Role</td>
<td>Z_PEE_SN_DISPLAY</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction code</td>
<td>/PEU/MM02, SU53</td>
</tr>
</tbody>
</table>

This is the result of performing the transaction SU53.

The first part always shows you what the system checks, and the part below shows you the authorizations that are available for the user and in what role(s). You can see that the check on the authorization object S_TCODE is relevant in this case, and that it’s not available in the role Z_PEE_SN_DISPLAY for the transaction VA01, since the only transaction he may execute are /PEU/MM02 and SU53.
3. Testing the roles

During an implementation of for example the SAP CRM module, you will make up the necessary single and composite roles.

As I explained before you will create the following:

- A basic role, which will be assigned to every SAP user (it contains authorizations that are necessary for all end-users such as printing authorizations, possibly SU3 for maintaining his/her preferences, SU53 to check for authorization errors and so on.
- Single Roles: a single role usually contains the authorizations to perform a specific task such as creating a Marketing plan, or creating target groups in case of marketing and campaign management.
- Composite roles: composite roles could contain several single roles. Depending on how you want to setup your role definitions, you could decide in this case to create a composite role for a Marketing manager who will have several single roles.

During an implementation it is important that you test the complete functionality (customizing and developments) initially with a super-user who has the authorization profile SAP_ALL, to ensure that everything works as designed independent of authorization issues.

UNIT TESTING

Next you will start with the unit testing, where you will test every single role you have defined. This can be tested by the corresponding key-users (it is best to have the single roles tested by a key-user for the specific domain/module like FI, MM, SD and so on.

You should make sure not only that you are able to perform the tasks such as processing transactions in the system (positive testing), but also check that you are NOT able to perform things in the system you should not be allowed to (Negative testing).

Once you have done the entire unit testing you can start with the integration tests.

INTEGRATION TESTS

Once the unit tests are done, the roles must also be tested during the role integration test phase. The objective of the unit tests was to ensure that the role functions properly, meaning that the transactions contained in the role can be executed.

For integration testing, the responsibility usually lies in the hands of key users and/or power users who are well familiar with the business processes that need to be tested and who have a basic understanding of the authorization concept and checks.
Usually the key user will logon with a user who acts in a certain function such as marketing manager or master data administrator and who has assigned one or more composite roles to his user-id.

Again you will do positive and negative testing during this integration test. First you will make sure that all activities, transactions, reports and so on can be executed. Next you will ensure that for example a specific transaction can be executed, but for example only in display mode or for a certain organizational level (such as company code, sales organization).

Often you will see that a single role works as designed, but that the combination of several roles (assigned in a composite role) can cause security problems, since an authorization object can occur in more than 1 transaction and have different values in one single role opposed to another single role. Since the SAP system does the authorization check on the entire authorization profiles you have assigned to your user-id and adds up the authorizations you have, this could result in conflicts.

**Example:**

Suppose you have a single role Z_MARKETING_PLAN where you have values maintained for authorization object **CRM_CPG** where you are allowed only to DISPLAY marketing campaigns (Value 03).

In another single role Z_MARKETING_CAMPAIGN you also have this authorization object where you are allowed to create/change and display a marketing campaign.

Both single roles are assigned into the composite role Z_COMP_MARKETING.

Since you have the composite role assigned to your user-id and in one role you have all authorizations assigned for maintaining campaigns, this value will overrule the restriction, which was made in the single role Z_MARKETING_PLAN.
4. User Maintenance

With user maintenance, an administrator can create a user master record for every user, so that the user can log on the SAP System. You assign one or more roles to the user using the user master record to determine which activities are contained in the user menu and which authorizations the user has.

User master records are client-specific. You therefore need to maintain separate user master records for each client in your SAP System. You can use “Central User Administration” to simplify cross-client user administration. Maintaining centrally administered users is slightly different from user maintenance without CUA.

The overview in this book is restricted to user administration without CUA.

4.1. Creation of a User in the CRM system

The existence of a User Master Record is a prerequisite for logging on the SAP system, being R/3, CRM, BW, SAP Portal. To uniquely identify a SAP user, each user must have a unique master record, where personal data is saved and authorizations are granted by assigning (composite) roles. Technically, authorizations can also be assigned to users through single roles, composite profiles and single profiles. But from my point of view, the best way is assigning roles, and more specific composite roles.

Note: the procedure for creating users is the same in R/3, BW or CRM system. Below I explain this for the CRM System.

Procedure:

Start user maintenance via the menu:
Sap Menu ➔ Architecture and technology ➔ System Administration ➔ User Maintenance ➔ Users (SU01)

You can also directly access user maintenance via the command SU01.

The initial screen will look like this:
4.1.1. Display user information

To display a user, just type in the username and press the display button. If you don’t know the username by heart, you can look up any user by pressing the input-help button.

You get a popup screen with different search criteria.

You will see that there are different tabs on the user maintenance screen.

1) **Address Data**

Use the address data tab page to record a specific user’s address data. You must enter at least the user’s last name here. This information is meant to identify the actual employee (first name, last name, department, phone number, business address and so on).

The User ID can be up to 12 characters. When creating usernames it is useful to make up naming conventions to make the usernames transparent for maintenance purposes.

Example: First 8 characters of the last name, followed by the first two characters of the first name.

Pelssers Davy  ➔ PELSSERSDA
Clinton Bill  ➔ CLINTONBI
### 2) Logon Data

<table>
<thead>
<tr>
<th>Alias</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Group for Authorization Check</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Validity Period</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid from</td>
<td></td>
</tr>
<tr>
<td>Valid through</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dialog</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Service</td>
</tr>
<tr>
<td></td>
<td>Reference</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Data</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Number</td>
<td></td>
</tr>
<tr>
<td>Cost center</td>
<td></td>
</tr>
</tbody>
</table>
Use the Logon data tab page to maintain user information in the user master record. Here you can set the initial password (this is the password the end-user or employee needs to enter the first time he logs on to the SAP system – at that moment he will get a popup asking him to re-enter a new password of his own choice) and the user group. If necessary, the administrator can restrict the validity period of the user master record.

You also can assign an alias up to 40 characters to a user to specify more descriptive names.

**User Groups**

User groups are basically used to distribute user maintenance among several user administrators. Only the administrator that has authorization for a group can maintain users of the group. If you leave the field empty, the user is not assigned to any group. This means the user can be maintained by any user administrator.

You can create and maintain user groups within the user maintenance screen, via the menu path: *Environment → User groups → Maintain*.

**User Types**

The user type attribute indicates how the user’s access to the SAP system is defined. SAP distinguishes among the following user types:

- **Dialog user:**

  User type for exactly one interactive user (all logon types including Internet users). During a dialog log on, the system checks whether the password has expired or is initial. The user can change his or her password himself or herself. Multiple dialog logons are checked and, where appropriate, logged.

  Every employee should generally be defined as a dialog user.

- **Communications:**

  User type for dialog-free communication between systems (such as RFC users for ALE, Workflow, TMS and CUA):
A dialog logon is not possible
Whether the system checks for expired or initial passwords depends on the logon method (interactive or not interactive). Due to a lack of interaction, no request for a change of password occurs.

- **System:**

User type for background processing and communication within a system (internal RFC calls).

- A dialog logon is not possible
- The password change requirement does not apply to the passwords, that is, they cannot be initial or expired. Only a user administrator can change the password.
- Multiple logons are permissible.

- **Service:**

User type that is a dialog user available to a larger, anonymous group of users. Assign only very restricted authorizations for this user type.

- During a log on, the system does not check whether the password has expired or is initial. Only the user administrator can change the password.
- Multiple logons are permissible.
- Service users are user, for example, for an anonymous system access through an ITS service. After an individual authentication, an anonymous session begun with a service user can be continued as a person related session with a dialog user.

- **Reference:**

User type for general, non-person related users that allows the assignment of additional identical authorizations, such as for Internet users created with transaction SU01. You cannot log on to the system with a reference user. (You can deactivate this field in accordance with SAP note 330067.)
3) Defaults

You can use the defaults tab page to specify user defaults, such as the standard printer, the start menu, date and decimal formats and logon language. The user administrator does not have to maintain these settings necessarily, because users can also maintain their own user defaults via transaction SU3. In that case however, the users need to have this authorization in their basic user role assigned to their user master record.

4) Parameters

© 2007   Contact Author: davy.pelssers@contactoffice.net
Use the tab page ‘parameters’ to set or get parameters to save default values for fields, such as the company code, plant and so on.

Defining these preassigned values makes it easier for users to enter organizational units when they encounter the units again. Maintaining the parameter values can help to reduce mistakes during input.

**Set/Get parameter ID**

A field can be filled with proposed values from SAP memory using a parameter ID.

**Example**

A user only has authorization for company code 001. This company code is stored in memory at the beginning of a transaction under the corresponding parameter ID. Fields that refer to the data element are automatically filled with the value 001 in all subsequent screen templates.

**Dependencies**

A field in the screen template is only filled automatically with the value stored under the parameter ID of the data element if this was explicitly permitted in the Screen Painter.

### 5) Roles

Use the tab page roles to assign composite and/or single roles to assign the correct authorizations to the end-user or employee. You can also enter validity dates, supposing that you give authorization to someone on a temporary basis. By assigning a role to the user, the corresponding active authorization profile will automatically entered on the tab page profiles.
6) Profiles

On the profiles tab page, you assign manually created authorization profiles and therefore authorizations to a user. The generated profiles of the roles assigned to the user are also displayed here.

Example:
In the screenshot above you can see that for my User ID two standard SAP Profiles have been assigned (SAP_ALL and SAP_NEW). The other profiles are generated profiles which are automatically displayed on this tab page, because they correspond to the roles which are assigned to my user master record on the tab page ‘roles’.

Remember that end-users usually should not get those special profiles SAP_ALL and SAP_NEW as explained in chapter 2.3.6.

7) Groups

You assign the user to a user group on this tab page. This is purely a grouping that is suitable, for example, for mass maintenance of user data (transaction SU10). Assignments that you make on the ‘groups’ tab page are not used for authorization checks that are specified on the logon data tab page using the User Group field.
8) Personalization

On the personalization tab page, you can make person-related settings using personalization objects. You can call this tab page both in role maintenance and in user maintenance. Here you can preassign application parameters that include more parameters than the user parameters provided by transaction code SU3.

Other Functions

User Maintenance: Initial Screen

On the initial screen you have several buttons, which allow you to do the following things:
• Create a new User: you create a new user and fill out all the details as explained before!

• Delete a user: use the trashcan icon.

• Copy a user: when copying a user you type in the username that you want to copy, and press the copy button. You will get a popup asking you what parts you want to copy. In the ‘TO’ field fill out the new username.

![Copy Users](image)

• Lock/unlock a user: depending on the system profile parameters, it is possible that a user can for example mistype his password up to 3 times. At that moment the system will lock the user and he no longer is able to log on to the SAP system. With this button the user administrator can unlock the locked user!

• Change the password: with this button you can give a new initial password to the user!
4.1.2. Initial Data load for Users and Authorizations

You can imagine that for a large international company a lot of users need to be created and maintained. For a smaller company this can easily be managed by one system administrator in a manual way, but for very large user numbers this might be unfeasible. Therefore SAP provides technical aid. You can either accomplish this with an ABAP program that reads the data automatically, or with an external tool for creating and managing user master records based on the standard SAP BAPI’s such as:

- BAPI_USER_CREATE
- BAPI_USER_GET_DETAIL
- BAPI_USER_CHANGE
- BAPI_USER_DELETE

You can access the existing BAPI (Business Application Programming Interface) overview directory via the transaction code BAPI.
Alternatively you can also use SAP CATT (Computer Aided Test Tool). The advantage here is that you do not need any additional programming. You can launch the CATT via the transaction code SCAT.

4.2. Creation of a User in the SAP Enterprise Portal

Users in the portal and the CRM system are linked to each other, based on a single sign-on.
You give the same Username here
First logon to the portal by entering your username and password.
As User-administrator you will have the role “user_admin_role”.

Select the navigation link “User Administration”.

You will get the following navigational submenu:

By selecting the link “Users” you can create a new User.
Next, press the create button at the bottom of the screen. You will get a next screen with all information you entered.
As a next step you will want to assign Portal roles to this user.

To do this, you need to click on the navigation link “roles”.

There are two ways to assign a role to a user. Either you select a role, and edit it to assign new users. Or you can select a user, edit the user and assign a new role for this user.
Example: (edit a user to assign a new role)

I select the user “VERMASSENJ” that I just have created and press the start button.

You will get a result-list! In this case there will of course only be one entry.

Press the link “edit”. In the screen below you can see that this User has no roles assigned at this moment.

To assign a new role, search the role you want to add. By typing in “*”, you will get all available roles for Portal Usage.
As you can see two roles have been created, a marketing role and a sales role.

Select the role you want to add for the user (flag the checkmark before the role-name) and press the “add-button”.

In the role assignment, you will now see that this role has been added for the user VERMASSENJ.
Press the save button.

The first time that the user VERMASSSENJ will logon to the SAP Enterprise Portal, he will use the Username and password that you created in the CRM system (VERMASSSENJ with initial password ‘init’).

Now the system will ask him to change his password, since the one he entered was only an initial password.
4.3. Creation of an Employee in the CRM system

You already have created the User ID’s for your employees in the CRM system and for the SAP Enterprise Portal.

There are 2 steps left to do now. First you should create a Business Partner for each employee (account managers and/or marketing people) and link this business partner to the USER-ID.

Next you should assign this business partner in your organizational model.

Example:

In the previous chapters you already created VERMASSENJ (who is an account manager of the company XYZ) as user on the CRM system and on the SAP Enterprise portal.

Now you will create him as an employee in the CRM System.

Step1: Launch transaction “BP”.

Press the button ‘create person’.
In the next screen, select the role “employee”.

© 2007  Contact Author: davy.pelssers@contactoffice.net
The system will ask you if you want to create the business partner in the role “employee” or if you first want to save it in the general role.

Choose “CREATE”.

On the address data TAB, fill out the necessary data:
On the Tab “identification” you make the link between the Business partner ‘employee’ and the USER-ID.

After filling out these necessary data, you can save the business partner. The Business partner with number 409611 has been created.
4.4. Maintaining the Organizational Model

The last step in the process is to maintain the organizational model.

You can do this via the SAP-menu:

```
SAP menu
- Activities
- Marketing
- Sales
- Service
- Analytics
- E-Selling
- Interaction Center
- Master Data
  - PPOSA_CRM - Display Organizational Model
  - PPOMA_CRM - Maintain Organizational Model
```

or directly by launching the transaction PPOMA_CRM.
You will get following screen:

You have created the account manager Jef Vermassen as an employee (business partner) in the previous chapter. You want to assign him now to the organizational model.

Select therefore the position (a position is indicated with the icon 📌) to which you want to assign the employee.

Example:
To assign Jef Vermassen to the position “Account Manager”, right-click on this position, and select “Assign”.

© 2007  Contact Author: davy.pelssers@contactoffice.net
Next you get a popup, asking you to choose between a business partner or User. (Select Business partner!)

Select the business partner (employee) by name or Business Partner number (101).
After selecting Business partner 409611, I see that the organizational model is updated!
Jef Vermassen is now assigned in the org model.
5. CRM specific Authorizations

As I explained before the SAP authorization concept is not only valid for R/3 but also for CRM and BW for example. However every module has its own particularities. As an authorization administrator you might perfectly understand how the authorization concept works, but this does not guarantee a successful implementation of SAP CRM or SAP BW authorizations. In my experience, you only will be able to successfully apply authorizations in such a module, if you at least have a functional understanding of such a module. Furthermore, when using some authorization objects, you also need to perform some customizing steps.

Since I had the luck to be a functional consultant in all three aspects (R/3, BW and CRM) I can give you some highlights on the specific aspects.

5.1. Marketing and Campaign Management

Use
The processing of a marketing project is protected by an authorization check. With this authorization check, the system controls whether a user is allowed to create, change, display or delete a marketing project. The results of the authorization check relate to the entire marketing project (including the related marketing elements). It is therefore not possible to forbid a user from changing a campaign header and, at the same time, to allow them to make changes to a campaign element.

The following actions are protected by an additional authorization check:
- Entering plan values in marketing projects (activity 72)
- Changing general settings (marketing element overviews, assignment of template plans and so on): authorization object CRM_MPL_AD (activity 23)
## Authorization objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM_MPT</td>
<td>General authorization object <em>marketing plan</em> (without field-dependency)</td>
<td>The user has authorization to create, change, and so on, marketing plans</td>
</tr>
<tr>
<td>CRM_MPLRES</td>
<td>Authorization object <em>marketing plan</em> dependent on the person responsible</td>
<td>The user only has authorization to create, change, and so on, marketing plans for which particular persons are responsible</td>
</tr>
<tr>
<td>CRM_MPLAGR</td>
<td>Authorization object <em>marketing plan</em> dependent on the authorization group</td>
<td>The user only has authorization to create, change, and so on, marketing plans for which particular authorization groups are responsible</td>
</tr>
<tr>
<td>CRM_CPG</td>
<td>General authorization object <em>campaign</em> (without field-dependency)</td>
<td>The user has authorization to create, change, and so on, campaigns</td>
</tr>
<tr>
<td>CRM_CPGRES</td>
<td>Authorization object <em>campaign</em> dependent on the person responsible</td>
<td>The user only has authorization to create, change, and so on, campaigns for which particular persons are responsible</td>
</tr>
<tr>
<td>CRM_CPGAGR</td>
<td>Authorization object <em>campaign</em> dependent on the authorization group</td>
<td>The user only has authorization to create, change, and so on, campaigns for which a particular authorization group is responsible</td>
</tr>
<tr>
<td>CRM_CPGCTP</td>
<td>Authorization object <em>campaign</em> dependent on the campaign type</td>
<td>The user is only allowed to create, change, and so on, campaigns that have a particular campaign type</td>
</tr>
</tbody>
</table>
Activities

The following activities can be carried out for the authorization objects.

- 01 – Create
- 02 – Change
- 03 – Display
- 06 – Delete
- 72 – Plan

When a marketing project is created, the system checks first whether the user has authorization to create a marketing plan or campaign by checking the general authorization objects (CRM_MPT for marketing plans and CRM_CPG for campaigns). Without this authorization, the user cannot create the marketing project. Otherwise the user can go on to create the marketing project. When the project is saved, a final check is carried out for all authorization objects. If authorization for one of the authorization objects is missing, the marketing project cannot be saved. If a user opens a marketing project for which they have no change authorization, it is opened in display mode.

I will illustrate some examples below, but once you have seen a few examples and understand how they work, you will easily be able to use the further authorization objects based on their explanation in the above table!!

5.1.1. Role for creating marketing plan and campaign

I already explained that you could make use of standard delivered SAP roles, which you can copy and adjust according to your own wishes. Suppose that you don’t find a suitable role, in this case for creating marketing plans and campaigns, you can start creating your own single role.

I already explained the different approaches and concepts how to tackle such a task. (Check authorization objects used in transactions via SU24, check which authorization objects are needed via tracing – ST01 and so on).

If you go into the CRM system, you first look up the transaction code for creating a marketing plan. (If you are not familiar with the CRM system, then ask the functional CRM responsible for the correct transaction code)
You open your sap menu and open the correct folder:

Creating a marketing plan and/or campaign happens via the path:

**SAP Menu → Marketing → Marketing Planning and Campaign Management → Marketing Planner**

Or directly by using the transaction code CRM_MKTPL in the command field.

If you do not see the transaction codes next to the description, you need to put them on via the menu: **Extras → Settings → display technical names**
What I want to do first is create a role with all authorizations for a marketing manager, so that he will be able to create marketing plans, campaigns, trade promotions and deals. Furthermore he should be able to assign target groups to a campaign, release the campaign and execute the “target group to channel”.

Since I will test this in the SAP GUI, I can use a combination of SU53 and ST01 to analyze missing authorizations when testing my single role.

**Procedure:**

Start the profile generator and create the single role Z_MARKETING_CAMPAIGN.

Now add the transaction code CRM_MKTPL on the tab page menu. I also add SU53 in this stage, since I want to test with this role and therefore will need to evaluate authorization checks during the testing phase.

On the tab page ‘authorizations’ the default authorization objects are automatically added into the role.

In this stadium you already can create a test user “MKTMANAGER” to whom you will assign the single role for testing purposes.
Now by adding the transaction code CRM_MKTPL, you will notice that the following authorization objects are inserted automatically into my role Z_MARKETING_CAMPAIGN.

<table>
<thead>
<tr>
<th>Description</th>
<th>Authorization-object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Management: Set/Delete User Status</td>
<td>B_USERSTAT</td>
</tr>
<tr>
<td>Status Management: Set/Delete User Status using Process</td>
<td>B_USERST_T</td>
</tr>
<tr>
<td>Transaction Code Check at Transaction Start</td>
<td>S_TCODE</td>
</tr>
<tr>
<td>Authorization Object: CRM Marketing Business Object Campaign</td>
<td>CRM_CPG</td>
</tr>
<tr>
<td>CRM Marketing: Campaign Authorization Group</td>
<td>CRM_CPGAGR</td>
</tr>
<tr>
<td>CRM Marketing: Campaign Type</td>
<td>CRM_CPGCTP</td>
</tr>
<tr>
<td>CRM Marketing: Person Responsible for Campaign</td>
<td>CRM_CPGRES</td>
</tr>
<tr>
<td>Authorization Object CRM Marketing Business Object Deal</td>
<td>CRM_DLM</td>
</tr>
<tr>
<td>CRM Marketing: Marketing Plan Authorization Group</td>
<td>CRM_MPLAGR</td>
</tr>
<tr>
<td>CRM Marketing: Person Responsible for a Marketing Plan</td>
<td>CRM_MPLRES</td>
</tr>
<tr>
<td>Authorization Object CRM Marketing - General Settings</td>
<td>CRM_MPL_AD</td>
</tr>
<tr>
<td>Authorization Object CRM Marketing Business Object Marketing Plan.</td>
<td>CRM_MPT</td>
</tr>
<tr>
<td>CRM Marketing: Segment Type</td>
<td>CRM_SEGTYP</td>
</tr>
<tr>
<td>Authorization Object: CRM Marketing Business Object Trade</td>
<td>CRM_TPM</td>
</tr>
<tr>
<td>CRM Marketing: Campaign Authorization Group</td>
<td>CRM_TPMAGR</td>
</tr>
<tr>
<td>CRM Marketing: Campaign Type</td>
<td>CRM_TPMCTP</td>
</tr>
<tr>
<td>CRM Marketing: Person Responsible for Trade</td>
<td>CRM_TPMRES</td>
</tr>
</tbody>
</table>

To display the technical names (object class, authorization object and so on) you go via the menu: *Utilities → Technical names on*
On the tab ‘authorizations’ make sure you assigned all necessary authorizations for the listed authorization objects (you will see green lights on the status display).

You will see that for the authorization objects B_USERSTAT and B_USERST_T the restriction for the object type was already made by the system, being CPG (campaign) and MPL (marketing plan).

On the tab page ‘user’ assign the USER-ID you just created: MKTMANAGER and perform the user comparison.

Next you logon with the user MKTMANAGER and launch the transaction CRM_MKTPL.

Create a Marketing plan and next a Marketing campaign:

© 2007   Contact Author: davy.pelssers@contactoffice.net
Fill out the necessary details on the campaign level and assign a target group.

I got an authorization problem when trying to assign a target group on the tab page 'segments'. At that moment you can use SU53 to analyze the authorization problem.

**Remark:** this authorization object is a non-critical basis authorization for all users and is available in the standard SAP role: SAP_BC_ENDUSER
Therefore, when testing a single role, I advise you to give upfront also the basic role, which will be assigned, to all end users. This avoids having to put in the missing authorization object manually into the role you are creating now!!

Without having assigned the basic end user role, I had to manually add the following authorization objects:

1) S_GUI
2) S_ALV_LAYO (activity 23)
3) S_BDS_DS:
   - Business document service:
     - Class name = CGPL_DOCUMENTS
     - Class type = OT

4) S_BTCH_ADM (background administrator ID = Y)
5) S_BTCH_JOB:
   - Job operations = RELE
   - Summary of jobs for group = ‘ ‘
To add an authorization object manually into your role, you do the following:

Press the button ‘manually’.

![Change role: Authorizations](image)

You will get a popup asking you which authorization objects you want to insert manually.

You can then enter the missing authorization object, which you found by using SU53, and maintain the corresponding field values for it!

**Tip:** To make sure everything works in the correct way using your role, you can test in parallel the same process with a SAP_ALL user.

Once you have created the role with “all authorizations” for creating a marketing plan and/or campaign, you can start with making more restrictive roles based on the authorization objects in the list

5.1.2. Restrictions made based on person responsible

**Used authorization objects:**

- CRM_MPLRES for marketing plan
- CRM_CPGRES for campaigns
I only will illustrate one case by using authorization object CRM_MPLRES.

I start by making a copy of my single role, which contained all authorizations:
Make copy of single role Z_MARKETING_CAMPAIGN into
Z_RESPONSIBLE_MARKET.

As an example I filled out the person responsible Davy Pelssers for the Marketing plan ZMKTPL_01.

I also took two other marketing plans:
1) CR600_06 where I did not fill out any person responsible
2) CR600_05 where I used person responsible with BP number 405033

In my new single role Z_RESPONSIBLE_MARKET I entered the business partner number 405800 as field value for the authorization object CRM_MPLRES.
Test Results:

1) Marketing plan ZMKTPL_01: I can display and change the marketing plan
2) Marketing plan CR600_06: no display authorization
3) Marketing plan CR600_05: also no display authorization

Remark: In this example I only limited the authorization object related to the Marketing plan, so even I you are not able to display the marketing plan, you still are able to view the underlying marketing campaign!

5.1.3. Restrictions made based on Authorization Group

Used Authorization Objects:
- CRM_MPLAGR for marketing plan
- CRM_CPGAGR for campaigns

I will again illustrate one example by using the authorization object CRM_MPLAGR!

The first thing you need to do is creating an authorization group in customizing.

Using the transaction SPRO in the command field you can access customizing.

Menu Path in customizing:
SAP implementation guide → Customer Relationship Management → Marketing → Marketing Planning and Campaign Management → General Settings → Define Authorization group
I created the authorization group ZMKT (Authorization group MPL Borealis)

Now I add this authorization group to a marketing plan!

**Role creation:**

Again you can make a copy of the role Z_MARKETING_CAMPAIGN and create the new single role where you will make restrictions on the authorization object CRM_MPL_AGR.

© 2007   Contact Author: davy.pelssers@contactoffice.net
When assigning this new role to a user you will see that you only will be able to display marketing plans for which the authorization group ZMKT was maintained.

5.1.4. Restrictions made based on the Campaign Type

Used authorization object: CRM_CPGCTP

TO BE ELABORATED

5.1.5. Set Restrictions for assigning Attribute Sets and Attributes

This topic elaborates the functional use of Marketing attribute sets and Marketing Attributes and how you can set restrictions via authorizations.

5.1.5.1. Attribute sets and attributes –Functional info

This chapter illustrates what marketing attribute sets and marketing attributes are, what they are used for and how you can create and assign them to one or more business partners in your system.

5.1.5.1.1. What?

The first thing you need to know is what marketing attribute sets and attributes are.

An attribute set is used to group attributes created specifically within CRM Marketing together for a marketing-related purpose. Each attribute set therefore contains those attributes belonging to a business partner that are relevant for the purpose/application at hand.

Use

Attribute sets are used in applications such as CRM Internet Sales and CRM Telesales. In Internet Sales, they record marketing attributes for all business partners visiting Web shops, enabling the business partner to be assigned to a marketing profile. In CRM Telesales, they can be used to profile Telesales agents.

An attribute is a criterion used to describe an object.

Attributes with the following sources can be used for business partner segmentation in CRM Marketing:

1. Business partner master data, for example "age", "gender", "address"
2. BW master data/transaction data, for example "number of purchases per month"

3. Attributes created especially in CRM for marketing purposes, for example "hobbies". Such attributes are combined to create attribute sets.

![Diagram showing examples of attribute sets for Amazon.com and HerbaLife.](image)

5.1.5.1.2. **How can you create them?**

In the SAP menu in CRM (if you do not see the same menu, you can add the CRM_MENU in your SAP User account as default) you can create and display attribute sets and attributes using the following path:

**SAP Menu → Marketing → Segmentation of business partners → Marketing Attributes**

```
SAP Menu → Marketing → Segmentation of business partners → Marketing Attributes
- CRMD_PROF_CHAR - Maintain Attributes
- CRMD_PROFTEMPL - Maintain Attribute Sets
- CRMD_PROF_BP - Assign Attribute Values to Business Partners
```
5.1.5.1.3. MAINTAIN/CREATE ATTRIBUTES

Launch the transaction code CRMD_PROF_CHAR to have a look at how these attributes are configured.

The first thing you will see is the locator.

Here you can search for attributes based on several criteria such as description, data type and name.

You can also create new ones using the “create attribute” or “create by copying” buttons.

**EXAMPLE**

In this section you will learn how to create a marketing attribute.
Use the transaction code CRMD_PROF_CHAR to maintain/create new attributes.

In order to create a new attribute, press the button “create attribute”.
Creation of first attributes relevant for bookstore Amazon

- Create attribute “Genre”

- Create attribute “Author”

- Create Attribute “PRICE”
Creation of attributes for HerbaLife

I will only create two attributes for this case, since the purpose is to illustrate how we can restrict authorization for maintaining attributes and attribute sets for a business partner.

- Create Attribute “Gender”

<table>
<thead>
<tr>
<th>Attribute Value</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MALE</td>
<td></td>
<td>Male</td>
</tr>
<tr>
<td>FEMALE</td>
<td></td>
<td>Female</td>
</tr>
<tr>
<td>TS</td>
<td></td>
<td>Trans Sexual</td>
</tr>
</tbody>
</table>
- Create Attribute “active sports”

For classification purposes you will next group attributes for which you decide that they logically belong together into an attribute set.

5.1.5.1.4. MAINTAIN/CREATE ATTRIBUTE SETS

Launch the transaction code CRMD_PROF_TEMPL and have a look at how these attribute sets are configured.

Again you will see that the locator for this Object is launched.

Maintain Attribute Sets
In my example I will group together the attributes I created for both Amazon and HerbaLife.

To create a new attribute set, press the button “create Attribute Set”.

A) Create the attribute set for customers of Amazon

You can see I assigned the three attributes I created to this attribute set:
- GENRE
- AUTHOR
- PRICE_CAT

Furthermore, since I only want this kind of information to be assigned to Persons, and not organizations, I removed the “flag” for organizations.

Next, I also maintained the field “Maintn” which corresponds to the field BGRKP (relevant for authorization object C_KLAH_BKP) with the value “AAA” and the field “assign” which corresponds to the field BGRKL (relevant for authorization object C_KLAH_BKL) with the value AAA.

B) Create the new attribute set for customers of HerbaLife.
For this Attribute I maintained the Value “BBB” for both BGRKP and BGRKL.

**Authorization specific fields on this screen are:**

- Class Maintenance Authorization Group (C_KLAH_BKP) - BGRKP
- Classification Authorization Group (C_KLAH_BKL) - BGRKL

<table>
<thead>
<tr>
<th>Object</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>C_KLAH_BKL</td>
<td>Authorization for Classification</td>
</tr>
<tr>
<td>C_KLAH_BKP</td>
<td>Authorization for Class Maintenance</td>
</tr>
<tr>
<td>C_KLAH_BSE</td>
<td>Authorization for Finding Objects</td>
</tr>
</tbody>
</table>

**Class maintenance authorization group**

Authorization key that determines whether a user is allowed to maintain this class. This authorization must be defined in the user master record. The authorization object is BGRKP.

**Classification authorization group**

Authorization key: determines whether a user is allowed to assign objects to this class. This authorization must be defined in the user master record. The authorization object is BGRKL.
5.1.5.1.5. Assignment of Attribute sets to Business Partners

You can do this by launching the transaction code CRMD_PROF_BP.

Again the locator for this process is launched.

You can first search for an attribute set, select it and next choose the business partner to assign it to.

Example: Search for the attribute set we just created “Z_AMAZON”.

By double-clicking on an attribute set, you get the following screen:
Now you can go into change mode and maintain the attributes within this attribute set for this specific customer.

By double clicking on an attribute you will see the possible values you can maintain on the right hand side of the screen.

Maintain for each attribute a value(s).

You will see that per value you maintain, a line with the combination Attribute-Maintained value will appear on the left side of the screen. After having maintained the necessary attribute values, save the changes.
Now you can check if the assignment of this attribute set, and the maintenance of the attributes has been processed. Launch the transaction code BP (maintain business partner) and select the business partner 100016113.

Next, select the tab page “Marketing attributes”.

You can clearly see that the attribute set Z_AMAZON has been assigned to this business partner. If you look more detailed at the attribute values, you can also see that those are the ones I maintained and belong the attribute set Z_AMAZON.

By double clicking on the name of the attribute set, you will display the maintained attribute values, which belong to this particular attribute set.
If you would have pressed the “create assignment” button, you would directly go to this screen, and could have selected the business partner and attribute set using the Input Help function.

So far we have seen one way of assigning and maintaining an attribute set for a specific business partner. Another way of performing this action is by directly assign an attribute set on business partner level (assuming you have the right authorizations for this action).

Launch t-code BP, go to the marketing tab.

**Example:** I will assign the attribute set Z_HERBALIFE to the customer 100016113.

If you are in change mode, you should be able to see the different existing attribute sets that are available. By selecting Z_HERBALIFE and pressing the button “assign attribute set” you will see that it will be added in the list.

Next you can maintain values for the different attributes within this attribute set.
By double clicking on the line of the attribute, you will get a popup with “possible values” if they are maintained on the level of the attribute.

5.1.5.1.6. Authorization Setup

To grant different users authorization to maintain attribute sets, in the transaction PFCG, you assign the appropriate three-digit attribute set key under the authorization group BGKRL to the authorization object C_KLAH_BKL for assigning attribute sets and to the authorization object C_KLAH_BKP for maintaining attribute sets.

The important authorization objects are:

A) C_KLAH_BKL

**Definition**

Classification: authorization to classify or assign (C_KLAH_BKL)

This authorization group defines whether the user is allowed to assign objects to a class. The *Classification* authorization group allows you to restrict access to certain classes. When you create or change a class, you can enter an authorization group for classifying objects in the class. A user can only classify objects in the class if the user master record contains the authorization group you enter.

Example:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutCl</td>
<td>AAA</td>
</tr>
<tr>
<td>Actvt</td>
<td>03</td>
</tr>
</tbody>
</table>

In this example, the user is only authorized to display objects assigned to or classified in classes if the class concerned has classification group AAA.

This authorization group is checked in all functions for assigning objects to classes in the classification system and in master record maintenance functions.

**Defined fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Possible entries</th>
<th>Description</th>
</tr>
</thead>
</table>

© 2007  Contact Author: davy.pelssers@contactoffice.net
### B) C_CABN

**Definition**

This authorization object allows you to restrict access to functions for maintaining characteristics. This authorization object is automatically checked in the following functions:

- Create characteristic
- Change characteristic
- Display characteristic

**Defined fields**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Possible entries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>1</td>
<td>The user is allowed to create characteristics data.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>The user is allowed to change characteristics data.</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>The user is allowed to display characteristics data.</td>
</tr>
</tbody>
</table>

**Note**

In PPPI process management, authorization object C_PROCCHAR controls external system access to characteristics. Please ensure that the authorization for creating and changing characteristics and the authorization for external system access to characteristics are not given to the same person.

### C) C_KLAH_BKP

© 2007   Contact Author: davy.pelssers@contactoffice.net
**Definition**
Classification: authorization to maintain classes (C_KLAH_BKP)
This controls the authorization of a user to maintain a class.
This check is made in the following class maintenance functions:

- Create class
- Display class
- Change class
- Delete class

You can use the *Class maintenance* authorization group to restrict access to certain classes.
When you create or change a class, you can enter an authorization group for editing or displaying the class. A user can only maintain or display the class if the user master record contains the authorization group you enter.

Example

<table>
<thead>
<tr>
<th>Field</th>
<th>Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutCl</td>
<td>030</td>
</tr>
<tr>
<td>Activity</td>
<td>01 - 03</td>
</tr>
</tbody>
</table>

In this example, the user is only allowed to create, change, or display classes with the authorization group 030. The user is not allowed to delete classes with group 030, nor use the activities listed above on classes with other groups.

**Defined fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Possible entries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutGp</td>
<td>AAA-999, 000-999</td>
<td>Authorization group for class maintenance</td>
</tr>
<tr>
<td>Activity</td>
<td>01</td>
<td>Create</td>
</tr>
<tr>
<td>(Activity) 02</td>
<td>02</td>
<td>Change</td>
</tr>
<tr>
<td></td>
<td>03</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>06</td>
<td>Delete</td>
</tr>
</tbody>
</table>

**Note**
In the class list functions, the authorization to display (03) is checked for each class.

**5.1.5.1.7. Example Role**
In the previous chapters we have seen how to create and maintain attribute sets and attributes. We also learned how to assigned these attribute sets to a business partner via two different methods.

Now suppose you have created several attribute sets, but do want to place restrictions in who is allowed to assign and maintain particular attribute sets for business partners.

**Case:** I want my employees be able to assign only a restricted number of attribute sets. Therefore we maintained a classification (authorization group) on each attribute set.

Only attribute sets with classification AAA and BBB should be allowed for assignment by this group of employees.

To test and elaborate this I have created 3 single roles.

![Reference User for Additional Rights](image)

- **Z_ATTRIBUTES:**
  - Transaction code assigned: CRMD_PROF_BP

- **Z_BASIC_ENDUSER_ROLE:** copy of end user role SAP_BC_ENDUSER
  - This role allows me to perform SU53 and other non critical authorizations and was necessary to do the necessary checks

- **Z_CRM_BUSINESS_PARTNER:** copy of standard role SAP_CRM_BUSINESS_PARTNER
  - Includes the following transaction codes (actually I only needed the T-code BP for this test case)
→ I assigned this role to my test user in order to test the assignment of attribute sets via the transaction code BP.

Now the actual restrictions we want to test are maintained in my single role Z_ATTRIBUTES.

If we take a look at it you will see the following:

- **Cross-application Authorization Objects**
  - OBJECT S_TCODE
    - Transaction code: CRMD_PROF_BP

- **Classification**
  - OBJECT C_CABN
    - Activity: 01,02,03
  - OBJECT C_CLA_PROF
    - Activity: 03,23,78
  - OBJECT C_KLAH_BKL
    - Activity: 01,02,03
    - Classification authorization: AAA, BBB
  - OBJECT C_KLAH_BKP
    - Activity: 01,02,03,06
    - Class Maintenance Authorization: AAA, BBB
  - OBJECT C_TCLA_BKA
    - Class Type: *

The restrictions we want to realize are obtained by restricting the Objects C_KLAH_BKL and C_CKLAH_BKP.

Only attribute sets with classification AAA or BBB may be assigned and maintained.
Unit Test:

Method 1: Use transaction code CRMD_PROF_BP

POSITIVE TESTING
I use a new business partner 100016114 as business partner to assign the attribute set Z_AMAZON.

Display Attribute Values for a Business Partner

<table>
<thead>
<tr>
<th>Business Partner</th>
<th>Attribute Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>100016114</td>
<td>Z_AMAZON</td>
</tr>
</tbody>
</table>

This works fine. (In fact this is my positive test, since I should be allowed to assign this Attribute Set).
Double-check this via transaction code BP:

![Transaction Code BP](image)

You can see that the assignment has happened and the attribute values I maintained are also available.

**NEGATIVE TESTING**

Now I will try to assign an exiting marketing attribute set which does not have the classification AAA or BBB maintained for the same business partner.

First of all, you will notice that in the locator search I only will be able to search for attribute sets of classification AAA and/or BBB.
If I would search for attribute sets using "Z*" as search criteria with another User who has all authorizations in the authorization objects C_KLAH_BKL and C_KLAH_BKP I would see the following list.

If I directly search on the attribute set Z_CUSTOMER_INFO with the user who has restricted authorizations I do not get to see it.

**Remark:** You will not get an authorization message, but you can see via the user authorization check that you do not have the right authorization values.
The following authorization object was checked:

<table>
<thead>
<tr>
<th>Object</th>
<th>C_KLCL_BK Authorization for Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object class</td>
<td>CLAS Classification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>Classification authorization group</td>
<td>...</td>
</tr>
</tbody>
</table>

Available authorizations for the object in the master record:

<table>
<thead>
<tr>
<th>Object</th>
<th>C_KLCL_BK Authorization for Classification</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Authorization</th>
<th>T-C49201320 Available in User Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>T-C4920132</td>
</tr>
<tr>
<td>Role</td>
<td>Z_ATTRIBUTES</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>01, 02, 03</td>
</tr>
<tr>
<td>Classification authorization group</td>
<td>AAA, BBB</td>
</tr>
</tbody>
</table>

If I actually try to create the assignment by filling out the Customer number and the attribute set, and next press the enter button, you do get to see an authorization message!

**Maintain Attribute Values for a Business Partner**

<table>
<thead>
<tr>
<th>Business Partner</th>
<th>Attribute Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>100016114</td>
<td>Z_CUSTOMER_INFO</td>
</tr>
</tbody>
</table>

**Attributes in Attribute Set**

<table>
<thead>
<tr>
<th>Description</th>
<th>Attribute Value</th>
</tr>
</thead>
</table>

**Maintain Attribute Values for a Business Partner**

<table>
<thead>
<tr>
<th>Business Partner</th>
<th>Attribute Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>199916114</td>
<td>Z_CUSTOMER_INFO</td>
</tr>
</tbody>
</table>

You are not authorized for Z_CUSTOMER_INFO.
Method 2: Use transaction BP to assign and maintain attribute set for a business partner

POSITIVE TESTING

Launch transaction BP and select the customer 100016114.

Maintain business partners

As you can see, in method 1 during positive testing we already assigned the attribute set Z_AMAZON to this customer. Now we will assign the attribute set Z_HERBALIFE.

You do this by selecting Z_HERBALIFE and pressing the button “assign attribute set”. In the list of profiles the new entry will be added.
Now we will try to maintain the two attributes belonging to this attribute set, and save the business partner changes.

NEGATIVE TESTING

Now, this test is done very quickly. Since I do not get to see any other attribute set in my dropdown list, accept the ones belonging to the classification AAA or BBB, I obviously cannot assign such an attribute set this way.
### RELEVANT OSS NOTES:

<table>
<thead>
<tr>
<th>Note Number</th>
<th>Object</th>
<th>Description/Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>674696</td>
<td></td>
<td>Inherited characteristics are not displayed</td>
</tr>
<tr>
<td>601349</td>
<td></td>
<td>Authorizations Enhancement of attribute set: Up to now, you can only assign one authorization for attribute sets, that is, you cannot differentiate between editing an attribute set and a classification.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAPKU40001</td>
</tr>
<tr>
<td>581373</td>
<td></td>
<td>Maintenance of attribute Sets in several languages: Currently, attribute sets are only valid in the language in which they are maintained. (release 3.0 and 3.1)</td>
</tr>
<tr>
<td>357914</td>
<td></td>
<td>Class Create: Authorization Check: When you create a class via the BAPI or the API CLMA_CLASS_MAINTAIN, the system does not check the authorization of object C_KLAH_BKP (authorization for class maintenance from the authorization group).</td>
</tr>
<tr>
<td>369818</td>
<td></td>
<td>Authorization check BAPIs for reading class data</td>
</tr>
<tr>
<td>1002036</td>
<td></td>
<td>MKTATT: wrong F4 values for markt attribute set authorization group: TRX: CRM_PROF_TEMPL. While creating an attribute set we give two authorizations. One for maintaining the attribute set and one for assigning that attribute set to BP. But for both these authorizations F4 help is same.</td>
</tr>
<tr>
<td>446634</td>
<td></td>
<td>Authorization Check for Characteristic groups (prerequisite is note 456375) (valid for release 3.0)</td>
</tr>
<tr>
<td>585415</td>
<td></td>
<td>Authorizations for attribute sets (prerequisite is note 446634) (Valid for release 3.0 and 3.1)</td>
</tr>
<tr>
<td>456375</td>
<td></td>
<td>Profiles: Creating a characteristic group via template (Valid for release 3.0)</td>
</tr>
<tr>
<td>1021841</td>
<td></td>
<td>Authorization check for Marketing attributes: Even though you only have read-only authorization (authorization object C_KLAH_BKP), the system allows you to enter changes and only issues an error message when you try to save your entries. (Valid for release 5.1)</td>
</tr>
</tbody>
</table>
## 5.2. Business Partner Security

The table below shows the security-relevant authorization objects that are used by the SAP Business Partner.

### Standard Authorization objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Partner</strong></td>
<td><strong>Authorization Types</strong>: With this authorization object, you can define authorizations for any number of input fields in business partner maintenance. You determine which business partners may be maintained, depending on the field values. In Customizing you define an authorization type and specify the names of the fields that should be checked.</td>
</tr>
<tr>
<td>B_BUPA_ATT</td>
<td><strong>Field Groups</strong>: With this authorization object you can define authorizations for individual field groups in business partner maintenance. You thereby define which fields in business partner maintenance can be maintained or viewed by a user.</td>
</tr>
<tr>
<td>B_BUPA_FDG</td>
<td><strong>Authorization Groups</strong>: With this authorization object you define which business partners can be edited on the basis of the authorization group.</td>
</tr>
<tr>
<td>B_BUPA_GRP</td>
<td><strong>Roles</strong>: With this authorization object you define which Business Partner roles can be edited.</td>
</tr>
<tr>
<td>B_BUPA_RLT</td>
<td><strong>Relationship Categories</strong>: With this authorization object you establish which relationship categories can be processed.</td>
</tr>
<tr>
<td>B_BUPR_BZT</td>
<td><strong>Relationship Field Groups</strong>: With this authorization object you can define authorizations for individual field groups in business partner relationship maintenance. You thereby define which fields of the business partner relationship can be maintained or viewed by a user.</td>
</tr>
<tr>
<td>B_BUPR_FDG</td>
<td><strong>Payment Cards</strong>: You can use this object to regulate authorization for display and/or maintenance of payment card master data. With this object, you control the authorization for the encryption or decryption of payment card data.</td>
</tr>
<tr>
<td>B_CARD_SEC</td>
<td><strong>Authorization Encryption Card Master</strong>: You can use this object to regulate authorization for display and/or maintenance of payment card master data.</td>
</tr>
<tr>
<td>B_CCARD</td>
<td><strong>Payment Cards</strong>: You can use this object to regulate authorization for display and/or maintenance of payment card master data.</td>
</tr>
</tbody>
</table>
Data Storage Security

The data of the SAP Business Partner is stored in the database of the SAP System. The security of data in SAP Business Partner is guaranteed by the general authorization concept of SAP Business Partner, which uses the authorization objects that were mentioned in the table above!

The security of sensitive data such as payment cards can additionally be protected by using encryption. (See IMG→ Cross application components→ Payment Cards→ Maintain Payment Card Type).

5.2.1. Functional insight into Account and Contact Management

All information in this chapter is based on the CRM 4.0 release. Some functionalities and concepts might not be available in previous releases.

In this chapter I will try to elaborate the most important concepts of the SAP CRM Business Partner that everyone needs to understand in order to be able to comprehend and set up business partner security.

Although I briefly mention all concepts, which you need to understand for SAP CRM security, related to SAP Business partners, I advise everyone to follow the CR100 course, provided by SAP. There you get the complete overview of the CRM basics and also do exercises, which might make things more understandable.

If you want to set up Business partner security in SAP CRM, these are the things you want to know.

1) SAP CRM Business partners
2) Business Partner Roles and Categories
3) Business partner Classification
4) Partner Functions
5) Business Partner Relationships
6) Data sets and field groups
7) Partner Processing

Account und Contact Management allows you to manage and maintain your accounts and contact persons. In the context of Account and Contact Management accounts can be understood as firms or organizations, but also persons and groups that have a relationship with your firm as customers or prospects. The terms account and business partner are used synonymously below.

In CRM Enterprise, business partners can be persons, organizations, or groups of persons or organizations in which your company has a business interest.
In **CRM Mobile Sales**, business partners can be organizations or persons. Contact persons in CRM Mobile Sales correspond to persons in CRM Enterprise.

The following basic elements are available to you within the business partner data:

### Business Partner Concepts

<table>
<thead>
<tr>
<th>People-Centric UI</th>
<th>SAP GUI</th>
<th>Mobile Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business partner category</td>
<td>The data available for your business transactions depends on the <strong>business partner category</strong>.</td>
<td></td>
</tr>
<tr>
<td>BP role</td>
<td>A business partner can take on different <strong>business partner roles</strong> that allow you to have different views of the business partner data, according to the business function.</td>
<td></td>
</tr>
<tr>
<td>Data set:</td>
<td><strong>Data sets</strong> offer you the flexibility to build the BP roles that your company requires for its business transactions.</td>
<td>In <strong>CRM Mobile Sales</strong>, data sets are the information that you enter into required fields on the user interface. Almost all this data is exchanged with the CRM Server.</td>
</tr>
<tr>
<td>BP relationship</td>
<td>A <strong>relationship</strong> connects two business partners and is characterized by the <strong>business partner relationship category</strong>.</td>
<td>In <strong>CRM Mobile Sales</strong>, when a relationship is created between two business partners, business partner 2 becomes a contact person of business partner 1.</td>
</tr>
<tr>
<td>BP group hierarchy</td>
<td>You can depict the structure of an organization using the <strong>business partner group hierarchy</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

© 2007  Contact Author: davy.pelssers@contactoffice.net
**Business Partner Category**

**Definition**

The business partner category denotes whether a business partner is a natural person (private individual), organization (legal person/entity or part of a legal entity, such as a department), or a group.

**Usage**

When you create a business partner, you have to select a business partner category. Depending on the business partner category, a certain set of fields has to be filled with data. For example, if you are creating a business partner as an organization, you can enter the legal form and industry, whereas in the case of a person you can enter first names, name affixes, gender and so on.

**Structure**

The standard business partner categories are:

- Natural person (private individual)
- Organization (e.g. company, department in a company, club, association)
- Group (e.g. married couple, shared living arrangement)

It is not possible to create any other business partner categories. You cannot alter the business partner category at a later stage.

**Example:**

By launching the transaction code “BP” you will see the following screen:

![Image of Maintain business partners screen]

As you can see there are three buttons available for the creation of a business partner.
- Person
- Organization
- Group

Each of these buttons represents the creation of a business partner in a certain business partner category. It seems obvious to me whether you would want to create a business partner as a person or as an organization, so therefore I will not go deeper into this matter. The most important consequences of this choice are:
- You will see **different input fields** appear on the screen when creating a business partner in a certain category.

**Example**: a person will have the fields First Name/Last name available whereas an Organization uses other fields such as Name Org1 and Name Org2.

**Organization**:

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>CARREFOUR SCE ENTRETIEN/ 751</td>
</tr>
</tbody>
</table>

**Person**:

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>0002 Mr.</td>
</tr>
<tr>
<td>First Name</td>
<td>Davy</td>
</tr>
<tr>
<td>Last Name</td>
<td>Pelssers</td>
</tr>
</tbody>
</table>

- Certain roles can only be maintained for a specific business partner category.
Display View “BP Roles”: Details

Here you can see an example of the standard role BUP001 (contact person). Since this role is flagged as valid only for the Business Partner Category “Person”, you will notice that it is not available when creating a business partner of the category “Organization”.

- This also has an impact on partner processing in business activities.
- In Marketing and Campaign Management you will also see that when creating target groups, you need to make a choice if you want for example to select all organizations (customers) or the contact persons of those organizations.
- …

Business Partner Roles

Business partners are created only once in your system, but they can have different roles.

- A business partner might be related to your company from different point of views. It depends on the business process that this business partner is involved in, which kind of information about him is needed.

For example, for the goods delivery transaction, information about the shipping and delivery conditions is required; for the sales order transaction, delivery dates and payment conditions are relevant.

- You can maintain a business partner in more than one role. A business partner in the SAP CRM system is at least created in the role “Business partner (general)”. General information that is valid for all roles is maintained on this level.
• Each partner role contains various data sets:
  - General data
  - CRM specific data
  - Relationships
  - ....

**What does this mean concrete?**

Let's have a look at the business partner creation screen. By launching the transaction code ‘BP’ you will see the following screen:

As explained in the previous topic, you have three buttons to create a business partner, determining the business partner category in which you will create him.

→ Either create a person, organization or group

Let us create an organization in the role BUP002 (prospect):
By immediately choosing to create the business partner in the role prospect (for that matter in any other role which is not the business partner (general) role) the system will come up with a pop-up asking you the following:

Should you already have maintained general information for the business partner (before choosing another role than the Business partner (general) you can save this information first. In this way the already entered information is not lost when maintaining the business partner in the other role.

If you did not maintain general information, and immediately chose to create the business partner in the role prospect, than you press the create button, and start maintaining information for this role. All general information is then automatically stored in the role Business partner-general.

Now depending on the role that you chose, you will see different tab pages that are available:

Again, what kind of information you will be able to maintain depends on both the business partner category and the role you are creating the business partner in.

**Definition of roles**

If you want to look at the definition of the standard delivered roles by SAP, you can launch the transaction code ‘BUPT’.

This will launch the SAP Easy Access menu for Business partners.
To have a look at the Business partner roles, you will choose transaction code **BUSD**.

**Change View "BP Roles" : Overview**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BP0000</td>
<td>Business Partner (General)</td>
<td>Business Partner (Gen)</td>
</tr>
<tr>
<td>BP0001</td>
<td>Vendor</td>
<td>Vendor</td>
</tr>
<tr>
<td>BP0002</td>
<td>Bidder</td>
<td>Bidder</td>
</tr>
<tr>
<td>BP0003</td>
<td>Portal Provider</td>
<td>Portal Provider</td>
</tr>
<tr>
<td>BP0004</td>
<td>Plant</td>
<td>Plant</td>
</tr>
<tr>
<td>BP0004</td>
<td>Purchasing Company</td>
<td>Purchasing Company</td>
</tr>
<tr>
<td>BP0005</td>
<td>Billing Unit</td>
<td>Billing Unit</td>
</tr>
<tr>
<td>BP0006</td>
<td>Contact Person</td>
<td>Contact Person</td>
</tr>
<tr>
<td>BP0007</td>
<td>Prospect</td>
<td>Prospect</td>
</tr>
<tr>
<td>BP0008</td>
<td>Employee</td>
<td>Employee</td>
</tr>
<tr>
<td>BP0009</td>
<td>Organizational Unit</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>BP0010</td>
<td>Internet User</td>
<td>Internet User</td>
</tr>
<tr>
<td>BP0011</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>BP0012</td>
<td>Sold-To Party</td>
<td>Sold-To Party</td>
</tr>
<tr>
<td>BP0013</td>
<td>Ship-To Party</td>
<td>Ship-To Party</td>
</tr>
<tr>
<td>BP0014</td>
<td>Payee</td>
<td>Payee</td>
</tr>
<tr>
<td>BP0015</td>
<td>Bill-To Party</td>
<td>Bill-To Party</td>
</tr>
<tr>
<td>BP0016</td>
<td>Competitors</td>
<td>Competitors</td>
</tr>
<tr>
<td>BP0017</td>
<td>Consumer</td>
<td>Consumer</td>
</tr>
</tbody>
</table>

In the screenshot above you see the standard SAP delivered roles.
If we take a look at for example the role BUP002 (Prospect), you will see:
Which roles your company will use, you can maintain in customizing (SPRO):

*SAP IMG ➔ Cross Application Components ➔ SAP Business Partner ➔ Business Partner ➔ Basic Settings ➔ Business Partner Roles*

Especially important here is the option where you can flag for which business partner category the role is valid.

If you want to know what the other fields serve for, place your mouse on the field, press F1 for technical help and the SAP Help info will come up.

**Remark:** Remember NEVER to change standard delivered roles!

If you need to make customer changes, just copy the existing role that you need to change into a Z or Y role and make the necessary settings there.

© 2007  Contact Author: davy.pelssers@contactoffice.net
This has an impact on the dropdown list for choosing the business partner role when creating a business partner via transaction code BP.

**Link Role and corresponding Data Sets**

In order to see the available data sets for this role, select this option in the dialog structure!

For the role Prospect, these are the ones available in standard SAP.

Data Sets are building blocks for defining business partner roles in the business processes of your enterprise.

**Link Data Sets and field groups**

If you now want to look at the details of such a data set, you will have to look up this information in customizing (SAP).
Select the role you want to analyse and press the button “Field Grouping”.

In this screen you see the different Data Sets that are available for the role Prospect. Each data set contains one or more field groups. For each field group you can decide whether it should be hidden, mandatory and so on.

To look at the different data sets, just double click on the data set on the left side of the screen and the corresponding field groups will appear on the right hand side of your screen.

**Link Field Group - Fields**
Now the last thing you might want to do is have a look at a specific field group to see which fields are contained in the field group.

**Check two field groups:**
- 63: Address: Street (Belonging to Data Set BUA010 – addresses)
- 8: Forms of address (belonging to Data Set BUP010 - Central Data)

Use the transaction code **BUS2** to look at the field groups and the corresponding fields.

© 2007   Contact Author: davy.pelssers@contactoffice.net
Customer data is divided according to business points of view into different classes in SAP CRM and SAP R/3. Customer data can represent customers, prospective customers, competitors or consumers, for example. This classification is realized in different ways in the data models of SAP business partner and R/3 customer master.

In SAP R/3 customer master, the R/3 account group controls the classification, whereas in SAP CRM the classification is controlled via an independent attribute called classification in SAP business partner, hereafter called the CRM classification.

**R/3 Account Group**

Every R/3 customer master has to be assigned an account group that determines the properties of business partners. These include in particular:

- Master data fields
- Number ranges
Specific functionality for sales and distribution

There are more than 20 different account groups available in the standard SAP R/3 delivery.

**CRM Classification**

You can assign one or more classifications to each business partner. These determine:

- Master data fields
- The number ranges are not directly assigned to the CRM classification. The number range is determined by the so-called business partner grouping. When creating a business partner you can assign a grouping to the business partner. If you do not assign a grouping, SAP CRM uses the specified standard grouping for internal or external number assignment.
- Specific functionality

The following classifications are available in SAP CRM:

<table>
<thead>
<tr>
<th>CRM Classification</th>
<th>Representation in PIDE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer: Organization</td>
<td>A</td>
</tr>
<tr>
<td>Customer</td>
<td>B</td>
</tr>
<tr>
<td>Prospective Customer</td>
<td>C</td>
</tr>
<tr>
<td>Competitor</td>
<td>D</td>
</tr>
<tr>
<td>Consumer: Person</td>
<td>E</td>
</tr>
</tbody>
</table>

You can assign more than one classification when creating a business partner. The classifications obey the following hierarchy.

Consumer > Customer > Prospective Customer > Competitor

For example, if you assign the classifications Consumer and Customer to a business partner, the leading classification in the mapping process to R/3 account groups in SAP R/3 is the classification Consumer.

Mapping rules have to be set between the CRM classification and the R/3 account group when exchanging data between R/3 customer master and business partner in SAP CRM. These mapping rules are defined in both directions, that is, SAP R/3 to SAP CRM and vice versa. You define these mapping rules in the transaction **PIDE** in SAP R/3.

Specifying the number assignment strategy that you choose for exchanging data between SAP R/3 and SAP CRM plays a deciding role in setting the mapping rules.
Classification on Business Partner level in SAP CRM:

Business Partner Functions and relationships

**Definition**

**Relationship categories**, such as *has the contact person*, are the definitions of business partner relationships, the business-relevant connections between partners.

**Partner function categories**, such as *contact person*, are hard-coded classifications representing sets of business responsibilities.

**Use**

Relationship categories are used in business partner master data. Partner function categories are also used in master data (for sales area-specific partner function assignments), and additionally in transactions and in Customizing for partner processing.
Relationship categories and partner function categories closely correspond to each other. This correspondence allows the system to use business partner master data in transaction processing. Using master data in transaction processing is a crucial part of partner determination.

For example, when you create the relationship "Johnson Electronics has the contact person David Wilson", the system knows that, in transactions where Johnson Electronics is the sold-to party, David Wilson performs the partner function contact person.

**Display Available Relationship Categories**

Launch the transaction code BUBA in order to have a look at the standard delivered ones.

<table>
<thead>
<tr>
<th>BUBA</th>
<th>Relationship Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUB001</td>
<td>Contact Person Relationship</td>
</tr>
<tr>
<td>BUB002</td>
<td>Activity Partner Role</td>
</tr>
<tr>
<td>BUB003</td>
<td>Shared Living Arrangement</td>
</tr>
<tr>
<td>BUB004</td>
<td>Marriage</td>
</tr>
<tr>
<td>BUB006</td>
<td>Alias (Identification)</td>
</tr>
<tr>
<td>BUB018</td>
<td>Family Relationship</td>
</tr>
</tbody>
</table>

When taking a more detailed look at for example the relationship category BUR001 (contact person relationship) you will see the following:
Since a relationship is always created between 2 business partners, you will have a description, which will be different from each business partner’s point of view.

Again, if you want to know more about the meaning of the different field options, use the F1 technical help to learn more about this.

**Creating relationships between business partners:**

Business partner relationships are created or maintained using the transaction code BP.

When creating or changing a certain business partner, you can also create a relationship for this business partner using the button “Relationships”.

After pressing the button relationships, you jump into the screen where you actually will be able to maintain them:
Partner Functions

Partner functions describe the persons and organizations with whom you maintain business relationships and who are therefore contained in your business transactions.

You can define your own functions. However the system already contains frequently used partner functions in service processes, like sold-to party, ship-to party, contact person or responsible employee.

Look at existing Partner functions or define new ones:

SPRO → Customer Relationship Management → Basic Functions → Partner Processing → Define Partner Functions.

When you define a new partner function in the Customizing activity Define Partner Functions, you assign it to a partner function category. The system then enters the corresponding relationship category automatically, if there is a relationship category hard-coded to correspond to this partner function category. If you enter a partner function category that is not hard-coded to correspond to a particular relationship category, you must enter the relationship category yourself. If you leave the field for the relationship category empty, the system cannot use business partner master data to determine partners for the new partner function because it does not know what relationship to look for. In
this case, for transaction processing, you must set the system to determine the partner from a source other than business partner master data, or enter it manually.

If we take look at a business transaction in the system, you will see where partner functions are used. When creating a lead in the system I will see the following screen:

The partner functions available on the details tab page are the ones that are defined in the User Interface Settings definition of your partner determination procedure.

The declaration of ALL partner functions that can be used in your business transaction type is done in the section „partner functions in Procedure“.

This brings us to partner processing in business transactions.
Partner Processing

Purpose

Partner processing controls how the system works with business partners in transactions. It ensures the accuracy of partner data in transactions by applying rules you specify in Customizing, and it makes users work easier by automatically entering certain partners and related information, like addresses.

One of the most important aspects of partner processing is partner determination, the system’s ability to automatically find and enter the partners involved in a transaction. In most transactions, the user manually enters one or more partners, and the system enters the others through partner determination. Various sources of information make partner determination possible; two of the most important are business partner master data and organizational data.

Define Partner Determination Procedure

In Partner Determination Procedures, you specify which partner functions are involved in a transaction, assign access sequences to the functions the system should determine automatically, and set other rules for working with partners in transactions.

SPRO → Customer Relationship Management → Basic Functions → Partner Processing → Define Partner Determination Procedure

Display View "Partner Determination Procedures": Overview

For every Partner function that you defined in your partner determination procedure, an access sequence is used to determine where the system should look to automatically fill in the correct business partner for this partner function.
By selecting the partner function, and look at the details, you can see the used access sequence.

**Define Access sequence**

In **Access Sequences**, you specify the sources of data the system uses for automatic partner determination, and the order in which it checks those sources.

![Diagram showing the Partner Determination Access sequence](image)

**SPRO ➔ Customer Relationship Management ➔ Basic Functions ➔ Partner Processing ➔ Define Access Sequences**

© 2007  Contact Author: davy.pelssers@contactoffice.net
In the previous screenshot you saw that the access sequence used in the Partner Determination procedure for Leads (00000016) for the partner function “contact person” is the access sequence 0002 “from activity partner”.

<table>
<thead>
<tr>
<th>Dialog Structure</th>
<th>Access Sequences</th>
<th>Individ. Accesses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 5.2.2. General role SAP_CRM_BUSINES_PARTNER

This standard role allows you to maintain business partners master records and business partner group hierarchies, as well as displaying the business partner Cockpit. In addition, two mini-apps for business partner search and birthday list are assigned to this single role.

You can make a copy of this standard role and assign it to people who need to have full authorization to create and maintain business partners in the system.

### 5.2.3. Restrictions for certain input fields based on Authorization Type

**Authorization object used:** B_BUPA_ATT

**Procedure:**

First, in customizing you define an authorisation type and specify the names of the fields that should be checked!

*SAP Implementation Guide > Cross-application components > SAP Business Partner > Business Partner > Basic settings > Authorization management*
As an example I created the authorization type ZADDRESS with two fields.

Look up Screen Field for business partner information.
Launch business partner maintenance via the transaction code ‘BP’. Next select the field for which you want to know the screen field name.

*Example:*
I want to know the screen field name of the field ‘Search term 1’:

If you want to know the name of a certain screen field, when displaying a certain Business Partner, you place your mouse on top of the field, and press F1. Next, in the performance assistant, press the button.
### Search Term 1 for Business Partner

#### Use

Denotes the term that you define for a business partner, and via which you can restrict the search for a business partner in the business partner search or in the locator.

### Technical Information

- **Screen data**
  - Program name: SAPLBU00
  - Screen number: 1110

- **GUI data**
  - Program name: SAPLBUFA_DIALOG_JOEL
  - Status: SCREEN_1000

- **Field data**
  - Transparent table: BUT000
  - Field name: BU_SORT1
  - Data element: BU_SORT1
  - DE supplement: 0

- **Field description for batch input**
  - Screen field: BUT000.BU_SORT1
  - Program name: SAPLBUS_LOCATOR
  - Screen no.: 3800
In my new role Z_CRM_BUSINESS_PARTNER_AUTH_TP, which is a copy of SAP_CRM_BUSINESS_PARTNER, I will maintain the values for the authorization object B_BUPA_ATT.

This means that the person with this role should only be able to create, change of display business partners that have the city 'LEUVEN' and postal code 3000.

I now searched for a business partner that did not live in leuven, and selected it to display.
I get the following message:

5.2.4. Restrictions for certain field groups

Authorization object used: B_BUPA_FDG

Example:

Create a new single role Z_BP_FIELDGRPS as a copy of the standard role SAP_CRM_BUSINESS_PARTNER.

In this role I will maintain the authorisation object by selecting out of the InputHelp:
For example; I selected the following field groups with display only:

- 0115: address: internet mail address
- 0005: Search terms

In customizing you first define which Field Groups need to be checked for authorisations:
Here I put in two field groups as an example:

**Change View "Field Groups for Authorization": Overview**

Now in my role, I will maintain the parameters for those field groups!
Select in your role the authorization object B_BUPA_FDG and use the input help to select your field groups.
I select the two fieldgroups I just defined in customizing: search terms & internet mail address. Next I give the authorization value I select the two fieldgroups I just defined in customizing: search terms & internet mail address. Next I give the authorization value "display" for the authorization field activity.

When finished, it will look like this:

This should mean that I am able to create, change and display all business partners, but not change or maintain those specific fields when I have this new role assigned to my UserID!

Result:

© 2007   Contact Author: davy.pelssers@contactoffice.net
5.2.5. Restrictions based on Authorization Group

**Authorization object used:** B_BUPA_GRP

**Procedure:**

Concrete this means that you first define an authorisation group in customizing, next assign on business partner level the authorisation group. In the role, you will restrict the authorisation object with the authorisation group you created in customizing.
Result: the user will only be able to change/display business partners for which the authorisation group is maintained!

Example:

1) Creation of an authorization group in Customizing:

*SAP Implementation Guide → Cross-application components → SAP Business partner → Business Partner → Basic Settings → Authorization management → Maintain Authorization group*

I create the authorization group ZEMP, which will be maintained for all Business partners in the role Employee. Only the HR responsible will be able to maintain the employee data in the system. Others will only be able to display the maintained information.

Now, I can maintain on business partner level, this authorisation group. In this case, I will do this for employees, which I only want End-users to be able to display and not change!!

On the Tab 'control data' I fill in the authorisation group:

In the Role I will maintain the following:

Role created: Z_CRM_BUSINESS_PARTNER_AUTHGRP as a copy of SAP_CRM_BUSINESS_PARTNER.

I change the authorisation object: B_BUPA_GRP and maintain the following:

© 2007  Contact Author: davy.pelssers@contactoffice.net
If I now select the business partner 409582 for which the authorisation group is maintained, I get the following:

**Display Person: 409582, role Employee**

Business Partner 409582  
Display in Role BUP003 Employee

I can only display this employee!

### 5.2.6. Restrictions for maintaining certain Business Partner Roles

For this topic I am brainstorming for which scenarios companies might want to restrict people in displaying, changing or creating Business Partners in a certain role.

**Scenario 1**

First of all, as I explained before, a business partner is created at all times in the role “business Partner (general). When creating the partner, you have the option to first create him in the general role and save the information, and next also maintain him in the other necessary roles. This general role only exists for the purpose of storing general information that is valid for all other roles. During business transaction processing however you normally will not be using Partners that only have the general role maintained. You might probably want to create a lead or activity for a prospect or customer, create a sales order for a consumer, for which sales area related data should be maintained on the master data of the business partner. This kind of information is not available in the general business partner role. So unless you would maintain a business partner also in another role then the general role, we might consider it as master data pollution.
Therefore a company could decide that employees that are responsible for the creation of prospects and employees directly should maintain a business partner in the role prospect or customer and not have the option just to maintain him in the general role, leaving the employee the chance to forget maintaining the necessary sales area data.

I have not tested this scenario, but if you think about it, you might not be able to use the authorization object B_BUPA_RLT for this purpose. Suppose you would set the following combinations:

**Activity:** 03 (Display) and **BDT: Object Part:** 000000 (Business Partner General)  
**Activity:** * and **BDT: Object Part:** BUP002 (Prospect)

You would expect that the employee would only be able to display a business partner in the general role, and furthermore create or change prospects. If you would try to create a prospect with such a combination, you will not succeed, since the system will complain about the fact that you are not able to maintain the business partner in the general role (remember I told you that every business partner ALWAYS needs at least to be created in this role?).

Another solution for this is making use of customizing options for field groups.  
→ SAP IMG→ Cross–Application components→ SAP Business Partner→ Business Partner→ Basic Settings→ Field Groupings→ Configure field attributes per BP Role

### Change View "Field Group BP Role": Overview

<table>
<thead>
<tr>
<th>Field Grouping Object Part</th>
<th></th>
</tr>
</thead>
</table>
| Obj...Descrip
| 000000 Business Partner (General) |

Select the role “business partner (general)” and press the button Field Grouping. If you set for each data set the field groups to “display”, you would obtain the required result.

<table>
<thead>
<tr>
<th>Data set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUPA17</td>
<td>Addresses</td>
</tr>
<tr>
<td>BUP010</td>
<td>Central Data</td>
</tr>
<tr>
<td>BUP020</td>
<td>Bank Details</td>
</tr>
<tr>
<td>BUP030</td>
<td>Payment Cards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field group</th>
<th>Description</th>
<th>Hide</th>
<th>Req entry</th>
<th>Opt entry</th>
<th>Display</th>
<th>Text spec</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2</td>
<td>Address: Language Key (CE)</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B3</td>
<td>Address: Street</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B4</td>
<td>Address: P.O. Box</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>B5</td>
<td>Address: City</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**Scenario 2**
Another most likely scenario is that your sales reps or sales manager might be able to create prospects and customers, but certainly no business partners in the role employee. Creation and maintenance of employees might be a specific job done by the HR responsible or a dedicated CRM person who not only creates the employees, but also maintains the organizational model and the assignment of employees to the org. model.

**Scenario 3**
I can also assume that a company might want the following:

- Marketing manager/assistant:
  - Can only display prospects and customers but not change them
  - Is not allowed to create/change/display employees

- A Sales rep/Sales Manager:
  - Can create/change/display prospects and customers
  - Is not allowed to create/change/display employees

Anyway, you should get the picture and realize that restricting business partner access based on roles might be necessary.

As an example I will elaborate the *role for the Sales Rep*:
Just make a copy of the standard role SAP_CRM_BUSINESS_PARTNER and create for the role Z_CRM_BUSINESS_PARTNER and assign this to a new test-user.

Now you will restrict the authorization object B_BUPA_RLT.

To quickly test if this works I just deselected the role “Employee” out of the F4-input help for maintaining the values.
For the activity I used “full authorization”. Now if you logon with this test-user and try to create a business partner in a certain role, you will see that the role Employee is not in this list. 

Hint: You should try this by creating a business partner of the category “Person”, since the role employee is only available for creation of persons.

Create Person

© 2007  Contact Author: davy.pelssers@contactoffice.net
In the above screenshot you see that the role employee is not available for creation. So far, you covered the creation part. Now, you should also check whether this test-user is able to display or change an existing employee.

Use the business partner search function (based on Role) to look up an employee.

Press F4 and in the option list select “Partner by Role”.

© 2007  Contact Author:  davy.pelssers@contactoffice.net
Select the Role “BUP003” and restrict the maximum hits to 10. We don’t want to wait too long to only check the first employee that comes up.

Select one employee out of the list.

Result: You WILL in this case be able to see the Employee, but only his general information, which is maintained on the role “business partner-general”.

If you would try to see the information stored on the role “employee”, you will see that this role cannot be selected.

If I would look at this business partner with another user, which does not have the restriction for seeing employees, you would see the following:

In my opinion, since you can still see the general information about the employee, this is not really a good strategy of protecting employee related data. The usage of restricting business partner data based on the role concept is best if you do not want people to see some sales related data.

To restrict access to critical employee information I would make use of the object B_BUPA_FDG to disable the display of critical fields you do not want every sales rep to have a look at.
5.2.7. Perform authorization checks for sales area related data for business partners.

Authorization object used: CRM_BP_SA

Relevant OSS notes:
- 524474: Sales Area related authorization check in business partner (prerequisite)
- 803453: Sales Area related check in business partner
- 999239: PCUI: Sales area authorization in partner function tab

Reason and Prerequisites
In every sales area, only certain employees are authorized to maintain (create and/or change) the sales-area-dependent data in the business partner master record, or to display them. The general business partner data can be displayed, changed or created by any of the employees. The authorization check should be done at the time of entering the sales area-dependent data. While calling the sales-area-dependent data, a sales area needs to be selected. This selection screen should display only those sales areas for which the user has an authorization, depending on the activity (creating, modification, display). This requirement cannot be met entirely with the help of the BDT- (Business Data Toolset)-tools alone, i.e., in modification-free or upgrade-resistant manner. A small modification, which is described in the following section, is necessary.

5.2.8. Restriction of business partner role in the BP transaction

Some companies would like their users only to create a Business Partner in a specific role. As we have seen already, the authorisation object B_BUPA_RLT can be used for such a setup. However, in such a case you are limiting the allowed role maintenance still by using the same BP transaction. Suppose you would like to have a separate transaction code to create an employee or prospect, you can do this by creating new transaction codes using SE93. Next you can assign these new transaction codes to a specific role related activity using the transaction code BUSF.
In the example above, you can see that using the transaction code BUA1 you will be able to “create” a Business partner in the role “contact person”.

You can look at the transaction code details using SE93.
5.3. Product Security

5.3.1. Relevant SAP Authorization objects

Standard Authorization Objects

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product General</strong></td>
<td></td>
</tr>
<tr>
<td>COM_PRD</td>
<td>Product Master, general authorization: Determines whether a user is authorized to maintain products or only to display them.</td>
</tr>
<tr>
<td>COM_PRD_CT</td>
<td>Product Master, authorization for category: This authorization object is used to determine whether a user can display and/or edit products, which are assigned to a particular category.</td>
</tr>
<tr>
<td><strong>Set Types and Alternative Identifier</strong></td>
<td></td>
</tr>
<tr>
<td>COM_ASET</td>
<td>Set Types/Attributes, general authorizations: Determines whether a user is authorized to maintain set types and attributes, or only to display them.</td>
</tr>
<tr>
<td>COM_ALTID</td>
<td>Authorization object for alternative IDs: Determines whether a user is authorized to create or change alternative identification types.</td>
</tr>
<tr>
<td><strong>Product Category and Hierarchy</strong></td>
<td></td>
</tr>
<tr>
<td>COM_HIER</td>
<td>Hierarchies, general authorizations: Determines whether a user is authorized to maintain product hierarchies or only to display them.</td>
</tr>
<tr>
<td>COM_CAT</td>
<td>Categories, general authorizations: Determines whether a user is authorized to maintain product categories or only to display them.</td>
</tr>
<tr>
<td>COM_CAT_CF</td>
<td>Categories, authorization for configuration-relevant data: Determines whether a user is authorized to maintain or display configuration-relevant category data.</td>
</tr>
<tr>
<td><strong>Product Relationship</strong></td>
<td></td>
</tr>
<tr>
<td>COM_IL</td>
<td>Authorization check for product relationships: Determines whether a user is authorized to display and/or maintain relationships.</td>
</tr>
</tbody>
</table>
5.3.2. Product maintenance

Before you start creating new roles for authorization restrictions concerning products, you should know some basic information!

PRODUCTS

Products are goods, which are the object of a company's business activities. Products can be tangible, such as a PC, or intangible, such as services like PC maintenance.

Use:

The product master provides you with all information on the products that your company purchases and sells. It is the central source from which product-specific data can be retrieved.

Product information is used in marketing, sales, and service processes. The product master functionality is integrated into various business roles and therefore provides all functionality you require for working with products within the relevant business context.

Product data includes the information required for specific business processes (such as customer inquiries, sales orders, service processes, contracts), and other basic data that essentially describes and categorizes the product. For example:

- Data of a descriptive nature such as size and weight
- Data with a control function such as the item category group for determining the item category for each item in a CRM order

This information is stored in individual product master records. The integration of such data in a single database object eliminates redundant data storage.

Structure:

Product Types

The product type describes the basic characteristics of a product. It also determines to which product categories a product can be assigned, thus defining the structure of the product and how it can be used.

The following product types are available:

- Material
- Service
- Warranty
- Financing
- Intellectual property

In the maintenance screen for products (transaction code COMMPR01) you can see different buttons, which allow you to create a product of a certain product type.
In this screen you see only four buttons for creating a:
- Material
- Service
- Financing
- Warranty

In customizing the product type IP (intellectual property) has been disabled.

SAP IMG ➔ Cross-application components ➔ SAP Products ➔ Settings for Product type ➔ Deactivate Product types

Attributes and Set Types
Attributes are used to describe products and are grouped together into set types. The use of set types makes it possible to model a product in a detailed manner in your system.

How can you create them?
In the SAP Menu for CRM, choose:
Master data ➔ Products ➔ Maintain Set Types and Attributes or directly by using the transaction code COMM_ATTRSET.

© 2007   Contact Author: davy.pelssers@contactoffice.net
Set types and attributes works more or less the same way as the creation of marketing attributes that you use for business partners. (See section Marketing and Campaign management). The main difference is that you do not directly assign such a set type to a product, but assign set types to a product category. Next each product that belongs to this category will have (depending on the settings you made) the option of maintaining the attributes for this product somewhere on the product maintenance screen.

You first also create the attributes and next group certain attributes logically together into a set type.

**Screenshot of an attribute**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>ZBRANDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Brand</td>
</tr>
</tbody>
</table>

**Characteristics**

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>CHAR Character String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Length</td>
<td>15</td>
</tr>
</tbody>
</table>

**Descriptive**

<table>
<thead>
<tr>
<th>Language</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EN English</strong></td>
<td>Brand</td>
</tr>
</tbody>
</table>

**Fixed Values Allowed**

<table>
<thead>
<tr>
<th>Single Value...</th>
<th>Upper Limit</th>
<th>Fixed Value Des.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHIL</td>
<td></td>
<td>Philips</td>
</tr>
<tr>
<td>PION</td>
<td></td>
<td>Pioneer</td>
</tr>
<tr>
<td>SON</td>
<td></td>
<td>Sony</td>
</tr>
</tbody>
</table>

**Language-Specific Descriptions for Fixed Values**

<table>
<thead>
<tr>
<th>Single Value...</th>
<th>Upper Limit</th>
<th>Language</th>
<th>Fixed Value Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHIL</td>
<td></td>
<td>EN English</td>
<td>Philips</td>
</tr>
<tr>
<td>PION</td>
<td></td>
<td>EN English</td>
<td>Pioneer</td>
</tr>
<tr>
<td>SON</td>
<td></td>
<td>EN English</td>
<td>Sony</td>
</tr>
</tbody>
</table>
**Categories and Hierarchies**

Categories and hierarchies are used for structuring purposes, and allow you to group together products according to different criteria. Categories define which set types and relationship types are allowed for a product, thereby enabling you to structure the information you require on your products through the assignment of categories.

Categories and hierarchies can be maintained using the following path in the SAP CRM Menu:

*Master data ➔ Products ➔ Maintain categories and hierarchies* or directly by using the transaction code **COMM_HIERARCHY**

Some standard delivered hierarchies are:

<table>
<thead>
<tr>
<th>Description</th>
<th>Hierarchy ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material group</td>
<td>R3MATCLASS</td>
</tr>
<tr>
<td>Product hierarchy</td>
<td>R3PRODHIER</td>
</tr>
<tr>
<td>Product Subtype</td>
<td>R3PRODSTYP</td>
</tr>
</tbody>
</table>

Anyhow, you can create your own hierarchies and product categories in the SAP CRM system. The link between product attributes, product set types and products is made the following way:

*How does this look like in the system?*

After you have created for example a set type ZTEST, you will assign it to either a product hierarchy or product category. On the maintenance screen of a category/hierarchy you have several tab pages. One of them is called “set types” where you can assign existing or own created set types. You can also define the view (tab page) on which the set type should be made available and the position (on the screen).

Furthermore, the flag inherited points to the fact if you have the set type inherited from a higher-level product category/hierarchy or not.
In customizing you can define your own Views for this purpose.
SAP IMG → Cross-application components → SAP Products → Settings for Product Maintenance → Define Views

**Relationships**

Relationships can be created between products and other products or objects to represent certain product information. For example, spare parts, accessories, or services might be available for a particular product, or products may contain or belong to other products, such as sets and prepacks.

On the maintenance screen of relationships for products, you will see that there are different tab pages available. They make up the type of relationship towards the product.
Standard role for product maintenance

SAP_CRM_PRODUCT

You can make a copy of this template role and make the necessary adjustments. Available transactions in this standard role are:

<table>
<thead>
<tr>
<th>Transaction Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMPR01</td>
<td>Maintain Products</td>
</tr>
<tr>
<td>COMM_PROD_RECATEG</td>
<td>Recategorize Products</td>
</tr>
<tr>
<td>COMMPR02</td>
<td>Mass Processing of Inactive Products</td>
</tr>
<tr>
<td>COMM_HIERARCHY</td>
<td>Maintain Categories and Hierarchies</td>
</tr>
<tr>
<td>COMM_ATTRSET</td>
<td>Maintain Set Types and Attributes</td>
</tr>
<tr>
<td>CRMD_SERV_SLA</td>
<td>Process Availability and Response times</td>
</tr>
</tbody>
</table>

5.3.3. Product Proposals

The product proposals consist of Cross-/Up-/Down-Selling, Accessories and Top N Lists. They use SAP Web Application Server and Business Information Warehouse. The people centric UI of the product proposals uses the Enterprise Portal.

The authorization object CRM_PAR manages the authorization requirements for the maintenance of product association rules (cross-/up-/down-selling). It manages authorization concerns related to:
- Creating new rules
- Changing existing rules
- Deleting existing rules
- Activating existing rules

If the authorizations are not maintained for a user, the user can search for product association rules and display them. However, it is not possible for the user to create, change, delete, or activate rules. It is recommended to maintain the settings of the authorization object according to the needed requirements.

There is no authorization object for top N lists. Therefore, it is not possible to handle authorization constraints, such as mentioned for the CRM_PAR authorization object.
5.4. Authorization check in Business Transactions

Before we start into the authorization concept for Business Transactions you should learn the difference between business transaction category, business transaction types and business transactions!

5.4.1. Relationship Business Transactions, Types and Categories

The first thing everyone should do who will analyze SAP CRM authorizations is reading the CR100 course. This is a good starting point for understanding SAP CRM.

If you would have read the course, you will realize that SAP CRM business transactions are based on a concept, which is different from R/3.

In customizing you will see that CRM business transactions are made up as follows.

Every transaction type in SAP CRM (= the R/3 document Type) belongs to one or more transaction categories, but only has 1 leading transaction category.

You can check this easily in customizing via the path: (tcode SPRO)

*SAP IMG → Customer Relationship Management → Transactions → Basic settings → Define Transaction Types*

**Change View "Definition of transaction types": Overview**

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Description</th>
<th>Leading Transaction Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>Sales Call</td>
<td>BUS2000126 – Business Activities</td>
</tr>
<tr>
<td>LEAD</td>
<td>Lead</td>
<td>BUS2000108 - Lead</td>
</tr>
<tr>
<td>OPPT</td>
<td>Opportunity</td>
<td>BUS2000111 - Opportunity</td>
</tr>
<tr>
<td>TA</td>
<td>Standard order</td>
<td>BUS2000115 - Sales</td>
</tr>
</tbody>
</table>

© 2007 Contact Author: davy.pelssers@contactoffice.net
If you look at Transaction type “0001” sales call in more detail, you will see this:

**Change View "Definition of transaction types": Details**

![Change View "Definition of transaction types": Details](image)

This is an important thing you should know, since per Transaction Category, you have a special authorization object that you should have assigned in your user master record, in order to process such a business transaction at all.

The value for those “transaction category related” authorization objects is “allow”, which you can maintain in the profile generator.

List of those specific **Transaction Category related objects**:

<table>
<thead>
<tr>
<th>Transaction category</th>
<th>Authorization Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activities</td>
<td>CRM_ACT</td>
</tr>
<tr>
<td>Opportunities</td>
<td>CRM_OPP</td>
</tr>
<tr>
<td>Sales Transactions</td>
<td>CRM_SAO</td>
</tr>
<tr>
<td>Service Transactions</td>
<td>CRM_SEO</td>
</tr>
<tr>
<td>Service Contract</td>
<td>CRM_CO_SE</td>
</tr>
<tr>
<td>Service Confirmation</td>
<td>CRM_CON_SE</td>
</tr>
<tr>
<td>Lead</td>
<td>CRM_LEAD</td>
</tr>
<tr>
<td>Complaints</td>
<td>CRM_CMP</td>
</tr>
<tr>
<td>Financing Contract</td>
<td>CRM_CO_SA</td>
</tr>
<tr>
<td>Sales Contract</td>
<td>CRM_CO_SC</td>
</tr>
</tbody>
</table>

**CRM Menu:**
The CRM menu I always work with is the following: CRM_MENU
You can assign this one to your user (via SU01):
Now you should see the following menu:

**SAP Easy Access  Extended Relationship Management**

- **Business activities**
- **Marketing related transactions**
- **Sales**
- **Service**

Per area you see that SAP has made a distinction in processing business transactions, such as:

- **Activities**
- **Tasks**
- **Leads**
- **Opportunities**

The most common business transactions that customers are using are:
- Quotations
- Sales orders and Service orders

If you for example open some folders such as “activities” and “sales” you see the following:

<table>
<thead>
<tr>
<th>SAP menu</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CRMD_BUS2000126 - Maintain Activities</td>
</tr>
<tr>
<td></td>
<td>CRM_ACT_JR_TMPT_TYPE - Maintain Activity Journal Template Type</td>
</tr>
<tr>
<td></td>
<td>CRM_ACT_JR_TMPT - Maintain Activity Journal Template</td>
</tr>
<tr>
<td></td>
<td>S_AE2_89000019 - Activity Monitor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td>CRMD_BUS2000111 - Maintain Opportunities</td>
</tr>
<tr>
<td></td>
<td>CRMD_BUS2000115 - Maintain Sales Transactions</td>
</tr>
<tr>
<td></td>
<td>CRMD_BUS2000121 - Maintain Sales Contracts</td>
</tr>
<tr>
<td></td>
<td>CRM_SP - Execute Sales Planning</td>
</tr>
<tr>
<td></td>
<td>CRMC_ACTION_JOB - Action Monitor</td>
</tr>
</tbody>
</table>

You can see the names of the transaction codes.
To display those you need to make the following setting:

In the menu, select “extras ➔ settings ➔ display technical names”.
Now that you know the transaction codes, you can try to launch one, for example:

This will call the following screen:

**Create CSD Interaction**

The system automatically opens the locator for searching objects belonging to the area you want to work in. In this case business activities.

This part displays the Business transaction details. If this is in display mode or change mode depends on your settings.
**Change Locator Settings:**

**Option 1:** change Locator settings permanently in a certain modus for your user.

Menu: choose Extras → Settings

**Option 2:** Change the size of the locator temporarily, in this user session
Change modus (display/change) when launching a certain transaction

Menu: choose Extras → Settings

Although you launched the transaction for creating/displaying business activities, you will that by using the “create business transaction” button, you can nevertheless create business transactions that belong to another business transaction category.

If you press the button, you will get a dropdown list for the authorized “transaction categories”. This is based on the authorization objects I mentioned before.

If you now select “business activities” you get the list of authorized “transaction types” that have the status “active” in customizing.
List of Transaction codes (most used business transactions)

<table>
<thead>
<tr>
<th>Transaction Code</th>
<th>Description</th>
<th>Authorization Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMD_BUS2000126</td>
<td>Maintain Activities</td>
<td>CRM_ACT</td>
</tr>
<tr>
<td>CRMD_BUS2000108</td>
<td>Maintain Leads</td>
<td>CRM_LEAD</td>
</tr>
<tr>
<td>CRMD_BUS2000111</td>
<td>Maintain Opportunities</td>
<td>CRM_OPP</td>
</tr>
<tr>
<td>CRMD_BUS2000115</td>
<td>Maintain Sales Transactions</td>
<td>CRM_SAO</td>
</tr>
<tr>
<td>CRMD_BUS2000121</td>
<td>Maintain Sales Contract</td>
<td>CRM_CO_SC</td>
</tr>
<tr>
<td>CRMD_BUS2000116</td>
<td>Maintain Service Processes</td>
<td>CRM_SEO</td>
</tr>
<tr>
<td>CRMD_BUS2000117</td>
<td>Maintain Service Confirmations</td>
<td>CRM_CON_SE</td>
</tr>
<tr>
<td>CRMD_BUS2000120</td>
<td>Maintain Complaints and In-house Repairs</td>
<td>CRM_CMP</td>
</tr>
<tr>
<td>CRMD_BUS2000112</td>
<td>Maintain Service Contracts</td>
<td>CRM_CO_SE</td>
</tr>
</tbody>
</table>

The Important thing that you should now is that for each and every one of those transactions, the screen is always built up the same way.

![Button Toolbar]

**LOCATOR**

**Business Transaction Information**

- The initial transaction type that is launched depends on user settings.
- Change/display modus also depends on user settings

As you can see the transactions in the previous table all start with CRMD_BUSxxxxxx. In fact, as you could have guessed the BUSxxxxxx part corresponds to the leading transaction categories we discussed earlier.
Since all screens are made up the similar way, SAP reuses this logical and structured UI framework for business transactions. The only thing they need to do is in this case look at the Leading transaction category, and therefore:

- Set other default search settings in your locator to start with
- Use a business transaction type of the transaction category that corresponds to the “BUSxxxxxx” you are launching to start in the initial business transaction information screen part.

Last, you have the transactions!
In fact, a transaction in this case would be a business transaction!!
For example; you create a business activity of the Type "sales call" in your system!
In that case the system will save this transaction as a number!

Create Sales Call

In the table CRMD_ORDERADM_H, after creating for example a standard transaction of the type 'sales call", you will find this back by entering the Number of the transaction!

© 2007 Contact Author: davy.pelssers@contactoffice.net
Or you can just look up all transactions by "process type", which in that case would be '0001'.

### Table CRMD_ORDERADM_H Display

<table>
<thead>
<tr>
<th>CLIENT</th>
<th>208</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID</td>
<td>501422180956049060540695625</td>
</tr>
<tr>
<td>O'Brien Language EN</td>
<td></td>
</tr>
<tr>
<td>LOCAL SYSTEM</td>
<td>COLLAB11</td>
</tr>
<tr>
<td>CRM RELEASE</td>
<td>BOSCMY 100</td>
</tr>
<tr>
<td>SCENARIO</td>
<td>A</td>
</tr>
</tbody>
</table>

**Template Type**

**Created At:** 25.01.2006 23:24:52

**Changed By:** DAVY

**Head Changed At:** 25.01.2006 23:24:52

**Object Type:** BUS20000128

**Archiving Flag:** Y

**Description UC:** CRMD_BUS2000126

**Object ID:** CRMD_BUS2000126

**Verify Date:** Y

**CRM Changed At:** 25.01.2006 22:24:52

**Postprocess At:**

**Impact on authorizations**

**Example:**

When creating a role for a sales rep (who is allowed to create activities, leads and opportunities for example) you would add the following transaction codes into your role using the profile generator (PFCG):

<table>
<thead>
<tr>
<th>Transaction Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRMD_BUS2000126</td>
<td>Maintain Activities</td>
</tr>
<tr>
<td>CRMD_BUS2000108</td>
<td>Maintain Leads</td>
</tr>
<tr>
<td>CRMD_BUS2000111</td>
<td>Maintain Opportunities</td>
</tr>
</tbody>
</table>

In order to process these 3 different kinds of transaction categories you would need to have the following authorization objects in your role with the value “allow”:

- **CRM_ACT** (allows you to process activities)
- **CRM_OPP** (allows you to process opportunities)
- **CRM_LEAD** (allows you to process leads)
**Impact on the User Interface:**

Before restricting to the 3 needed transaction categories:

![User Interface Before Restriction]

After restricting the role to only the three authorization objects:

![User Interface After Restriction]

**Remark:**
I have set the authorization object CRM_ORD_LP to inactive; otherwise my restriction did not seem to work. Furthermore I also restricted the object CRM_ORD_PR where I also defined which transaction types are allowed for processing.
When I assign this role to a user, he will only have the option for creating a transaction belonging to one of the three transaction categories. Which transaction categories may be executed, depends on which “transaction category related objects” you have with value “allow” in your role. Which transaction types will be displayed on the right side of the dropdown-list depends on the restrictions made in the authorization object CRM_ORD_PR.

The reason why I set the authorization object CRM_ORD_LP to inactive is because of the fact that in both CRM_ORD_PR and CRM_ORD_LP the authorization field PR_TYP is being checked. If you do not restrict both authorization object with the same transaction types, then the restrictions which I only made in CRM_ORD_PR are overwritten by the fact that I had “*” as value in PR_TYPE for the object CRM_ORD_LP.

See the table with Transaction category related objects.
**Hint:**
Why would SAP create multiple transaction codes for accessing certain transaction types that belong to a certain “leading transaction category” if in the end, you see that with the button “create transaction” I still have the option of creating another transaction belonging to another transaction category?

My guess is the following:

1) This eases the structuring of the user menu. You will logically assign the transaction codes into a folder area.

In the folder “activities” they will place the CRMD_BUS2000126 which will start the initial screen with “default settings for searching business activities” in the locator.

![SAP menu]

Furthermore on the right hand side of the screen, a “business activity” will be started. As I explained before, this also depends on the user settings. You could choose to have your last transaction displayed (in either display or change mode).

2) This also eases the maintenance of authorizations, since the system normally automatically includes the corresponding authorization object, which belongs to this transaction category when adding the transaction into a role.

**Example:** if you would add the transaction CRMD_BUS200108 (leads) into your role, you will see that in the profile generator, the system automatically includes the necessary object CRM_LEAD into your role.

© 2007  Contact Author: davy.pelssers@contactoffice.net
5.4.2. Process flow authorization check

Business transaction processing in CRM is protected by an authorization check based on alternatives, so that only authorized users can create, change or delete a transaction. The authorization check follows a specific sequence, that is, the check runs through several levels. This means that the authorization can be granted at each level, and therefore no check is necessary in the subsequent levels. If, for example, an employee is entered in a document as the employee responsible, he is allowed to process this document regardless of whether further checks would lead to a positive or negative result.

The authorization concept in the CRM business transaction has the following characteristics

Role-related protection:

Users have access to existing business transaction documents, regardless of all other authorization checks, if they are entered as an "employee" or "responsible" in these documents in a partner function for the partner function category. The type of activity allowed is linked to the type of partner function.

See also: Partner Processing

Sales area/effects in the organization model:

Users have access to business transactions, which are or were already created in or above a certain level in the organization model, regardless of all other authorization checks. If need be, users can only execute specific activities.

Business transaction category:

Users can only create transactions if they have authorization for the corresponding business transaction category (for example, activity - CRM_ACT, opportunity - CRM_OPP).

Business transaction type:

Users only have access to business transaction documents if they have authorization for the corresponding business transaction type. If need be, users can only execute specific activities.

Sales area

Payment card processing:

Only authorized users are able to see the payment card number.

Prerequisites

Users for whom an authorization check is to be executed must be assigned in the organization model.

In order that other functions can be executed, for example, partner determination, SAP recommends that you assign an employee, to whom a user is assigned in the business partner record, to the position.
Maintenance of the Organizational model was already explained in chapter 4.4.

**PROCESS FLOW**

Your own documents (authorization object CRM_ORD_OP)

The system checks whether the user takes on a specific partner function for the activity executed in the relevant document, for example, whether he is the employee responsible. Furthermore, the system checks whether the user has the authorization to change, display or delete a transaction. If the result of this check is positive, no further checks take place at transaction level.

Visibility in the organization model (authorization object CRM_ORD_LP)

If the user is not authorized in the first step of the check, the second check is carried out. This check enables the employee to control the access to specific organizational units via his position, depending on his assignment. This authorization object defines which documents can be processed by the user in the individual organizational levels, and which activities he can carry out here. If the user is authorized for the chosen activity (create, change, display, delete) and the relevant organization level, no further checks are carried out.

When maintaining the authorization field CHECK_LEV, you should only choose the organizational unit at the highest level of the units to be checked. If, during the authorization check, the relevance to a specific sales organization is checked, the organizational units underneath this are also automatically checked. This means that you
do not have to choose the (lower-level) organizational unit sales office. This would cause considerable deterioration in performance.

**Combination of several authorization objects**

If the first two checks were not successful, this combination of different authorization objects is checked. All the checks must be successful before the user is authorized to process the required transaction. This means the user only receives the authorization to process if he is authorized to:
- Process the **leading business transaction category** in the corresponding transaction type
- Process the corresponding transaction type
- Process in the corresponding sales area

**a) Authorization objects CRM_ACT, CRM_OPP, CRM_SAO, CRM_SEO, CRM_CO_SE, CRM_CON_SE, CRM_LEAD, CRM_CMP, CRM_CO_SA, CRM_CO_SL**

Using these authorization objects, the system checks, which business transactions the user is allowed to process, and whether he is allowed to carry out the functions create, display or delete in these transactions. The relevant authorization object is checked, depending on the activity executed:
- Activities: CRM_ACT
- Opportunities: CRM_OPP
- Sales transactions: CRM_SAO
- Service transactions: CRM_SEO
- Service contract: CRM_CO_SE
- Service confirmation: CRM_CON_SE
- Lead: CRM_LEAD
- Complaints: CRM_CMP
- Financing contract: CRM_CO_SA
- Sales contract: CRM_CO_SL

**b) Authorization object CRM_ORD_PR**

Using this authorization object, the system defines which action the user is allowed to execute for each business transaction type.

**c) Authorization object CRM_ORD_OE**

Using this authorization object, the system defines in which sales area or in which service organization the user is allowed to process the CRM business transaction, and which activities he can carry out here.

If the user is not authorized in the third step of the check, he will not be able to process the document in the required way. He will receive a system message, which contains the corresponding authorization object and refers to the lacking authorization.
5.4.3. Examples of the authorization assignment

1. A user wants to keep the authorization to process sales transaction with the transaction OR in the sales organization 0001 and for distribution channel 01.

You assign the following authorizations:
- CRM_ORD_PR: PR_TYPE ‘TA’, ACTVT ‘*’
- CRM_SAO: ACTVT ‘*’

2. A user wants to keep the authorization to process all types of sales transactions (independently of the transaction type and the organizational assignment).

You assign the following authorizations:
- CRM_ORD_PR: PR_TYPE ‘TA’, ACTVT ‘*’
- CRM_SAO: ACTVT ‘*’
- CRM_ORD_OE: SALES_ORG ‘*’, DIS_CHANNE ‘*’, SALES_OFFI ‘*’, SALES_GROU ‘*’, ACTVT = ‘*’

3. The user wants to keep the authorization to display all opportunities in the transaction type OPPT that (accordingly to the organization model) belong to "his" sales office.

You assign the following authorizations:
- CRM_ORD_LP: CHECK_LEV ‘C’, PR_TYPE ‘OPPT’, ACTVT ‘03’

4. A user wants to keep the authorization to process a document in which he himself is entered as the employee responsible.

You assign the following authorizations:
- CRM_ORD_OP: PARTN_FCT ‘*’, PARTN_FCTT ‘0008’, ACTVT ‘*’

Combinations of different authorizations are also possible, for example, 1. + 2. + 4.
Since I received a lot of questions concerning the fourth example using the authorization object CRM_ORD_OP I would like to explain a bit more about this one.

The exact set-up as mentioned in example 4 is only valid if the employee X does not need to create any business transaction, but only should be able to process a certain business transaction in the case where another person Y assigned employee X as person responsible.

I can imagine the following scenario:
As I explained in most companies the partner determination procedure assigned to transaction types is used in such a way that the person responsible is automatically filled in with the Business partner (employee) who is creating the business transaction. This business partner number is mostly derived from the SAP USER that is creating the business transaction. This is in the first place why I explained that you need to make the link between user and business partner.

However, suppose you have a scenario that within your organization you have employees that are not actually CREATING business transactions, but only need to process them. Scenario: Company X is making use of call lists (marketing and campaign management). A call center is next processing those calls (transaction type 0003- Outgoing Phone Call) via the Interaction Center Webclient..they call potential customers to see whether they would like to have information about a new product model or not... Suppose 30% of the called prospects is interested in this new product.

In such a case the Call Center Agent will for example create a follow-up activity of the transaction type 1003 (Task), where he will MANUALLY assign a person responsible (this can be a sales rep), so not automatically via partner determination procedure. In such a case the sales rep does not need to create any transaction type. He will only look at tasks that are assigned to him for which he is made 'person responsible’. He can use the activity monitor for such a purpose. Therefore the following setup would be sufficient:

You assign the following authorizations:
**CRM_ORD_OP:**
- PARTN_FCT: *
- PARTN_FCTT: 0008’
- ACTVT: *
Now another scenario could be that I want to be able to create any transaction type, but only should be able to display/change/delete business transactions in which I am assigned as person responsible.

This only makes sense if you are using a partner determination procedure (assigned to your transaction types), which automatically fills out yourself as person responsible when you are creating the business transaction.

In such a case the "Partner function" person responsible is automatically filled out by using an access sequence that derives the business partner number (employee) from the SAP User that is creating the business transaction. In this case this would be you.

Since the authorization object CRM_ORD_OP does not contain the activity “create”, you should maintain this in CRM_ORD_PR.

Next you will also notice that the system needs to know for which distribution chain you should be allowed to “create” such a business transaction. This is indicated via CRM_ORD_OE.

This set-up seemed to work fine at first glance.
5.4.5 Authorization Check at Field Level

USE
You can use this function to allow certain authorization groups to change fields in the sales order, or prevent them from overwriting certain fields. For example, you only want to allow employees with special authorization to change quantities retroactively after the sales order has already been delivered.

Prerequisites

- You have created an authorization with reference to authorization object CRM_FLDCHK, assigned this authorization to an authorization profile, and assigned this profile to the corresponding user.

  When you create the authorization with reference to the authorization object, you can only specify one value (whole number) for field Authorization Level. The authorization check cannot process ranges (for example, 1 – 12) or multiple values (for example, 5,7,9).

- You have defined authorization groups in Customizing and assigned fields to them. An authorization group is a type of field group, and consists of a collection of fields. You make the entries in Customizing for Customer Relationship Management at Basic Functions → Authorizations → Define Authorization Groups.

- You have assigned an authorization level for each authorization group in Customizing in dependency with the key fields, for instance transaction type and item category. You make these entries manually in Customizing for Customer Relationship Management at Basic Functions → Authorizations → Maintain Authorizations at Field Level. You fill the control table CRMM_AUTH_FIELD with these entries.

  Control table CRMM_AUTH_FIELD is created as a master data table, and therefore cannot be transported. For this reason, you should maintain this control table in your productive system.
Features

In order to be able to carry out an authorization check for the user at field level, particular authorization information has to be read into the sales order for the authorization check. These are:

- Key fields (transaction type and item category) that are used to read the data from the control table
- Authorization level from the authorization object of the user. The authorization object contains the following fields:
  - Activity
  - Authorization Group
  - Authorization Level
- Other entries in the control table, such as authorization groups and authorization level for each authorization group (field group)

If you have made entries in the Customizing table for the definition of authorization groups, and assigned an authorization level for each authorization group in the control table, the system carries out the authorization check when a transaction is processed.

In the authorization check, the system evaluates the control table and checks whether the authorization level from the control table is higher or lower than the authorization level in the user’s authorization object. If the user’s authorization level is at least as high in his or her authorization object as the authorization level in the control table, he or she is permitted to overwrite the field. If his or her authorization level is lower than that in the control table, he or she cannot change the field.

If a field is assigned to several authorization groups, the authorization check determines the authorization group with the highest authorization level.

If the control table does not contain any data, the authorization check cannot be carried out.

You can use a Business Add-In (BAdI) to make further fields available for the authorization check at field level. The Transaction Type and Item Category fields are shipped for this purpose as standard. If you want to use more fields (which you have added to the control table CRMM_AUTH_FIELD) for the authorization check, you can locate these additional fields with this BAdI and transfer them to the authorization check.

For more information, see the Implementation Guide (IMG) at Customer Relationship Management → Basic Functions → Authorizations → Define Authorization Groups and Business Add-In for Checking Fields.

Activities

Process the Customizing activities described in section 'Prerequisites'.
Example

Authorization group 0001 consists of the following fields:
- Quantity
- Unit of Measure

Authorization group 0002 consists of the following fields:
- Pricing Date
- Price List

The following entries are maintained in the control table:

Entries in the Control Table

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Item Category</th>
<th>Authorization Group</th>
<th>Authorization Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA</td>
<td>TAN</td>
<td>0001</td>
<td>15</td>
</tr>
<tr>
<td>TA</td>
<td>TAN</td>
<td>0002</td>
<td>10</td>
</tr>
<tr>
<td>AG</td>
<td>AGN</td>
<td>0001</td>
<td>5</td>
</tr>
<tr>
<td>AG</td>
<td>AGN</td>
<td>0002</td>
<td>3</td>
</tr>
</tbody>
</table>

The user has the following authorizations:

<table>
<thead>
<tr>
<th>Authorization group 0001</th>
<th>Authorization level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization group 0002</td>
<td>Authorization level 12</td>
</tr>
</tbody>
</table>

When the user creates a sales order with transaction type TA and item category TAN, he cannot change the fields of authorization group 0001 (Quantity and Unit of Measure), as he only has authorization level 6 for this, and this value is below authorization level 15 from the control table. He can, however, change the fields of authorization group 0002 in the order (Pricing Date and Price List), as he has authorization level 12, which is above authorization level 10 from the control table.
5.4.6. Business add-in for authorization check in business transactions

SAP also delivers a business add-in CRM_ORDER_AUTH_CHECK you can use for additional authorization checks in business transactions.

You can display the details of this BADI using transaction code SE18.

It is also possible to find back this BADI via the following customizing path:
SPRO ➔ Customer Relationship management ➔ Transactions ➔ Basic Settings ➔ Business add-ins ➔ Business Add-in for authorization check in the business transaction

5.5. Authorizations in E-commerce (Internet Sales)

In this chapter I will elaborate the authorization Setup within a B2B scenario.

5.5.1. Customizing settings for Internet Sales

SAP IMG ➔ Customer Relationship Management ➔ Internet Sales ➔ Internet User

Here you have 2 scenarios, being B2C (business to consumer) and B2B (business to business).

Depending on the scenario you are using you will maintain different settings.

The scenario for B2B will be illustrated in this documentation.

5.5.1.1. Internet User Settings

Set B2B Internet User:

- User Internet Users only (SU01)
- Use Internet User only (SU05)
- Convert Internet Users (SU05) to Internet Users (SU01)
Since SU05 Internet User concept is out of date, we will only focus on the use of the SU01 Internet Users.

This type of user scenario uses an SU01 user that is connected with a contact person business partner.
You have the option with this structure to define personalization, workflow and specific user roles. Additionally, you also have the option in Internet Sales to use the user administration via a Web-based application with which, for example, integration with the portal is made possible.
This user scenario is an example of the recommended configuration setting.

The entry Role for Authorization Check (see below) should be maintained in this context.

**Role for Authorization Check:**

In the standard configuration (client 000), the default value is the SAP_CRM_INTERNET_CUSTOMER role that must be transported to each client in order to be used, and through which a user-defined role can be replaced.

As you can see, here you define that you make use of the SU01 Internet User concept, and also which role will be used for authorization check purposes!

**5.5.1.2. Set Web-based User Administration**

**Use**
With this IMG activity you have the option of making settings for Internet Sales User Management that differ from the standard.

1) The business partner grouping determines the number range in which a new contact person is to be created. A grouping with internal number assignment is only possible. If the field is left empty, the standard grouping for internal number assignment is used.

2) The contact person role is used to create new Internet users. If you leave the field empty, the standard business partner role for contact persons (BUP001) is used.

3) The sold-to party role is used for the company search of a Web shop manager. Only business partners with the specified role and the entered search criteria are searched for. If you leave the field empty, the standard business partner role for customers (CRM000) is used for the company search.

4) Using the maximum number of users, you can limit the number of possible Internet users per company. When a new Internet user is created, the number of existing users is compared with the specified maximum number. It is not possible to create another user once the maximum number of users has been reached.

5) The e-mail-address is used as the sender address for e-mail notifications. If no e-mail address is specified, the address of the current Internet user of User Management is used as the sender address.

---

### New Entries: Details of Added Entries

<table>
<thead>
<tr>
<th>Internet User Administration: Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping</td>
</tr>
<tr>
<td>Contact Person Role</td>
</tr>
<tr>
<td>Contact Per. Role</td>
</tr>
<tr>
<td>Max. User No.</td>
</tr>
<tr>
<td>E-Mail Address</td>
</tr>
</tbody>
</table>

---

5.5.1.3. **Set Roles for Web-based User Administration**

**Use**

© 2007  Contact Author: davy.pelssers@contactoffice.net
You can assign authorizations by means of roles and reference users in Internet Sales and Channel Management User Administration.

In this IMG activity, you can define roles that can be assigned in user administration for Internet Sales Internet users.

These roles contain all of the authorizations that an Internet user requires in order to carry out relevant activities. You have the option of defining a name under which the role is displayed in the Web UI, otherwise the name of the role is displayed.

**Standard Roles available:**

The following roles are delivered as default values in client 000 as standard:

- SAP_CRM_INTERNET_CUSTOMER (Authorizations for the B2B Internet Sales Application)
- SAP_CRM_ISA_UA_SUPERUSER (Authorizations for Internet Sales User Management)
- SAP_PCC_COL_PARTNEREMPLOYEE (Channel Management: Partner Employee)
- SAP_PCC.COL_PARTNERMANAGER (Channel Management: Partner Manager)
- SAP_PCC.COL_PARTNERMANAGER_CC (Channel Management: Partner Management Channel Commerce)

If you want to use the roles that are delivered as standard, transport them to the appropriate client. You can replace these roles with your own.

**Change View "Internet User Administration: Selectable Activity Groups"**

In the online User Administration the roles you defined here in customizing will be available and can be assigned to a new Internet User!
5.5.2. User Administration

In this section more details are explained about the creation of the SUPERUSER (user administrator) and the creation of Internet Users.

5.5.2.1. Creation of an Internet Sales User Administrator

The User administrator will need to have the role SAP_CRM_Isa_UA_SUPERUSER assigned to his User Master Record!
Furthermore you assign the roles SAP_CRM_INTERNET_CUSTOMER and the role SAP_CRM_Isa_WEBSHOP_MANAGER.
(The customer can of course first make a copy of the standard delivered role, and make adjustments to the copied role should this be necessary).

Start user maintenance via SU01:

Fill out the username for the User Administrator:
In the next screen you fill out the necessary details such as first name, last name and e-mail address:

On the tab page “Logon data” fill out at least the following data:
- Alias (is required, since the alias serves as the user Id for logging on into the Online User Administration.
- Initial password (after logging on for the first time, you will need to change the initial password).
On the Tab page “Roles” you enter the role which allows Internet user administration.

Remark: Assignment of roles to the user master record can also be taken care of via the Profile Generator!

Edit the role for Internet User administration, and on the tab page “Users” you enter the username and validity period.

The User administrator should also exist as employee in the CRM system. On this level you link the User ID (SU01 user) to the Business partner.

Next you should also maintain this business partner in the Internet User role:
Since you already linked the SU01 user ID with the Employee, the Internet User automatically will take over the necessary data on this level such as ‘Alias and User ID’, the role assignment, and the initial password!

The last thing you need to do is create the employee 409666 also in the role contact person, and link him to your organization with the relationship ‘is contact person for’.

After all this is done, the Administrator will be able to logon to the Online User Administration tool:

http://Hostname:Port/isauseradm/useradmin/init.do
After logging on the first time with your initial password, the system will ask you to change your password:

<table>
<thead>
<tr>
<th>Change Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter your new password and repeat it to confirm</td>
</tr>
<tr>
<td>Old password</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Verify Password</td>
</tr>
</tbody>
</table>

### 5.5.2.2. Internet User Creation

There are two ways for creating Internet Users. To have a consistent procedure in user creation I advise to follow only of the two procedures!

Either you can create and maintain all necessary data (User, Contact Person, relationships and assignment of the Internet Sales User role) via the SAPGUI, or you will do this via the online user administration console.

**Creation of the Internet User in the SAPGUI (SU01 and PFCG)**

**Step 1: Creation of a SU01 user**

Again maintain the Username, Alias (acts as User Id in the web shop), email address, and the role SAP_CRM_INTERNET_CUSTOMER (either on user master record level, via the profile generator or via the BP role Internet User).
Make sure a User Comparison is done if you assign the role manually to the user master record!
Step 2: Creation of a Business Partner in the Role ‘Contact Person’.

Create a relationship for this contact person of the type “Is contact person for” and link this with a Business partner. (Organization in the role CRM000 – general business partner or other role).

Remark:
You should assign the contact person to an organization in a specific role depending on the customizing settings you made in step 5.5.1.2. Point 3!
Step 3: Creation of the contact person in role “Internet User”.

The business partner you just created in the role contact person now needs to be maintained in the role “Internet User” (BUP005) in order to have access to the web shop.

After performing all these steps the Customer will be able to logon to the web shop! (Since you created the user and business partner (roles) for this user manually, you will need to send him an email manually telling him what his User-ID and initial password are!)

Just search the SU01 User ID you created before (ISA_CONSUMER) and the alias, initial password and the assigned role will be entered automatically!
The URL will probably look like this:

http://hostname:port/b2b/b2b/init.do

**Online Internet User Creation**

**Process Flow**

The following business process runs in SAP CRM.

© 2007  Contact Author: davy.pelssers@contactoffice.net
1. Log on to user administration
2. Create contact person
3. Assign contact person to sold-to party
4. Update business partner master record
5. Create internet user for the contact person

The user administrator can create Internet Users online! This is the easiest way to do. Again depending on what you defined in customizing the system will react in a certain way when looking up existing Contact persons and/or organizations.

The User administrator launches the site for user administration:

URL should look like this: http://Hostname:port/isauseradm/useradmin/init.do

As you can see you have two options:
- Create new users
- Display and change existing users

I only will show the creation of new ‘Internet Users’ here.

There are two options here:
- Create a New User AND a new contact person
- Create a New User for an existing contact person

If you already created the contact person in the system for a certain organization via the SAPGUI, you can search on Business partner number:

I enter the business partner number of an existing company (or you can search this with the look-up button).

![Create New User for Existing Contact Person](image)

Press the button 'Go!'.

I get a result list with one or more contact persons that exist for this company.

![Contact Person Search](image)

Select the contact person for whom you want to create an Internet user and press the 'copy' button.

![Create New User for Partner 0800-0800-078](image)

© 2007  Contact Author: davy.pelssers@contactoffice.net
Fill out (mandatory) the User ID and select the role ‘Authorizations for Internet Customers’.

**Example:**
I created the User Id ‘juliel’ and assigned the role “authorizations for Internet Customers”. The email address ‘davy.pelssers@cernum.com’ is the email address, which is maintained on the relationship ‘is contact person for’.

The next screen you see is the following:

Here you could maintain the correspondence language, phone number and fax. Press the “create” button.
Finally you see that a new Internet user has been created! An email will be sent out to davy.pelssers@cernum.com to let the user know his user Id and password.

In the SAPGUI you can check now that the user with ALIAS ‘JULIEL’ has been created with the role SAP_CRM_INTERNET_CUSTOMER.
By pressing enter you see the generated User ID.

Furthermore you see information that is automatically filled in by the system when you created the Internet User online!
<table>
<thead>
<tr>
<th>Role</th>
<th>Type</th>
<th>Valid From</th>
<th>Valid To</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_CRM_INTERNET_CUSTOMER</td>
<td></td>
<td>23.01.2606</td>
<td>31.12.9999</td>
<td>Authorizations for Internet</td>
</tr>
</tbody>
</table>
5.6. Interaction Center Winclient

5.6.1. Technical System Landscape

The CRM Server includes the IC WinClient framework and the following SAP applications:

- **SAPphone**
  SAPphone provides a telephony function to the interaction center. It allows data to be exchanged between the CRM Server and the telephony component.

- **SAPconnect**
  SAPconnect provides an integrated e-mail function to the interaction center. It enables **communication management software** to connect to the SAP system (for example, an e-mail server or SMTP server).
5.6.2. User Administration and Authentication

- User Management
- The IC WinClient uses standard user management tools to maintain users.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Detailed description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User maintenance (transaction SU01)</td>
<td></td>
</tr>
<tr>
<td>Profile Generator (transaction PFCG)</td>
<td>You use the Profile Generator to create roles and assign authorizations to users in ABAP-based systems.</td>
</tr>
</tbody>
</table>

5.6.3. Users Overview

<table>
<thead>
<tr>
<th>System</th>
<th>User</th>
<th>Delivered?</th>
<th>Type</th>
<th>Default Password</th>
<th>Detailed description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM system</td>
<td>End user</td>
<td>No</td>
<td>Dialog user</td>
<td>INIT</td>
<td>User who can access IC WinClient functions. Created by CRM system administrator</td>
</tr>
<tr>
<td>CRM system</td>
<td>WF-Batch</td>
<td>Yes</td>
<td>System User</td>
<td>No</td>
<td>User who can process background workflow tasks</td>
</tr>
<tr>
<td>R/3 Backend</td>
<td>End User</td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>User who can access R/3 background functions. Depending on RFC destination, user can be individual user or system RFC user. Created by R/3 system administrator.</td>
</tr>
<tr>
<td>BW User</td>
<td>End User</td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>Created by BW system administrator if you want to evaluate interactive scripting through BW reporting</td>
</tr>
<tr>
<td>Multichannel Interface</td>
<td>Administrator</td>
<td>No</td>
<td>Communic. user</td>
<td>No</td>
<td>User with multichannel support using Multichannel Interface. Created by system administrator.</td>
</tr>
<tr>
<td>Multichannel Interface</td>
<td>User</td>
<td>No</td>
<td>System User</td>
<td>No</td>
<td>Created by multichannel interface administrator to replicate CRM user in multichannel interface and allow those users to access multichannel support (such as e-mail, chat, paging).</td>
</tr>
</tbody>
</table>
5.6.4. Data synchronization between CRM system and other systems

<table>
<thead>
<tr>
<th>Data Exchanged</th>
<th>When synchronized</th>
<th>How Synchronized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business partner data</td>
<td>When business partner is created in CRM, the data is replicated to R/3. When</td>
<td>Automatically by CRM middleware settings</td>
</tr>
<tr>
<td></td>
<td>business partner is created in R/3, the data is replicated to CRM.</td>
<td></td>
</tr>
<tr>
<td>Call related information between SAPphone and communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>management software</td>
<td>Automatically by SAPphone setting</td>
<td></td>
</tr>
<tr>
<td>Data between SAPconnect and communication management</td>
<td>Automatically by SAPconnect setting</td>
<td></td>
</tr>
<tr>
<td>software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data between multichannel interface and CRM if multichannel</td>
<td>Automatically by CRM settings</td>
<td></td>
</tr>
<tr>
<td>interface is used as multichannel support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data between CRM and third-party communication management</td>
<td>If you want to use the predict call functionality, call list data is replicated</td>
<td>Synchronize when managing the call list to predict calls</td>
</tr>
<tr>
<td>software</td>
<td>from CRM to third-party communication management software.</td>
<td></td>
</tr>
<tr>
<td>Data between CRM system and BW system</td>
<td>Evaluation of interactive scripting using BW</td>
<td>Manual synchronization of evaluation data from CRM to BW</td>
</tr>
</tbody>
</table>

5.6.5. Authorizations

- No roles are delivered with the IC WinClient.
- For an agent to access the IC WinClient, transaction **CIC0** must be assigned to the user’s profile.
- For a user to work as an interaction center agent, the agent must be defined in the following transactions (in the SAP Menu: Interaction Center → Interaction Center WinClient → Multichannel Interface Administration):
  - Assign Agents to E-Mail Queue Groups
  - Assign Agents to Chat Queue Groups
  - Assign Agents to Paging Queue
- For an agent to receive e-mails, the user has to be maintained in transaction SO28.
- For a user to start the interactive scripting editor, transaction **CRMM_TM_SCRIPT** must be assigned to the user’s profile.
5.7. CRM IC Webclient

The IC WebClient uses the CRM standard for authorizations. No roles are delivered with this application. However, one CRM back-end role (SAP_PCC_IC_AGENT) is delivered with SAP Enterprise Portal (SAP EP). If you run this application in SAP EP, the CRM back-end user has to be assigned to this CRM back-end role.

This application restricts the users that can change system settings. Only users with authorization S_TABU_DIS can change CRM customizing. The user JAVA_IC has authorization in mySAP CRM to allow remote function modules to be called via remote function call (RFC) (authorization object S_RFC, ACTVT 16, RFC_TYPE: FUGR).

ABAP Stack Standard Roles Used by mySAP CRM

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_PCC_IC_AGENT</td>
<td>SU01 IC agent user</td>
</tr>
</tbody>
</table>

If SAP EP is used to access IC functions, it is very important to match roles between SAP EP and the CRM Server.

Standard Authorization Objects

The following table shows the security-relevant authorization objects used in the IC agent scenario.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_TABU_DIS</td>
<td>ACTVT</td>
<td>02, 03</td>
<td>For all IC Customizing</td>
</tr>
<tr>
<td></td>
<td>DICBELCLS</td>
<td>CRMC or CRMS</td>
<td></td>
</tr>
<tr>
<td>BSP_APPL</td>
<td>BSP_APPL</td>
<td></td>
<td>This authorization is for protecting the People-Centric UI application. For a user to access a People-Centric UI application through the transaction launcher, the user must have authorization to access the People-Centric UI application.</td>
</tr>
<tr>
<td></td>
<td>BSP_VIEW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRM_CATEGO (As of release 5.0)</td>
<td>ACTVT (activity)</td>
<td></td>
<td>(Optional) This authorization object is used in the auto suggest in the IC WebClient. For more information, go to SAP Help Portal and choose Documentation mySAP Business Suite mySAP Customer</td>
</tr>
</tbody>
</table>
5.7.1. Customizing of the IC Webclient

For each User Interface version you have a separate customizing path:

**Winclient:** SAP IMG → Customer Relationship Management → Interaction Center Winclient

**Webclient:** SAP IMG → Customer Relationship Management → Interaction Center Webclient

Basically you will create your own IC Webclient profile in customizing. This is the main profile, which contains different sub profiles:

SAP IMG → Customer Relationship Management → Interaction Center Webclient → Define IC Webclient Profiles

If you look at the details of such an IC Webclient Profile, you will see the different sub profiles for:
An important difference between customizing the IC Web client and Win client is that several IC Web client sub profiles are based on XML.

For example, the Transaction Launcher Profile (DEFAULT) looks like this:

```
<?xml version="1.0"?>
<soap:Body>
<ns1:GetTransactionList>
<ACTID>100</ACTID>
</ns1:GetTransactionList>
</soap:Body>
</soap:Envelope>
```
5.7.2. Assignment of the IC Webclient Profile

Let's suppose you have actually customized your own IC Webclient Profile. To assign such a profile to an employee of your company, you need to perform several steps:

1) **Assign your employee to the organizational model**:

Maintenance of the organizational model can be done via the transaction code **PPOMA_CRM**. There you will define your organizational structure by defining organisational units (sales organizations, sales office…) and positions.

You will assign either the user or the business partner (in the role Employee) to a position in your org. model.

If you assign a business partner (employee) to a position, you should not forget to create the link between this business partner and the SAP USER he is using.

This can be done via the transaction code **BP**:

Choose the maintenance screen for the role Employee and select the tab page “identification”.

![Organizational Model Maintenance Screen](image)

After assigning your employee to the org model you will define for which organizational unit or position a certain IC Webclient Profile should be available.
2) **Assign IC Webclient Profile to an org unit or position**

You can do this using the SAP CRM menu:

SAP Menu → Interaction Center → Supporting Processes → IC Structure → Change Organization and Staffing

Or directly by using the transaction code **PPOMW**.

Select the org unit or position to which you want to assign your customized IC Webclient Profile by double clicking on it.

Next, in the menu, choose “Goto → Detail Object → Enhanced object Description”

You can maintain here which IC Webclient profile should be used for this org unit or position.

© 2007  Contact Author:  davy.pelssers@contactoffice.net
5.7.3. How to launch the IC Webclient

To launch the IC Webclient you have several options that should work, if everything is configured correctly.

A) Launch the Webclient via transaction code CRM_IC

B) You can also look up the URL to launch the IC Webclient:

Use the transaction code **SE80** to launch the Object Navigator.
Next, choose the BSP Application CRM_IC (this is the standard delivered IC Webclient BSP Application by SAP).
Next, open the folder “pages with Flow Logic” and double click on the page “default.htm”.

5.7.4. Useful Parameters

Actually, I do not know the first two parameters, but the parameter CRM_ICWC_TEST allows you to display the technical names of the combination BSP application/View that you are looking at in the IC Webclient.
By moving your mouse over the description field of the view, you will get the name of the current BSP Application and the view you are looking at.

5.7.5. Useful information about the IC Webclient

If your company is about to implement the SAP CRM IC Webclient, I would advise you to have a look at the following information:

1)  http://help.sap.com

A) Via the following URL, you can read the basics about the usage of the SAP CRM Interaction Center. Also the differences between the Winclient and the Webclient are more or less explained.


B) If you want to learn some basics about creating Web Applications with BSP’s and the Model View Controller concept, you can launch the following URL:

http://help.sap.com/saphelp_crm40sr1/helpdata/en/c8/101c3a1cf1c54be10000000a114084/frameset.htm

2) If your company has a user account on SAP Service Market Place you can also find a lot of useful presentations and the IC Webclient cookbook.

http://www.service.sap.com

I am not sure about the path but if you use for example the "SAP support portal” and use the ‘advanced search’ there, you will find it back too!

Search term = Webclient cookbook
Method = phrase
In this way I find back two entries:

1) Interaction Center WebClient Cookbook
2) Interaction Center WebClient Cookbook - Service Industry Ext

3) **Online Knowledge Products (OKP)**


Your company can also buy access to Online Knowledge Products.

4) **Specific SAP Courses:**

   - CR400: SAP CRM Interaction Center Winclient
   - CR410: SAP CRM Interaction Center Webclient
   - NET200: SAP Web Application Server: Developing BSP Applications

5) **SAP BOOKS:** [www.sap-press.com](http://www.sap-press.com)

<table>
<thead>
<tr>
<th>ISBN 1-59229-049-9</th>
<th>Advanced BSP Programming</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISBN 1-59229-067-1</td>
<td>mySAP CRM Interaction Center</td>
</tr>
</tbody>
</table>

© 2007  Contact Author: davy.pelssers@contactoffice.net
6) **Online SAP Forums:**

   A) [www.sapfans.com](http://www.sapfans.com) (my nickname is **drago** if you want to search on postings by Author.)
   B) [www.erpgenie.com](http://www.erpgenie.com)

7) **Very useful OSS notes related to IC Webclient usage:**

<table>
<thead>
<tr>
<th>OSS note Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>759923</td>
<td>IC Webclient: FAQ note</td>
</tr>
<tr>
<td>894493</td>
<td>Frequently Asked Questions about Fax and Letter</td>
</tr>
<tr>
<td>947917</td>
<td>FAQ: Dispute Management for Financial Customer Care</td>
</tr>
<tr>
<td>947917</td>
<td>FAQ’s about the Agent INBOX</td>
</tr>
<tr>
<td>741940</td>
<td>FAQ: IC Webclient JCO Connection</td>
</tr>
<tr>
<td>1013376</td>
<td>FAQ: CRM IC Webclient Transaction Launcher</td>
</tr>
</tbody>
</table>

5.8. **ACE (Access Control Engine)**

At this moment I did not have time to really look into ACE, although the concept is pretty useful if you are using SAP CRM in the PCUI solution (e.g. when using SAP Enterprise Portal). I will briefly mention what the concept is about based on the finding from Boris Dingenouts (a senior SAP CRM consultant working at Exxap).

5.8.1. **Introduction**

Large and complex (international) CRM installations all face the same problem: how do we show the users only the data that they need to see? We don’t mean authorizations related to functionality, but related to business content. Imagine you run a big business and have a million customers worldwide. Then a sales rep responsible for a group of customers in Belgium should not see any customers from Asia in his search results. Or a sales rep with responsibility for a certain branch should not be bothered with customers of other branches. Furthermore, if the structure of the sales organization changes, you don’t want to end up changing all kind of authorization profiles.

To solve these issues, SAP came up in CRM for the PCUI with a pretty nice solution: CRM-ACE. This stands for Access Control Engine and is a framework to calculate user dependent access rights on object level. It originates from Channel Management but works in all PCUI functionalities. Unfortunately it doesn’t work in other environments like IC Webclient or via the SAP GUI (but Boris Dingenouts created a development request for this….).
When Boris started looking into ACE a while ago there was very little documentation and information on this topic. There is some information in the IMG and a very basic SAP tutor file but posts in SDN Forums asking for info got almost no reply. As usual he found out how it works himself by debugging and tracing….and therefore he thought it would be a good idea to share it with you.

You can take a look at his personal “blog” using the following the URL:


6. BW specific authorizations (TO BE ELABORATED)

Since the main focus of this eBook is on SAP CRM security, I could not find the time to elaborate any BW related authorization topics. Hopefully I can do this in a near future.

- Authorization objects
- Technical side: Administrator workbench
- Functional side: Bex Analyzer
- …. 

TO BE ELABORATED

7. Frequently Asked Questions

1. Where can I learn SAP CRM authorizations?
2. Where can I find back which authorization objects are being used in a transaction or program?
3. How do I know which fields are available in the profile generator and for which specific transactions?
4. How to start the design of my authorization concept and implementation?
5. How to restrict authorizations in PCUI screens and in the IC Webclient user interfaces?
6. Is there any way for an administrator to know whether the user has been locked by him (admin) or whether it is locked by incorrect logons?

Tcode SUIM has report RSUSR006 that reads this information in table USR02 from the field UFLAG.

You could use SE16, table USR02, field UFLAG :

© 2007   Contact Author: davy.pelssers@contactoffice.net
0 not locked
32 locked by central admin of CUA
64 locked by security administrator
128 locked due to incorrect logon (wrong password > 3 times)

7. How to restrict “/h”?

Obj S_DEVELOP
DEBUG

8. Critical authorization objects?

S_BTCH_ADM
S_RZL_ADM
S_ADMI_FCD
S_LOG_COM
S_PROGRAM
S_DEVELOP
S_RFC
S_TRANSPRT
S_CTS_ADMI
S_SPO_AUTH

9.

8. Tips and Tricks

1. How to bypass authorization checks?

   As a developer you can bypass authorization checks by going into debug mode. Via the command “/h” you start a program or transaction in debug mode. At the statement AUTHORITY-CHECK you change the sy-subrc into 0.
Of course this is not the intention, and therefore you should now that you can restrict people from debugging with the authorization object S_DEVELOP!

Check of hierarchy entry debug in it!

This is all right for developers to have, but only in a development system or quality assurance system, but definitely not in a production system.

2. Best practice cases … functional consultant per module will explain and test the setup of single roles and integration test… Writing of scripts for authorization administrator to test his setup

3.

---

9. Relevant OSS notes regarding SAP Authorizations

9.1. SAP CRM related

<table>
<thead>
<tr>
<th>Note Number</th>
<th>Authorization Object</th>
<th>Description/Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>865068</td>
<td>CRM_TXT_ID</td>
<td>Authorization Object for Text Type as of release 5.0: There is no authorization check for accessing individual text types of a text determination procedure.</td>
</tr>
<tr>
<td>786045</td>
<td>CRM_OPP_LK</td>
<td>Missing Authorization Check when creating references: No authorization check is performed when creating a relationship within an opportunity between the Opportunity itself and a Sub Opportunity for example.</td>
</tr>
<tr>
<td>831212</td>
<td>CRM_ORD_OE</td>
<td>BP Identification Popup: Authorization check; During the business partner identification process, no authorization check is performed when displaying the business partner in the popup.</td>
</tr>
<tr>
<td>831813</td>
<td>B_BUPA_GRP</td>
<td>Authorization check for One Order from MKTPL: The authority check was not set</td>
</tr>
<tr>
<td>877128</td>
<td>CRM_MKTPL</td>
<td>Authorization check for One Order from MKTPL: The authority check was not set</td>
</tr>
<tr>
<td>Document Code</td>
<td>Authorizations</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>712613</td>
<td>B_BUPA_GRP</td>
<td><strong>Authorization check for B_BUPA_GRP only if group is filled:</strong> In the portal environment, you always have to assign an authorization for authorization object B_BUPA_GRP although this should be optional.</td>
</tr>
<tr>
<td>524474</td>
<td>CRM_BP_SA</td>
<td><strong>Sales Area related authorization check in business partner</strong></td>
</tr>
<tr>
<td>803453</td>
<td>CRM_BP_SA</td>
<td><strong>Sales Area related check in business partner</strong></td>
</tr>
<tr>
<td>999239</td>
<td></td>
<td>PCUI: <strong>Sales area authorization</strong> in partner function tab</td>
</tr>
<tr>
<td>453616</td>
<td></td>
<td>In Transactions COMM_SET_UPD_PME and COMM_ATTR_UPD_PME (reports COM_SETTYPE_UPD_PME and COM_ATTRIBUTE_UPD_PME), an <strong>authorization check on attribute and set type level and on the level of the category is missing.</strong></td>
</tr>
<tr>
<td>446634</td>
<td>CRMD_PROF_TEMPL C_KLAH_BKP C_KLAH_BKL</td>
<td><strong>There is no authorization check when you maintain characteristic groups.</strong></td>
</tr>
<tr>
<td>652949</td>
<td>CRM_CGRP</td>
<td><strong>Simulation: Enhancement in Authorization check</strong></td>
</tr>
<tr>
<td>829723</td>
<td>COM_PRD_CT</td>
<td><strong>Product Proposal: missing authorization check;</strong> The CRM_ISU_GET_PRODUCT search help always displays all products, which correspond to the entered search criteria. However, the system does not check whether the user may actually display the products.</td>
</tr>
<tr>
<td>619410</td>
<td></td>
<td><strong>Archiving: Dynamic authorization, no check indicator</strong> (ARCHIVE_PRODUCT, Transaction COMM_PRDARC, ARC_OBJ: PRODUCT_MD)</td>
</tr>
<tr>
<td>568128</td>
<td>CRM_ORD_OE</td>
<td>You defined authorizations for <strong>authorization object CRM_ORD_OE</strong> for a user. For example, the user wants to use a document for which only the distribution channel is maintained. The check is incorrect. Occurs in release 3.0 and 3.1</td>
</tr>
<tr>
<td>812318</td>
<td>CMS*</td>
<td><strong>Missing Authorizations in CMS Transactions</strong></td>
</tr>
<tr>
<td>1010492</td>
<td>CRM_TPM</td>
<td>Default Authorizations for the objects (type transaction) 'CRM_MKTPL_ALLMDC' and 'S_PNC_50000053' are not fully/appropriate maintained. Check Manager errors of severity 2 have been issued on these objects.</td>
</tr>
<tr>
<td>625725</td>
<td></td>
<td>PCUI: <strong>Authorization check “create product”</strong></td>
</tr>
</tbody>
</table>
APPENDIX

Some general information about Authorizations:

Authorization means permission to perform a particular function in the SAP system. It is achieved by assigning authorization profiles to users.

The various terms used in Authorizations are:

- **Authorization fields:**
  
  Authorization fields identify the elements of the system that need to be protected. These fields are associated with the data elements of the ABAP/4 dictionary. For example if you consider Sales order creation as an activity, for which authorization is required, the fields associated with this activity are:

  VKORG – Sales Organization  
  VTWEG – Distribution Channel  
  SPART – Division  
  These fields form the part of the standard ABAP/4 function call AUTHORITY –CHECK.

- **Authorization object:**
  
  Authorization object identifies an activity that needs to be protected in the SAP system. For example Creation of a Sales Order is an activity. An object is made up of authorization fields. A user can perform an activity only if they satisfy the authorization check for each field in the authorization object.

  E.g. V_VBAK_VKO is an object for Sales Area comprising of the following fields:

  VKORG – Sales Organization  
  VTWEG – Distribution Channel  
  SPART – Division  
  ACTVT – Activity
Authorization objects are grouped into Object Class depending up on the application area.

- **Authorization:**

Authorization is used to define permitted values for the fields of an authorization object. For example you want to define an authorization for displaying a sales order for a *Sales organization 3000, Distribution Channel 01 and Division 02*, the values that will be assigned to fields of the object V_VBAK_VKO are:

VKORG – 3000  
VTWEG – 01  
SPART – 02  
ACTVT – 03 (display)

- **Authorization profiles (roles):**

As a rule authorizations are not directly assigned to a user. Instead these authorizations are clubbed in an authorization profile (role) and then assigned to the user master records via SU01.

**Types of profiles (roles):**

There are two types of authorization profiles – Simple and Composite (collective).

**Simple Profiles:**

A simple profile is composed of only Authorizations.

**Composite profiles:**

Composite profiles are sets of authorization profiles, both simple and Composite. A composite profile can contain an unlimited number of profiles. They can be assigned to users just as Simple profiles in the user master records are. Composite profiles are suitable for users who have different responsibilities of job tasks in the system. These profiles are sometimes known as reference profiles for assigning a larger group of access privileges and having the possibility to better match users with several responsibilities.