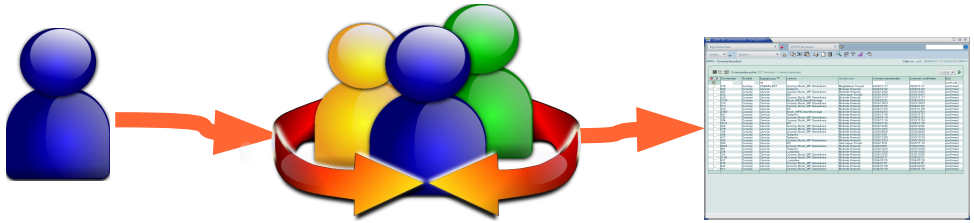
ERP5 Security

This guide will teach you:

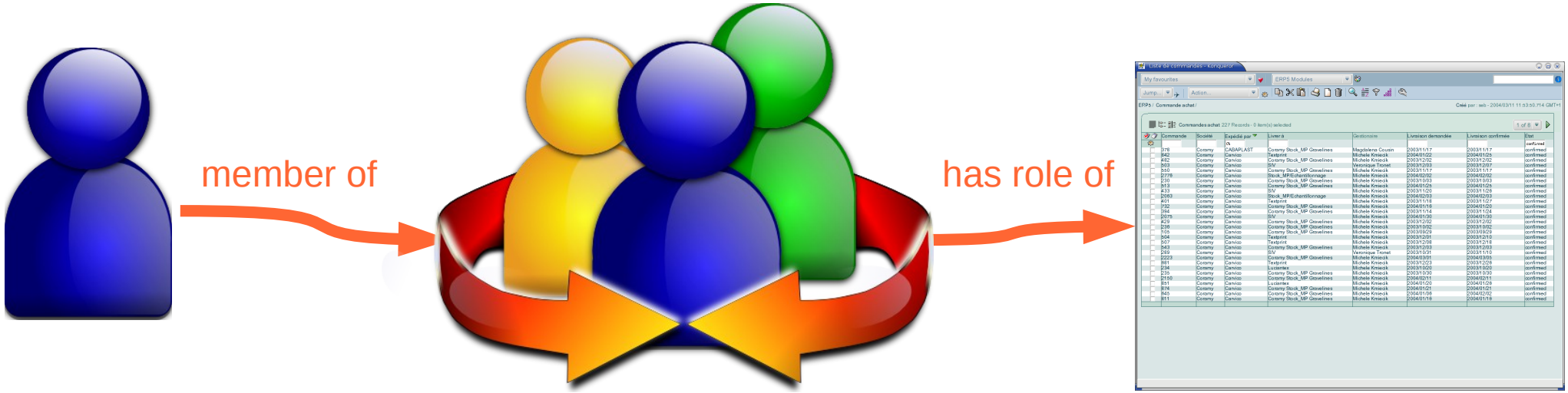
- How ERP5 creates a dual indirection from users to roles
- How ERP5 defines security groups based on classification
- How ERP5 assigns security groups to local roles



Support ERP5 !
www.erp5.org/howtohelp

Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

Group Indirection



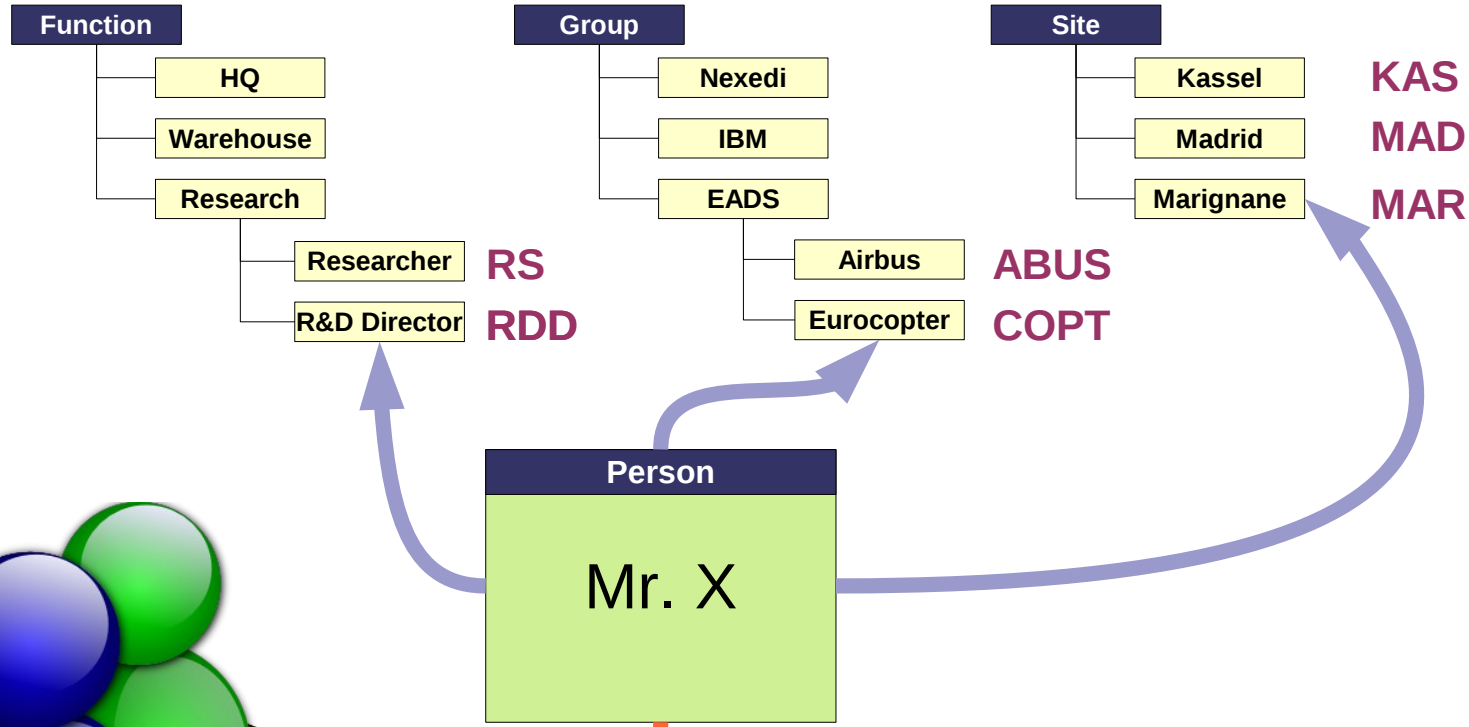
Mr. X

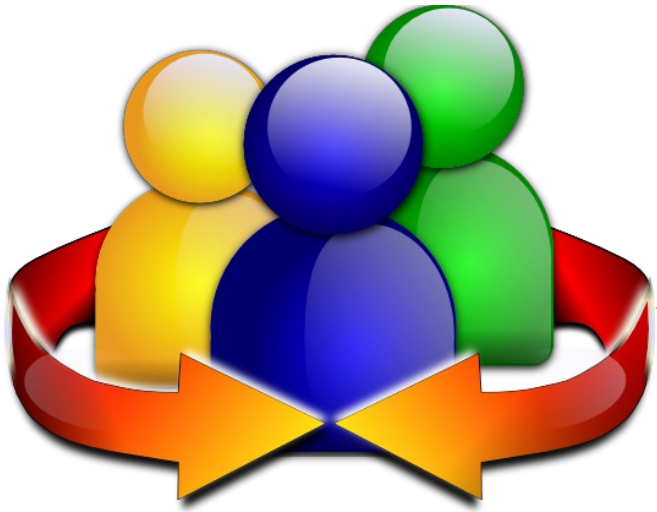
Group of
Accounting Managers

Assignor

© Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

Group Codification





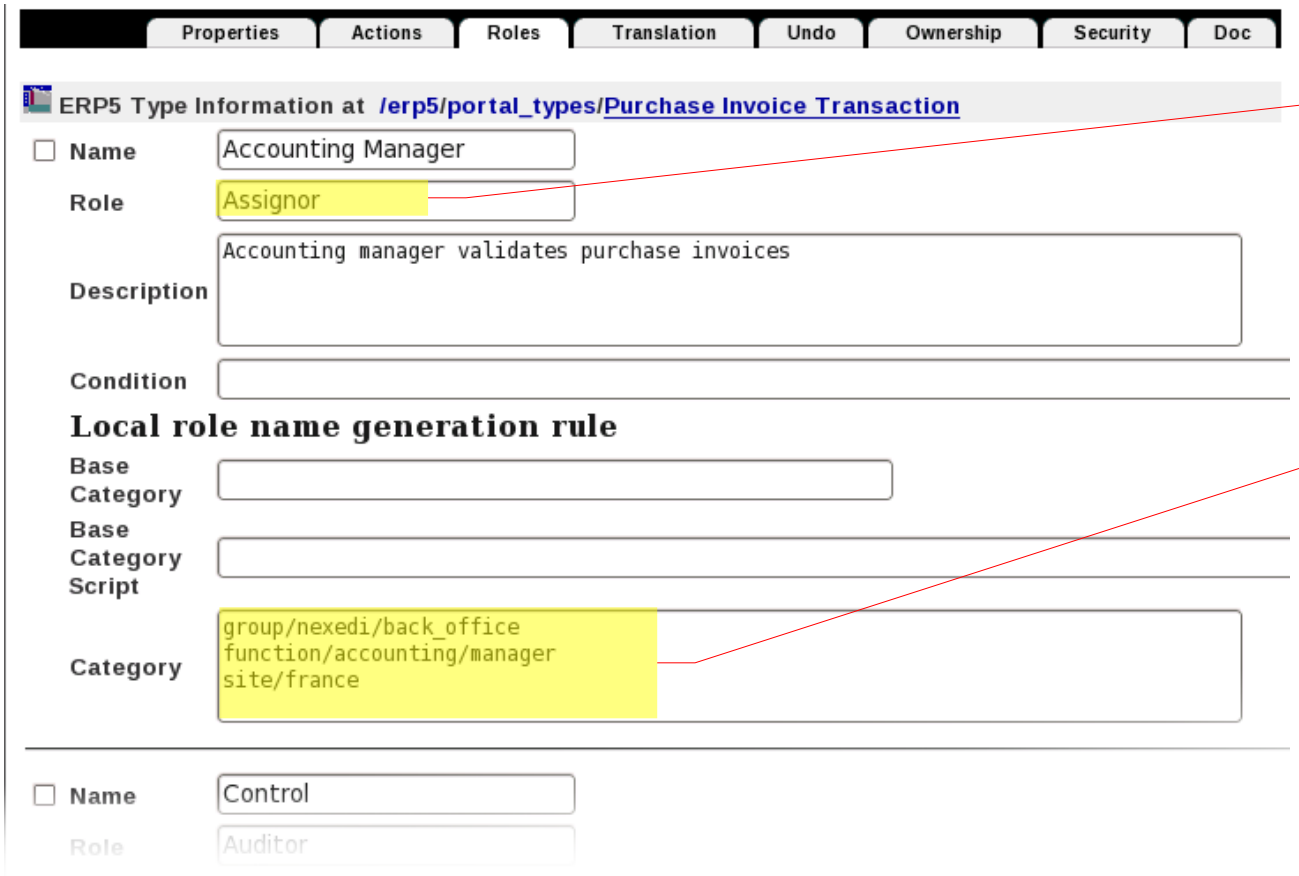
member of

RDD_COPT_MAR

© Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

Local Role Group Assignment



Role Definition

- Assignor
- *Assignee*
- *Author*
- *Auditor*
- *Associate*

Static Categories

- group/nexedi/back_office
- function/accounting/manager
- site/france

© Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

Dynamic Local Role

Properties | Actions | Roles | Translation | Undo | Ownership | Security | Doc

ERP5 Type Information at /erp5/portal_types/Purchase Invoice Transaction

Name: Accounting Agent for this gro

Role: Assignee

Description: Accounting agents can input transactions for their group (and only their group)

Condition:

Local role name generation rule

Base Category: group

Base Category Script: ERP5Type_getSecurityCategoryFromDestinationSection

Category: function/accounting/agent

Name: Control

Role: Auditor

Role Definition

Assignee

Dynamic Categories

Get the group from the organisation defined on this accounting transaction

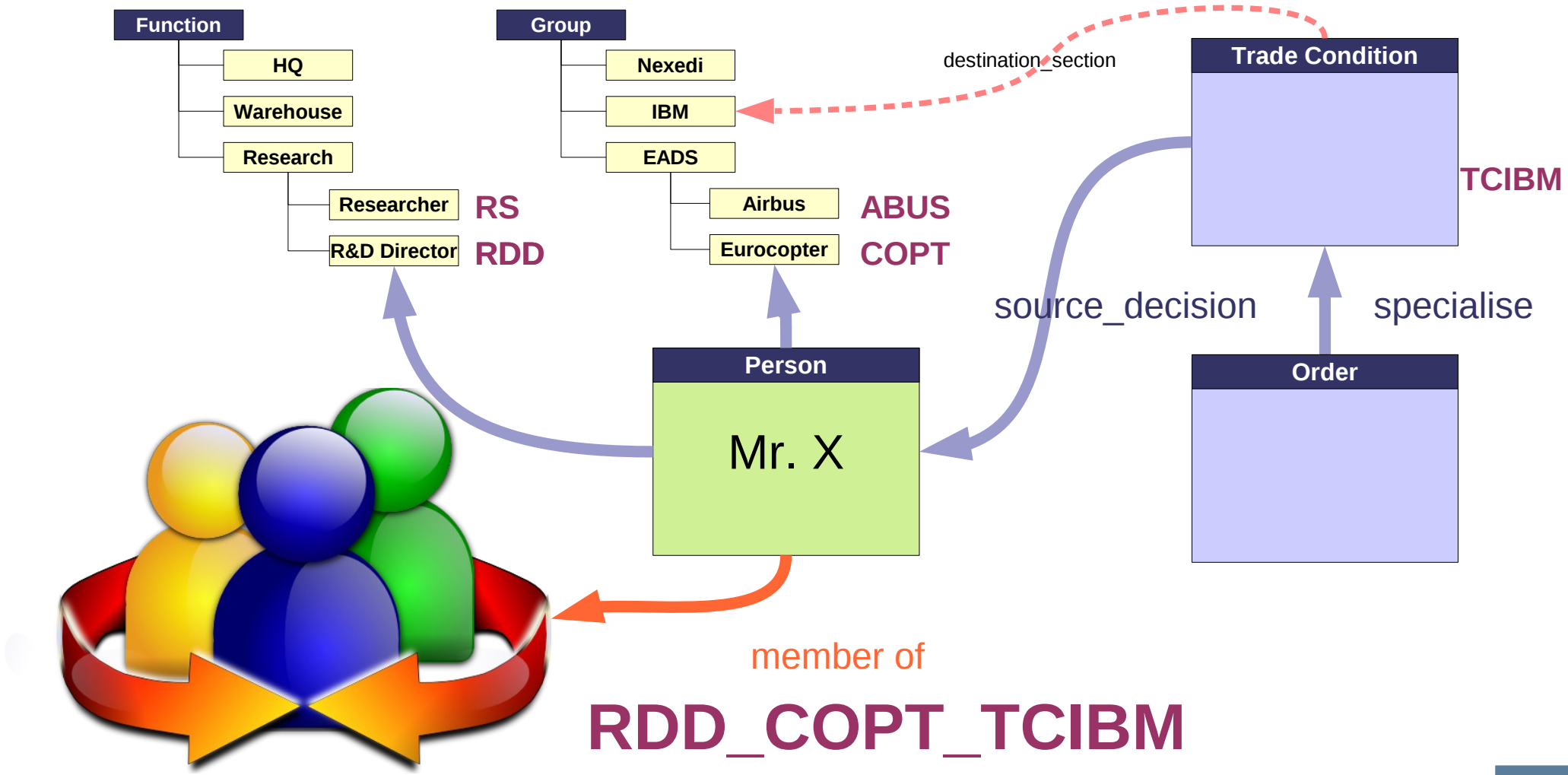
Static Categories

function/accounting/agent
(any site)

© Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

Example: Account Managers



Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

Example: Account Managers

Properties | Actions | Roles | Translation | Undo | Ownership | Security | Doc

ERP5 Type Information at /erp5/portal_types/Sale Order

Name: Account Manager

Role: Assignor

Description: R&D directors defined on the trade condition will confirm orders related to this trade condition

Condition: here/getSpecialise

Local role name generation rule

Base Category: specialise

Base Category Script: ERP5Type_getSecurityCategoryFromContent

Category: group/eads/eurocopter
function/research/rd_director

Save | Delete | Move up | Move down

Role Definition

Assignor

Dynamic Categories

The Trade Condition act as a dynamic category

Static Categories

group/eads/eurocopter
function/research/rd_director

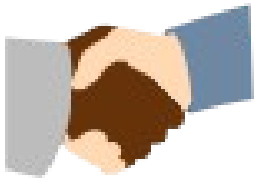
Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

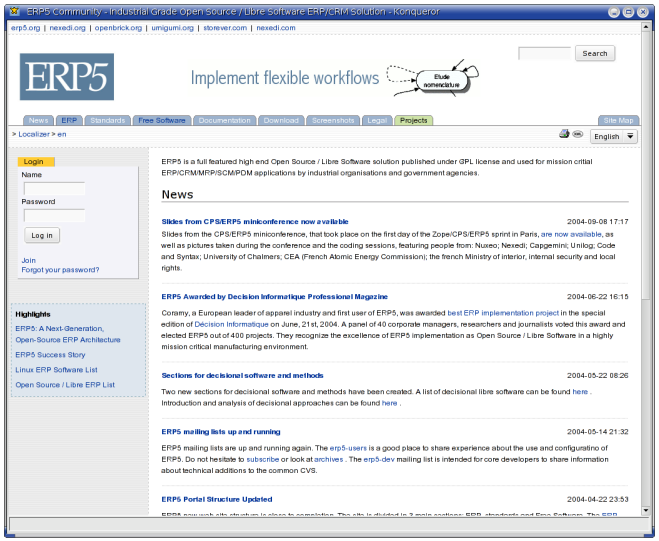
ERP5

Commercial Support

Enterprise Services

- Consulting
- Professional Training
- Custom Development





www.erp5.org
Open Portal

Join ERP5 Service Network !
www.erp5.org/support

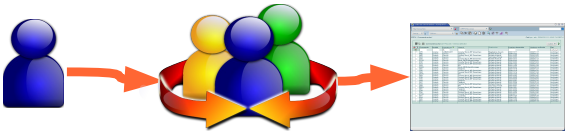
© Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

ERP5 Security

This guide will teach you:

- How ERP5 creates a dual indirection from users to roles
- How ERP5 defines security groups based on classification
- How ERP5 assigns security groups to local roles



Support ERP5 !
www.erp5.org/howtohelp

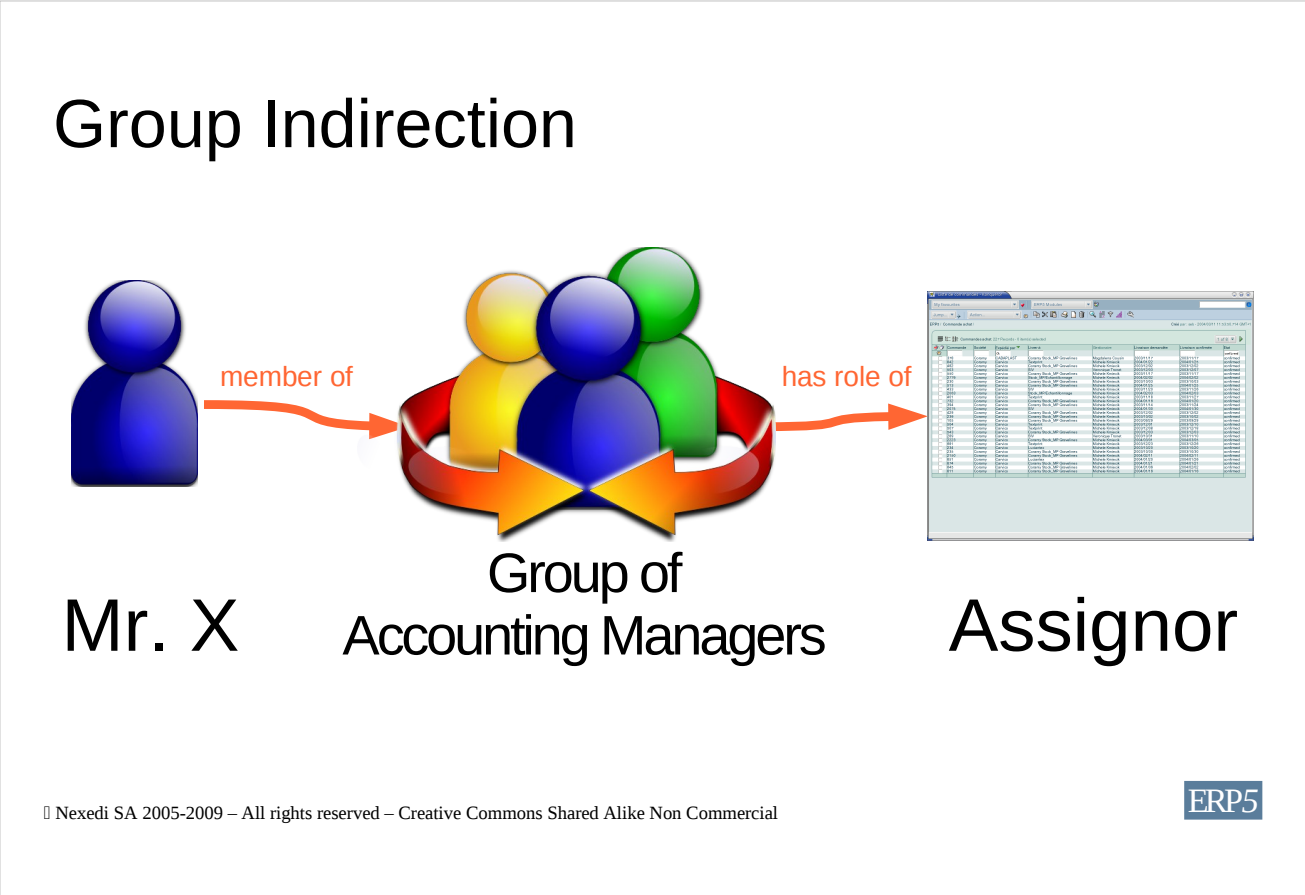
Nexedi SA 2005-2009 – All rights reserved – Creative Commons Shared Alike Non Commercial

ERP5

This visual guide has been created for learning and for teaching security in ERP5.

It is distributed under Creative Commons Shared Alike Non Commercial.

Note: Please note that the examples sited in this document are only of academic interest and imply no relation of any kind between ERP5 and the entities/organisations mentioned herein.

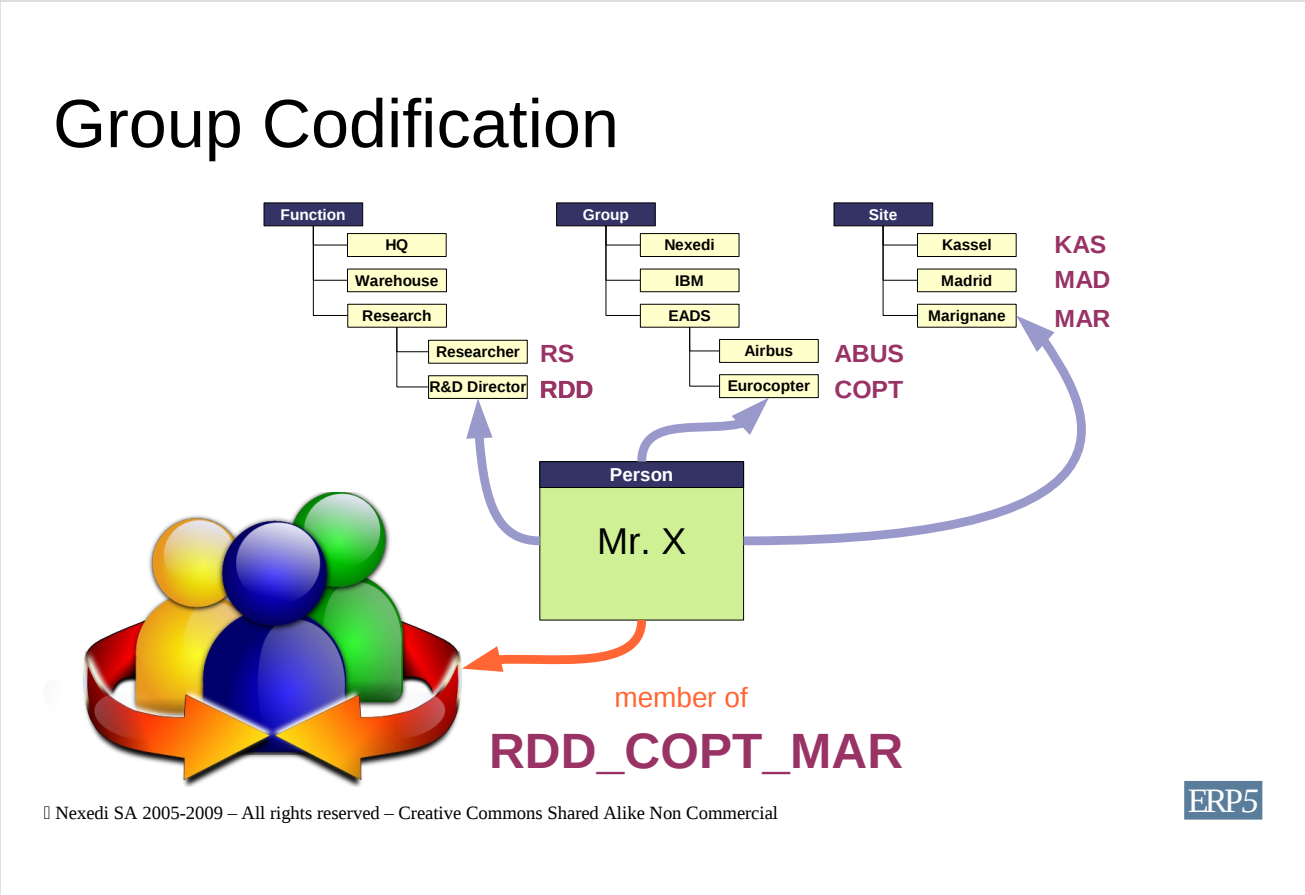


Usually in a zope application we create users and roles and thereafter associate roles to users. For example, Mr. Y is assigned the role of Principal Cashier and **Mr. X** is assigned the role of **Accounting Manager**. In real world ERP applications the number of users and roles can become very large which may make security completely unmanageable.

To counter this problem, ERP5 uses the concept of **Group Indirection** to reduce the number of roles through the use of groups. Hence instead of assigning Mr. X, the role of Accounting Manager, we make him a **member of** the **group of Accounting Managers** and then associate this group to the role of **Assignor**, which is one of the 5 generic local roles in ERP5.

For security configuration in ERP5, we use a minimal number of 5 generic local roles. They are **Author**, the document creator; **Assignor**, the one who assigns a document to an **Assignee**, also a local role; **Auditor**, one who has complete access to document contents and **Associate**, a participant in document processing. These are explained in more details in another document. This helps in managing security efficiently even if the number of users and groups grow to very large numbers.

Hence in ERP5, we can create several groups and thereafter associate each group to an appropriate generic local role. This is demonstrated by an example in the following pages.



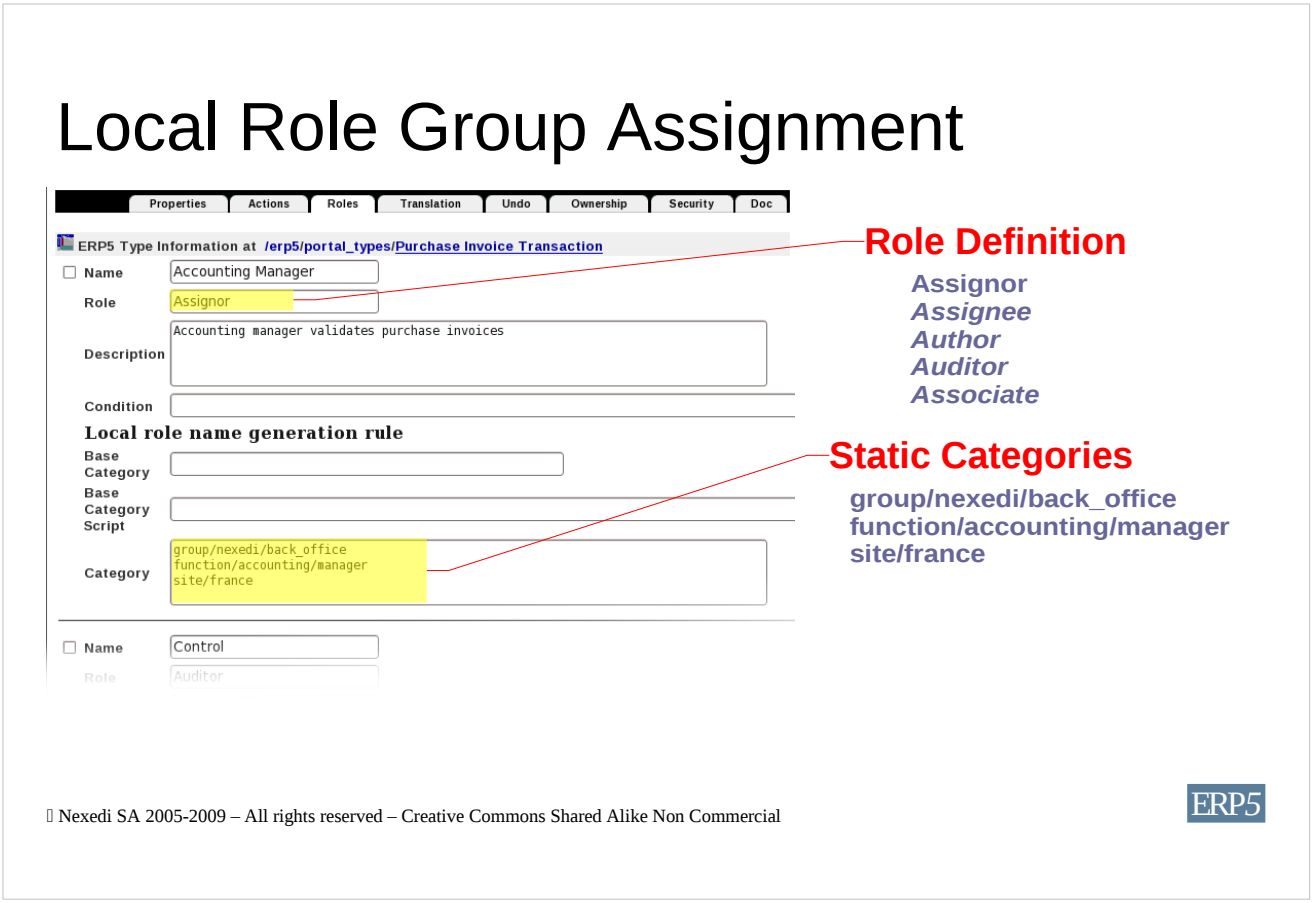
Having countered the problem of numerous roles, the main challenge for ERP5 security configuration is in defining the relevant groups in an application.

We usually encounter a scenario where a **person** is assigned a certain **function** at a stage in his career and he is working in a certain branch/**group** of the company located at a particular **site**. As depicted above, **Mr. X** is a **Research & Development Director** for **Eurocopter**, a subsidiary of the **EADS** group and is located at their **Marignane** site in the south of France.

Hence, Mr. X should be allowed access to the research documents of Eurocopter but not of Airbus. To implement this, we define a group by a combination of the elementary codification of the function, group and site and as a result we have **RDD_COPT_MAR**. The function of Research & Development Director is denoted by **RDD**, the group for which he is working, Eurocopter, is denoted by **COPT** and the location at Marignane site is denoted by MAR.

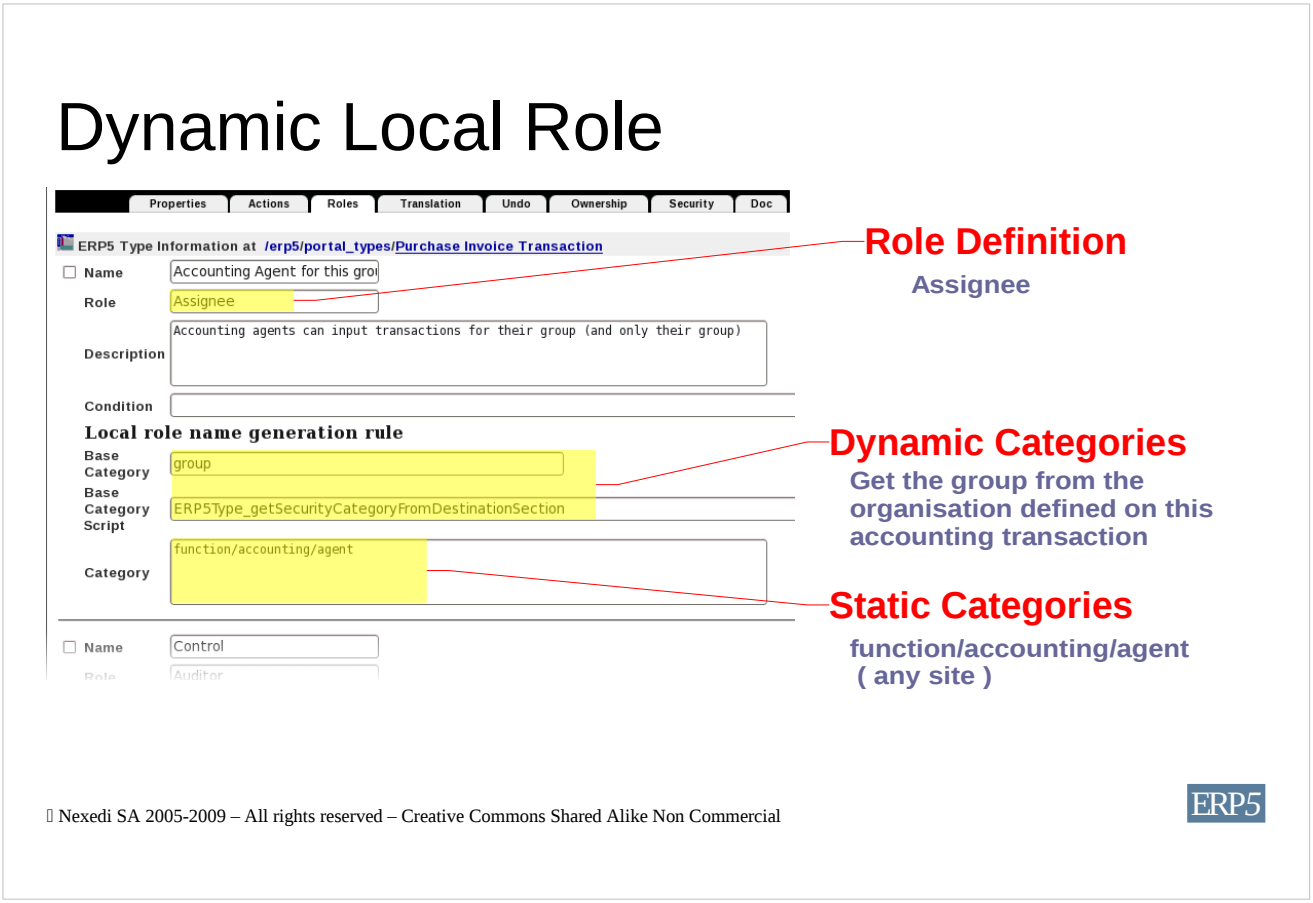
Hence, if we have to add a user we may do so by defining a person in the Person module and thereafter to make the person a **member of** a group we define the user's current assignments or step in career. This security is at the very core of ERP5 as user management is done though Human Resource Management.

This can be termed as a simple case of configuring static security as the security group is merely determined by career-step and human resource management.



To denote the fact that a given user is working as a **Accounting Manager** for a particular group located at a certain site and has certain rights we use the **Roles** tab in **portal_types**. For every possible role, 7 fields are provided to define the security policy : Name, Role, Description, Condition, Base Category Script, Base Category and Category.

The **Name** field denotes the common name, as is used by an implementer to refer to this role such as "Accounting Manager". **Role** is used to specify one of the 5 generic local roles in ERP5 such as **Assignor**. **Description** is a text zone where you can describe this role definition. **Condition** denotes the basis in which this role definition would be applicable or not applicable, as usual it is a TALES expression. In **Base Category Script**, we may reference a script that provides the machinery of associating groups dynamically, usually based on document properties. **Base Category** will be the dynamic categories, returned by the base category script. **Category** are the categories ensures that the Assignor should have the function of accounting manager, for the back office in nexedi group, and in the site france, this is denoted here by the **static categories** *function/accounting/manager*, *group/back_office/nexedi* and *site/france***.**

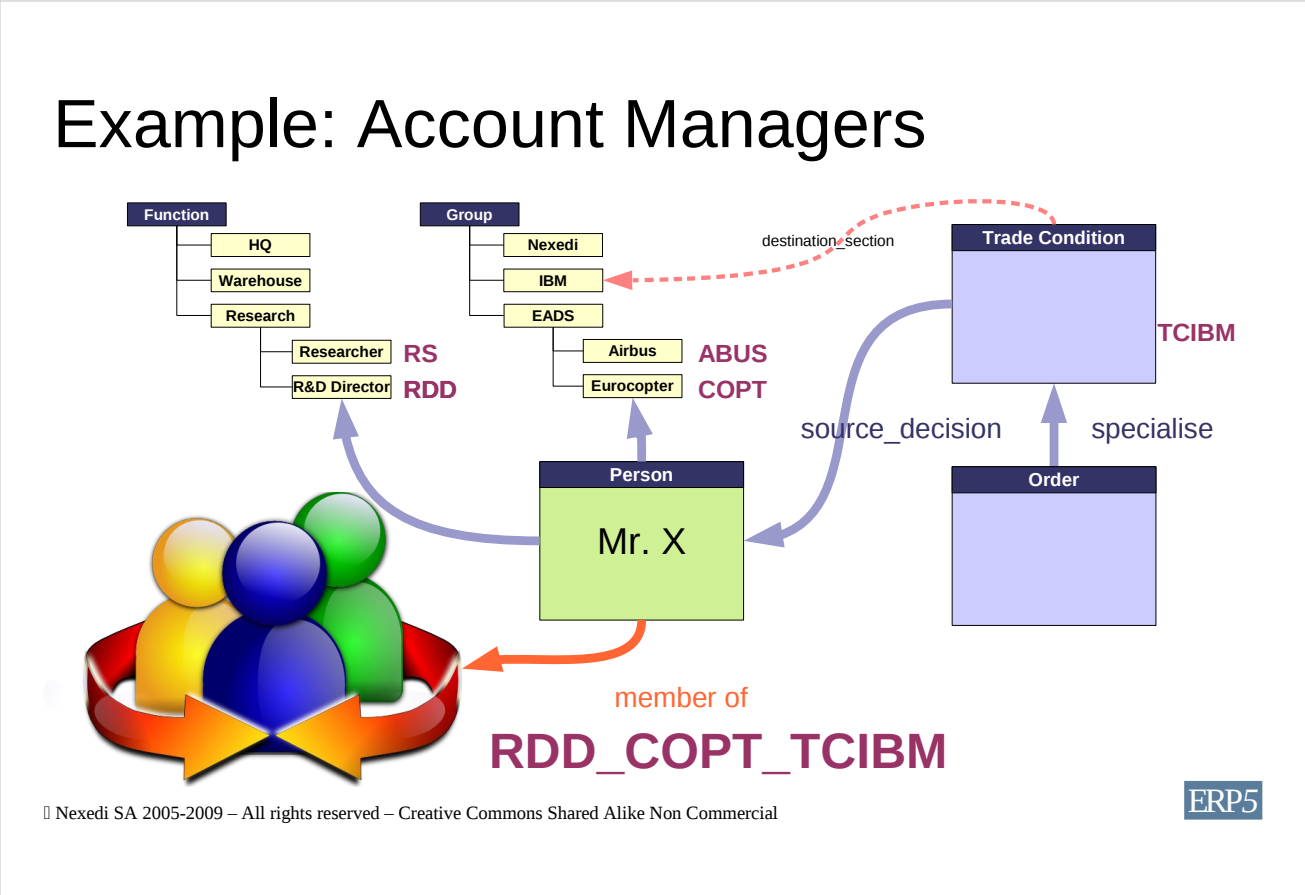


The example above is more realistic for the case of a multi-company accounting, where each accounting agent will only have access to the accounting transactions that relates to the branch of the group where this agent is affected. Here we introduce so-called **dynamic categories**, the group is not statically defined and applied for all purchase invoices, but will be taken from the group of the vendor organisation for each invoice.

To implement such security, in the **Base Category** field, we specify *group*, this is the category that will be dynamic, and in the **Base Category Script**, we reference a script that gets the category from the document, here it will take the group of the vendor of the invoice. For different cases, we have to use a different script.

The *function* is still defined statically in **Category**, this role definition will only be applied for persons with assignments as Accounting Agents. Another interesting point from this example is that site is not specified, which mean that the site is not taken into account here.

Explaining further with another example, consider a clerk in a multi-branch, multi-country and multi-service company entering accounting transactions. The manager responsible for validating this accounting must belong to the same service and the same branch as the clerk, and this is denoted by the group and site entries respectively in the Base Category field and he should have the function of accounting manager as denoted by the entry in the Category field.

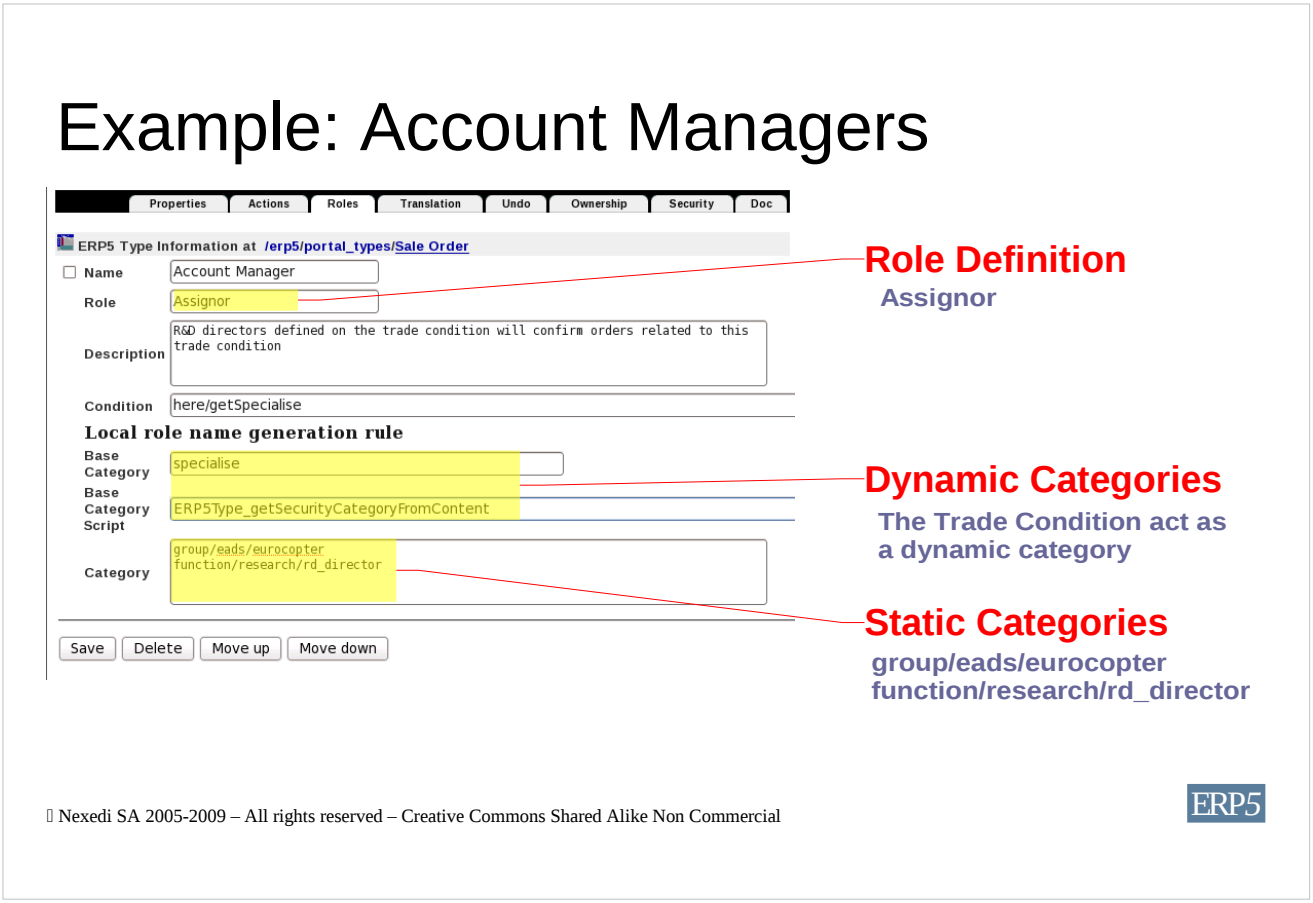


The main advantage of the above approach is that the definition of all local roles and mapping between common names and generic names are defined in a central place.

Let us study a more complex case where the security group is not only governed by career and human resource management but by a combination of Human Resource Management and Service Level Agreements. Extending our example of Mr. X, we state that he is in-charge of every research contract between Eurocopter and IBM. We denote this in a **trade condition**, which means that each time there is a contract, which is an **order** in ERP5 and every time a contract is being implemented it is according to an order trade condition which refers to Mr. X through the **source_decision** base category.

As depicted above, this trade condition has the elementary codification **TCIBM** and Mr. X is a **member of** the group **RDD_COPT_TCIBM**, which denotes a group of all research directors of Eurocopter, in-charge of IBM contracts. In this manner one can implement security with the concept of key account managers which may mandate that a company's documents or orders pertaining to a particular customer can only be accessed by the personnel in-charge for that customer.

In the next page we can see the effect of this scenario on the security configuration.



As we can see the fields above, there is not much of a change in the fields from the previous configuration except for the User and the Base Category.

The **Name** field denotes the customer's reference for this role and the **Role** field has one of the 5 ERP5 local role definitions, **Assignor**. The **Condition** in this example is set to *here/getSpecialise*, which mean that this role definition will only be applied if there is a trade condition related to the order.

In the **Base Category Script** field we specify the name of the script which is used to return dynamic categories that will be used to calculate security groups. The **Base Category** field has the dynamic category entry **specialise** which is used to denote the relation between the order and the trade condition. ERP5Type_getSecurityCategoryFromContent is a simple script that returns a category from the current object (ie. the order). Again the **Category** field ensures that the Assignor should have the function of R&D director for Eurocopter group, which is denoted here by the **static categories** *function/research/rd_director* and *group/eads/eurocopter*.

So far we have configured which groups have Assignor role on Sale Orders. The last part needed is to configure with groups a user will be member of. This is configured in the ERP5Type_getSecurityMapping script. Here you'll have to define that **group** and **function** are taken from users open assignments, and that **specialise** is taken by all trade conditions where the user is listed in the **source_decision** list of persons.

The ERP5 project is coordinated by Nexedi. Certified Consulting and Development services are provided worldwide by a network of partner companies.

Just like any ERP, ERP5 is complex system which requires experience in order to provide complete satisfaction to clients. Configuring ERP5 requires much more effort and experience than simply installing ERP5 software components alone.

Companies interested in joining ERP5 professional services network are encouraged to contact Nexedi. Nexedi provides complete training and certification services. Nexedi can assist ERP5 service providers in providing optimal presales, implementation and aftersales service to enterprise clients. Nexedi is looking forward to assist consulting or software companies to build a sustainable, profitable and independent business.

For more information, please refer to www.erp5.org/support.