Introduction on Authorizations

- Authorization objects enable complex checks of an authorization, which allows a user to carry out an action. An authorization object can group up to 10 authorization fields that are checked in an AND relationship.
- For an authorization check to be successful, all field values of the authorization object must be maintained accordingly. The fields in an object should not be seen as input fields on a screen. Instead, fields should be regarded as system elements, such as infotypes, which are to be protected.
- You can define as many system access authorizations as you wish for an object by creating a number of allowed values for the fields in an object. These value sets are called authorizations. The system checks these authorizations in OR relationships.

Key Authorization object for HR

P_ORGIN – *HR: Master Data*

This authorization is used to restrict access to personnel master data.

The *authorization level* field specifies the access mode. The following authorization levels exist:

Authorization Field	Long Text
INFTY	Infotype
SUBTY	Subtype
AUTHC	Authorization Level
PERSA	Personnel Area
PERSG	Employee Group
PERSK	Employee Subgroup
VDSK1	Organizational Key

- R (Read) for read access
- M (Matchcode) for read access to input helps (F4)
- W (Write) for write access
- E and D (Enqueue and Dequeue) for write access using the Asymmetrical Double Verification Principle. E allows the user to create and change locked data records and D allows the user to change lock indicators.
- S (Symmetric) for write access using the Symmetric Double Verification Principle
- * always includes all other authorization levels simultaneously

Problems can arise in some programs when write authorizations exist but no read authorizations. To avoid this, you should always specify R along with the authorization levels W, E, D, and S.
This applies for authorizations with PSIGN = I in the P_PERNR authorization object. In certain cases, it is appropriate not to enter read authorizations for authorizations with PSIGN = E. This is not an exception to the rule. PSIGN = E can be used to deny authorizations, which is, of course, allowed. This can occur, for example, if you have specified an authorization using P_ORGIN and authorization level *, and then use P_PERNR to determine that the user should be authorized to display his or her own data but not change the data. In this case, you would specify an authorization for P_PERNR with AUTHC = W, E, D, S and PSIGN = E.

Example of of Period Determination Using P_ORGIN

P_ORGXX *HR: Master Data - Extended Check*

The authorization object *HR: Master Data - Extended Check* is used during the authorization check on HR infotypes. The checks take place when HR infotypes are edited or read.

- The SACHA, SACHP, SACHZ, and SBMOD fields are filled from the *Organizational Assignment* infotype (0001). Since this infotype has time-dependent specifications, an authorization may only exist for certain time intervals depending on the user's authorization. A user's period of responsibility is represented by all the time intervals for which he or she has P_ORGXX authorizations.
- In the administrator group, all administrators who are responsible for an organizational area in Personnel Administration or in Applicant Management are grouped together.
- In the standard system, the check of this object is not active. You can use the authorization main switch (transaction OOAC) to determine whether this check is to be carried out in addition to or instead of the *HR: Master Data* check.
- If the additive check is activated, an authorization check according to *HR: Master Data* takes place first. If this check is positive, the object is then checked according to *HR: Master Data- Extended Check*.

P_PERNR *HR: Master Data - Personnel Number Check*

You use the *HR: Master Data - Personnel Number Check* authorization object if you want to assign users different authorizations for accessing their own personnel number. If this check is active and the user is assigned a personnel number in the system, it can directly override all other checks with the exception of the test procedures.

- The following values are possible for the PSIGN field:
- I = Authorization for personnel number assigned, that is for own personnel number
- E = Authorization for all personnel numbers excluding own personnel number
- You can assign a user a personnel number using infotype 0105, subtype 0001 (in earlier releases using the V_T513A view).
- This check does not take place if the user has not been assigned a personnel number, or if the user accesses a personnel number other than his or her own. In other words, this check is completely irrelevant for personnel numbers that are not assigned to the user.

Example of P_PERNR

Authorization for Payroll

- P_PCR - This authorization object is used by the authorization check for the payroll control record. This check takes place when the control record is displayed using transaction PA03, or when the control record is maintained. The check also takes place in particular during maintenance using the payroll menu.
- P_PYEVRUN - You can use this authorization object to control the actions possible for posting runs.
- The following specifications are possible for the *Run type* field:
  - AP Posting tax/SI Austria
  - PP Payroll posting
  - TP Posting Third-Party Remittance
  - TR Posting travel expenses
  - ZA Payroll evaluation - South Africa
  -
- P_PYEVDOC - You use this authorization object to protect actions on posting documents.
- P_TCODE - Access authorization to payroll schemas (transaction PE01) and personnel calculation rules (transaction PE02) is granted by authorization for the *HR: Transaction Code* authorization object.
- If only the employee entered as person responsible in the attributes of the schema or rule should be authorized to change a schema or a personnel calculation rule, you must activate the *Changes only by person responsible* field there. If the indicator is flagged, other employees are granted only read authorization for the schema or rule.

- This attribute can only be removed by the employee responsible or by running the RPUCTF00 report, *Change attributes for schemas and personnel calculation rules*.
    - *Note*: The authorization objects *HR: Authorization for Personnel Calculation Schemas* and *HR: Authorization for Personnel Calculation Rules* contained in the HR object class are not used in the standard system.

Create custom authorization – Customer specific object

- If you have requirements that cannot be met using the P_ORGIN and P_ORGXX authorization objects (for example, because you want to build your authorization checks on additional fields of the *Organizational Assignment* infotype (0001) that are customer-specific), you can include an authorization object in the authorization checks yourself.
- Create the authorization object using transaction SU21. Make sure you keep to the customer name range (Z/Y). To be able to use the new authorization object you have created in the master data authorization check, the object must contain the INFTY, SUBTY, and AUTHC fields. You can use any of the fields of the *Organizational Assignment* infotype (0001) for the other fields. You can also use customer-specific additional fields provided they are CHAR or NUMC type fields.
- After you have created the object, you must start the RPUACG00 report. This report overwrites the MPPAUTZZ standard include with the code that is needed to evaluate the authorization object you created. Note: Technically speaking, this involves a modification. However, SAP fully supports this procedure. And you should not have more maintenance work as a result of this modification.

    Note: that if you use customer-specific authorization objects, you must maintain these objects in transaction SU24 (*Maintain Assignment of Authorization Objects to Transactions*) in the same way as you maintain the authorization objects P_ORGIN, P_ORGXX, and P_PERNR

HR Security

Structural profiles are assigned in a different way to general authorization profiles. To assign structural profiles, you use table T77UA (User Authorizations = Assignment of Profile to User), not Role Maintenance (PFCG transaction) as with general authorization profiles. The authorization profiles are specified in the T77PR table (Definition of Authorization Profiles). You can protect (sub)structures by making relevant entries in this table

A user's Overall Profile is determined from the intersection of his or her structural and general authorization profiles, when you use both structural and general authorizations.
The structural profile determines which object in the hierarchical structure the user has access to; the general profile which object data (infotype, subtype) and which type of authorization (Read, Write, ...) the user has for these objects. The access mode for authorization objects in HR Master Data is determined in the AUTHC field (Authorization Level).

Steps to do Structural Authorisation:

Step1 : TC OOAC (table T77S0)
Activate the Structural Authorisation switch

Step 2 : TC OOSP
Create Structural Authorisation profiles

Step 3 : Assign Structural Authorisation profile to user Id
TC : SE38 and assign report RHRPROFL0 enter object id for example (Org unit)

Assign regular Role authorisation

Table - T77UA (User Authorizations = Assignment of Profile to
User), not Role Maintenance (PFCG transaction)
The
Table T77Pr - authorization profiles are specified in the T77PR table.
You can protect (sub)structures by making relevant entries in this table.

Organizational Plan are created using PPOCE

SAP HR Asymmetrical Double Verification

- In this procedure, two users are always required to be able to create or change an infotype's data. Here, the users do not have the same authorizations, which is why the process is called asymmetrical. User A is granted authorizations with the authorization level E (enqueue), R (read) and M (match code) for the P_ORGIN (or P_ORGXX) authorization object instead of complete write authorizations (authorization level W or *). These authorizations allow the user to create, change or delete locked records only.
- User B is granted authorizations with the authorization level D (dequeue), R and M for the authorization object P_ORGIN (or P_ORGXX) instead of complete write authorizations. These authorizations allow the user to unlock locked records (or lock unlocked records) only.
- New data is entered by user A and unlocked by user B. Existing data can be changed in two ways: User B locks the data, user A changes the data, and user B unlocks the data again. Alternatively, user A creates a locked copy from the unlocked data and changes this copy. User B then unlocks the data. To delete unlocked data, user B locks the data which is then deleted by user A.
- In this process, user A is always responsible for entering and changing data and user B for approving the changes.

SAP HR Symmetrical Double Verification

- In this procedure, two users are always required to be able to create or change an infotype's data. The users have the same authorizations for this. Both users are granted authorizations with the authorization level S (symmetric), R (read) and M (match code) for the P_ORGIN (or P_ORGXX) authorization object instead of complete write authorizations (authorization level W or *). These authorizations allow each user to create locked data records, change locked data records, and relock unlocked data records. In addition, each user can unlock data as long as he or she is not the last person to have changed the locked data. Neither user can delete data.
- New data is created by user A (or user B) and locked by user B (or user A).
- To change existing data: user A (or user B) locks and changes the data and user B (or user A) unlocks the data.
- Another user must be consulted to delete existing data.

HR Auhorization Objects

P_ORGIN

Authorization Object *HR: Master Data* is used during the authorization check on HR infotypes. The checks take place when HR infotypes are edited or read. The system queries the contents of the fields during the authorization check.

P_ORGXX

The object*HR: Master Data . Extended Check* is used during the authorization check on HR infotypes. The checks take place when HR infotypes are edited or read.

The Authorization Object *HR: Master Data - Personnel Number Check* P_PERNR is used when you want to assign users different authorizations for accessing their own personnel number. If this check is active and the user is assigned a personnel number in the system, it can directly override all other checks with the exception of the test procedures.

The Authorization Main Switches(OOAC)

You can use these switches to adjust the behavior of the authorization check on HR infotypes to meet your requirements. You can specify the switch settings at client level differently.
You can use the master data check (ORGIN) and the extended check (ORGXX) additively (both switches are set to 1) or alternatively (only one of the switches is set to 1).

The authorization object for Personnel Planning PLOG

You can use this authorization object to check the authorization for specific fields in the Personnel Planning components (Organizational Management, Personnel Development, Training and Event Management, and so on).

The Authorization Object HR: Transaction Code P_TCODE

This authorization object enables you to check whether a user is authorized to start the different HR transactions. The transaction code is checked. Note that this object is not used in all HR transactions. We distinguish between:
. HR transactions with a natural (their own) authorization object
. HR transactions without a natural (their own) authorization object
This authorization object contains the HR transaction codes without their own authorization object.

TheP_TCODE authorization object was implemented before the S_TCODE authorization object. Given the increased need to protect data in HR, it was retained as an additional protection measure.

The Authorization Object HR: Clusters P_PCLX

The Authorization Object *HR: Clusters* is used during the authorization check for access to PCLx HR files (x = 1, 2, 3, 4) if these files are accessed via the PCLx buffer (interface supported by HR).
The possible values for the area indicator are the fixed values of the RELID_PCL domain. The fixed values and definitions of what they mean are stored in the T52RELID table (transaction PECLUSTER).

HR: Master Data - Customer-Specific Object z_CUSTOMER

SU 21- Creat Authorization Object

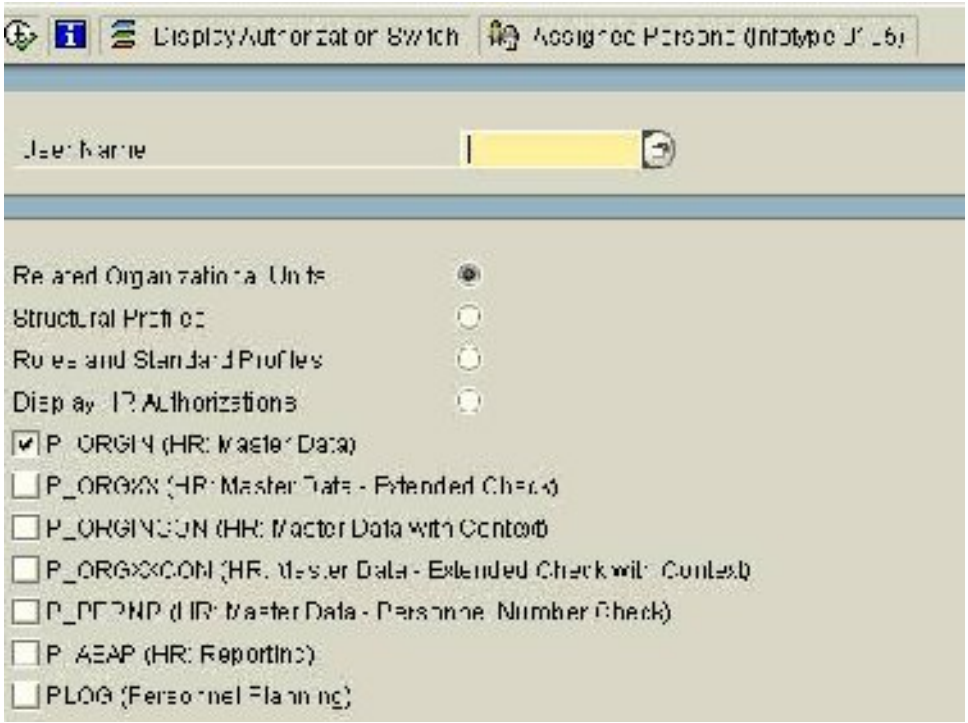
start the report **RPUACG00**

SU24- Assign objects to transaction

Set NNNNN Authorization manin switch to 1.

Tip and Tricks SAP HR Security

Report RHUSERRELATIONS



- This report enables you to evaluate all the HR authorization profiles that exist for a user. This includes the structural authorization profiles as well as the HR Basis authorization profiles that are assigned to the user directly (using role maintenance) or indirectly (in Organizational Management).
- In this report you can access several functions that enable selective evaluation of the authorization profiles. You can display the following information:
  - The entire list of authorization main switches with the set values (on the selection screen using the function bar)
  - All persons assigned to the user in the *Communication* infotype (0105) (on the selection screen using the function bar)
  - The organizational units to which the user is related
  - The structural authorization profiles
  - The user's role assignments and standard profiles
  - Authorizations based on HR authorization objects (from Personnel Administration/ Personnel Planning - here you can make a multiple selection)

Employee should be able to change their own address data (infotype 0006) using employee self service.

AUTHC = R, M PSIGN = I INFTY = * SUBTY = *	AUTHC = * PSIGN = I INFTY = 0006 SUBTY = *

1. Prerequisites: The AUTSW PERNR main switch must be activated for the authorization check by personnel number to take place.
2. The user assignment for all employees who use the SAP Employee Self-Service must be maintained in infotype 0105.

3. Users who are not administrators should not be granted P_ORGIN authorizations.
4. Each user accessing the SAP Employee Self-Service is granted the authorizations shown in the graphic for the P_PERNR authorization object. The first authorization grants the employee read access to all infotypes stored under his or her own personnel number. The second authorization grants write authorization for all data records of the 0006 infotype of the employee's own personnel number.

No maintenance of own data by Administrator

AUTHC = W, S, D, E PSIGN = E INFTY = * SUBTY = *	INFTY = * SUBTY = * AUTHC = * PERSA = CABB PERSG = 1 PERSK = * VDSK1 = *

Prerequisites:
The AUTSW PERNR main switch must be activated for the authorization check by personnel number to take place.

- The user assignment for the corresponding administrator must be maintained in infotype 0105.
- Each employee affected is granted the P_PERNR authorization shown in the graphic.