

## NOTE JULI 2006

---

### The matching authorization

It is of no importance whether the matching authorization results from a profile in a role or a manually created profile. That means that the origin of a matching authorization is of no relevance.

I. Our first test case for a better understanding.  
The following authorization is required for a successful pass of the authority-check:

for authorization object	<b>F_LFA1_APP</b>
for field	<b>ACTVT</b> value <i>02</i>
for field	<b>APPKZ</b> value <i>F</i>

Scenario 1:  
The user has the following authorizations assigned.

<u>Authorization A</u>	
for authorization object	<b>F_LFA1_APP</b>
for field	<b>ACTVT</b> value <i>03</i>
for field	<b>APPKZ</b> value <i>F</i>

<u>Authorization B</u>	
for authorization object	<b>F_LFA1_APP</b>
for field	<b>ACTVT</b> value <i>02</i>
for field	<b>APPKZ</b> value <i>M</i>

The user has no matching authorization because the required values are not combined in one authorization.

Scenario 2:  
The user has the following authorizations assigned.

<u>Authorization A</u>	
for authorization object	<b>F_LFA1_APP</b>
for field	<b>ACTVT</b> value <i>02</i>
for field	<b>APPKZ</b> value <i>F</i>

<u>Authorization B</u>	
for authorization object	<b>F_LFA1_APP</b>
for field	<b>ACTVT</b> value <i>02</i>
for field	<b>APPKZ</b> value <i>M</i>

The user has one matching authorization [Authorization A].

Scenario 3:

The user has the following authorizations assigned.

Authorization A

for authorization object **F\_LFA1\_APP**  
for field **ACTVT** value *02*  
for field **APPKZ** value *F*

Authorization B

for authorization object **F\_LFA1\_APP**  
for field **ACTVT** value *\**  
for field **APPKZ** value *\**

The user has full authorization. He has even higher authorization [Authorization B] than required. That means that he is able to do whatever is possible within this context.

The highest assigned authorization that meets the requirements will always prevail.

II. Second test case for verification:

Required for a successful pass of the authority-check is the following authorization:

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *02*  
for field **DICBERCLS** value *FC01*

Scenario 1:

The user has the following authorizations assigned.

Authorization A

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *03*  
for field **DICBERCLS** value *FC01*

Authorization B

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *02*  
for field **DICBERCLS** value *FC32*

The user has no matching authorization.

Scenario 2:

The user has the following authorizations assigned.

Authorization A

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *02*  
for field **DICBERCLS** value *FC01*

Authorization B

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *03*  
for field **DICBERCLS** value *FC01*

The user has one matching authorization [Authorization A].

Scenario 3:

The user has the following authorizations assigned.

Authorization A

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *\**  
for field **DICBERCLS** value *FC01*

Authorization B

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *03*  
for field **DICBERCLS** value *FC32*

The user has one matching authorization [Authorization A].

Scenario 4:

The user has the following authorizations assigned.

Authorization A

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *02*  
for field **DICBERCLS** value *\**

Authorization B

for authorization object **S\_TABU\_DIS**  
for field **ACTVT** value *03*  
for field **DICBERCLS** value *FC32*

The user has one matching authorization [Authorization A].

### Scenario 5:

The user has the following authorizations assigned.

#### Authorization A

for authorization object	<b>S_TABU_DIS</b>
for field	<b>ACTVT</b> value <i>02</i>
for field	<b>DICBERCLS</b> value <i>FC01</i>

#### Authorization B

for authorization object	<b>S_TABU_DIS</b>
for field	<b>ACTVT</b> value <i>*</i>
for field	<b>DICBERCLS</b> value <i>FC01</i>

#### Authorization C

for authorization object	<b>S_TABU_DIS</b>
for field	<b>ACTVT</b> value <i>*</i>
for field	<b>DICBERCLS</b> value <i>*</i>

The user has full authorization. He has even higher authorization [Authorization C] than required.

#### **Conclusion**

The authorizations are accumulated within the user master record. The user master data will be scanned during the different steps of the authorization check procedure (see Note\_06\_06). If a match or an even higher authorization is detected, the user will successfully pass the authorization check.