PiSA sales Documentation:

Inheritance of access authorizations in the project context

Release:	05.01-20110204
Datum:	15.04.2011
Dok.-Nr.:	D- D-11-112984, V0

PiSA sales GmbH
D-14050 Berlin, Fredericia Str. 17-19
phone.: + 49 (0)30/81 07 00 –00
fax: + 49 (0)30/81 07 00 – 99
e-mail: info@pisasales.de

Content

In general

1.1 Short information

PiSA sales offers comprehensive data protection by a concept to allocate authorizations for user groups. The user administrations and group management allow the generation of groups, group hierarchies and users as well as their assignment to groups. The access of groups on data is controled by group access keys which are administered in “Access lists”. Access lists can be defined for classes, records, fields and functions. Thus the data stock of the application can be protected by restrictions of access for complex, as well as for single objects.

The access concept supports the inheritance of the access of superior objects (project) to subordinated objects (activities etc.). Thus the global access controler can go out basically from the superordinate project.

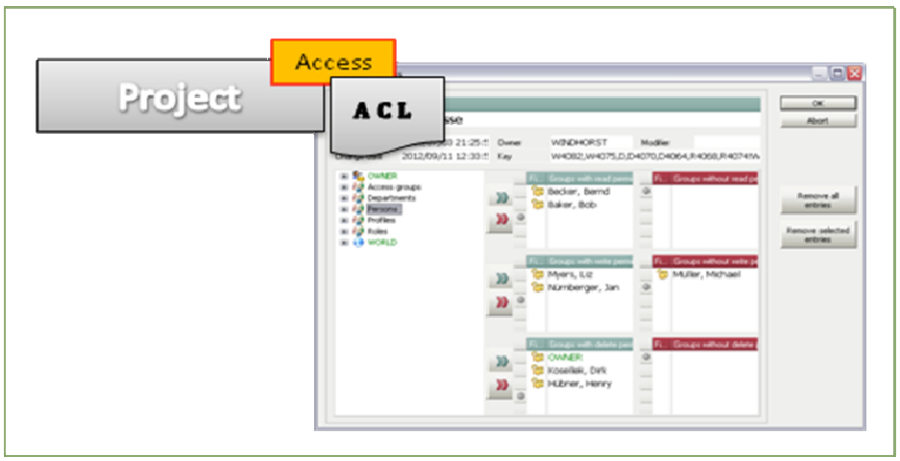
In addition, the access concept is extended by the fact that in the process definition the access to superior objects can be defined status-dependent. Walking along with it a role concept is implemented with which access authorizations on projects can be controled status-related activity-related.

In subordinated objects (activities) an access extension can follow, so that persons foreign to projects after overwriting the inherited project access furthermore can access on activities of the project.

1.1 Standard record access

The project has like all objects an own acessliste which defines which access which user on the object has. With, no restrictions are planned in the PiSA sales standard (WORLD = delete).

The record access defines basically the access to the master data of the project and can be defined user specific and group specific through variable as a standard record access (PSA_... _PSC_ACC). Thereby explicit by key (R; W; D) the standard access is agreed.



Inheritance of the access to subordinated objects

The relation data in a project among the known tabs with lists (activities, contacts etc.) enact of own standard access opposite to the project. This mechanism influences the access of the contacts from the relations on the project, e.g., the reading authorizations and writing authorizations.

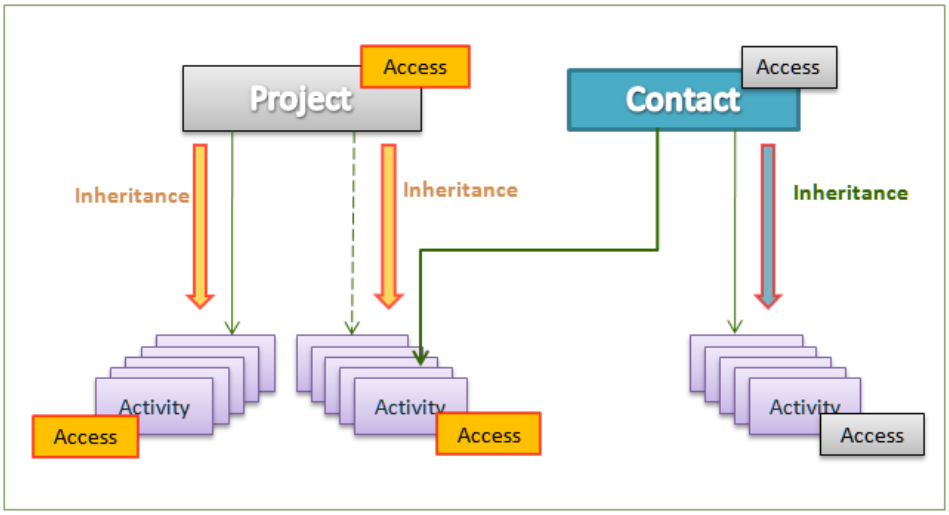
That's why the access of the project to the subordinated objects can be left bequeath.

1.2 Acquisition of the access to relations

The inheritance in the PiSA sales standard follows basically:

+ from the project on the activity or
+ from the contact on the activity

However, the access from the contact on the activity is left bequeath only normally if the activity is not assigned to the project. Otherwise the access of the project captures.



The standard access is always defined in the record access in the project (standard record access). It is provided by variable as a default (PSA_ ... _PSC_ACC) and can be set of course by the OWNER also directly.

With inheritance of the access of the superior object (project), access authorizations on subordinated objects are dependent by the superior object.

This in PiSA sales automatically happens, if the variable: CPY_PSC_ACC_ASS_OBJ on actively (y) is set and if an object is subordinated to a case. Besides, it is unimportant whether the object in the project is anew constructed or is linked with the project.by relation attributes

Contacts foreign to project therefore are defeated by the access of the project, even if they have in own rights to an assigned project activity.

1.2.1 Temporary access authorizations

In activities the access to the project is checked at the *responsible* of the activity. With delegating the activity assigned to the project to a person foreign to project the access to the activity can be granted temporarily *(… Do you want to grant write permission to this contact?*). Thus the responsible can edit this activity if it is assigned to a protected project.

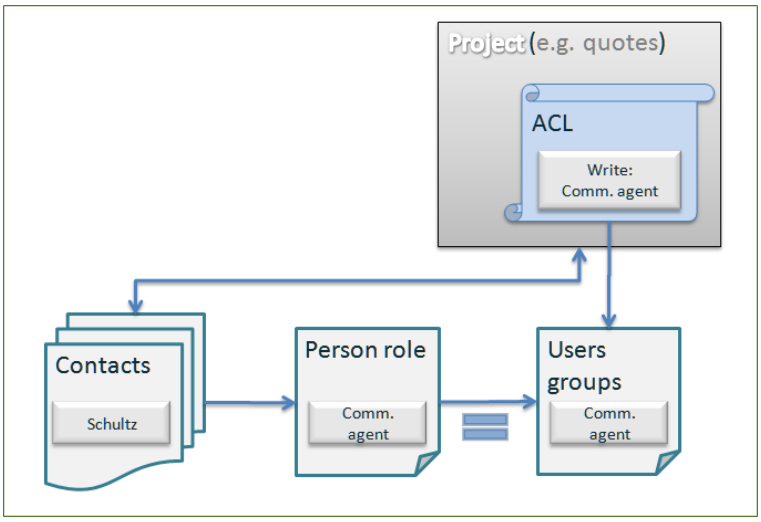
Note:

But with status change of the project this access to the activity is overwrote by the project access again. To this fact is taken into account by the role concept in the project or with the advanced access in activities.

1.2.2 Access authorizations with roles

With inheritance of the access of the project on the activity role-based access authorizations can be granted. Thus it is possible to record persons foreign to a project in the contact relation of the project and to appoint access authorizations of a defined role to them. Thus *responsible* can perceive the access authorizations of the role appointed to them in activities and edit its activities in the project.

The roles in project are based on user groups *(Placeholder)* which have defined access authorizations (e.g., **** COMMERCIAL_AGENT ****) in the project.



Note:

Internal contacts have if necessary access authorizations. If you appoint a role in the case to a contact, PiSA sales provides for the fact that the access of the case to the honest person is extended. This signifies: this contact is recorded in the access list of the case. But with the consequence that an once assigned authorization at a case does not disappear automatically again if the internal contact changes the role, has no more role in the case or is not assigned to the case any more.

If the authorizations/roles should be took away now sometime again, it has to happen explicitly by hand in the access of the access dialogue of the project.

1.2.3 Status-dependent accesses

With inheritance of the access from the project on the activity in the process status-dependent access authorizations. can be defined.

This access authorizations apply independent of project access if this status in the project is set.

For the access can be set R (read) and D (delete). Besides the so-called placeholder groups (rolesl) with can be get rights too. In combination with the key D or R a placeholder group can be stated which receives the respective rights by the concerning status .

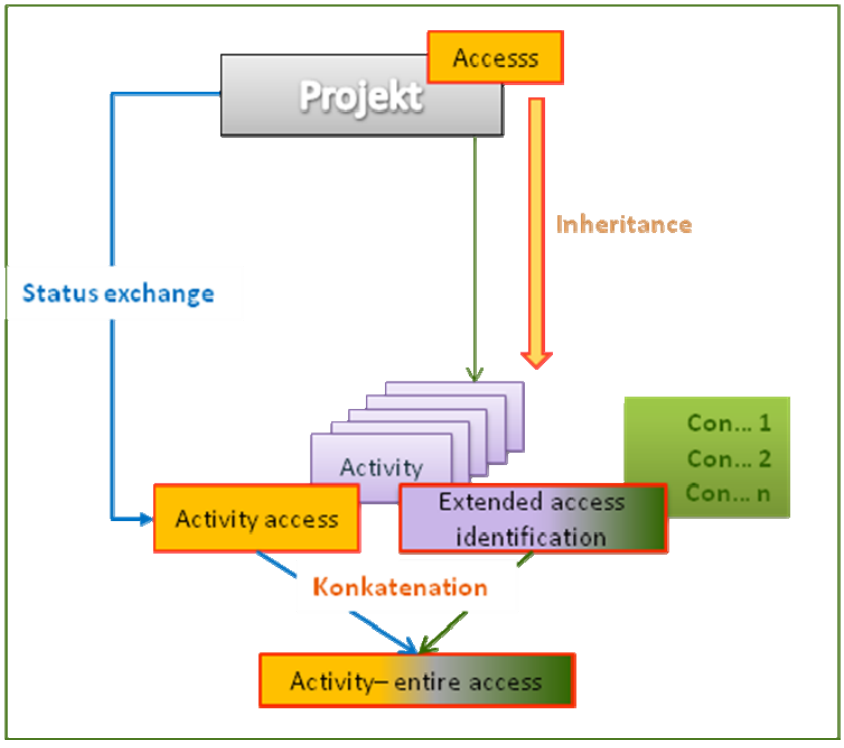
Note:

As soon as access authorizations are defined with the status in the process the defined standard-project access is not valid any more. Then the accesses are always realized by the process definition.

The advantage here is that in contrast to give roles in the project the assigned right is took away with the status change automatically again. Because the accesses are defined directly in the process, the authorizations are overwritten with status change from the process definition.

1.3 Expansion oft he activity access (customizing)

The activities which have inherited the access of a project have beside the standard record access an additional attribute *"access identification"*. Thus it is guaranteed that the access to activities in a project.can be controled regardless of role concept and status-dependent access



If a person foreign to project is added to a project-related activity, the person key is registered on the access identification.

If a further person is added to the project and the new project access is left bequeath, then with overwriting the activity access (e.g., status change in the project) the project access to be left bequeath with the persons who are registered in the access identification of the project activities becomes concatenated.

Therefore access authorizations are not any more temporarily but the access for persons foreign to project on activities remains regardless leave bequeath or overwriting the activity access granted.