This document is for anyone who wants simple explanations - covering some of the basics of the SAP® Authorization Concept. The information contained in this paper will be especially useful to CIOs, CISOs and SAP Authorization Managers, and will enable them to quickly and more effectively interact with outsourced consultants - and to better understand what to request from them.
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION TO AUTHORIZATIONS</td>
<td>02</td>
</tr>
<tr>
<td>TERMINOLOGY OF AUTHORIZATIONS</td>
<td>03</td>
</tr>
<tr>
<td>THE PROCESS</td>
<td>05</td>
</tr>
<tr>
<td>KEY POINTS TO REMEMBER</td>
<td>08</td>
</tr>
<tr>
<td>ABOUT XPANDION</td>
<td>08</td>
</tr>
</tbody>
</table>
The SAP Authorization Concept protects SAP systems against unauthorized access and system use – and can be viewed as the KEY to SAP security. It enables authorizations to be centrally-managed. Users (individuals with unique IDs that allow them to log onto and use a specific SAP system) are granted the authority to perform certain specific actions, and are not allowed to perform any actions for which they have not been granted authorizations.

In some applications (such as Microsoft’s), authorizations can be granted or denied to a user; meaning that the user is “allowed” or “denied” access to certain authorizations. However, in SAP, the opposite is true; without values, there are no authorizations and, unless specific permission for access or activity has been granted, it is NOT authorized. ABAP is the name of the SAP language. Determining whether or not a user has been granted a specific authorization can usually be accomplished through an ABAP command.

Multiple authorizations may be required in order to perform certain operations within SAP. For example, the task of paying a vendor’s invoice may require a dozen or more different authorizations. All authorizations that are required for the performance of any task must be granted to the user whose job it is to perform that task. However, according to the most up-to-date and generally accepted authorization concepts, only the minimum number of authorizations should be assigned to each user and, only those that are specifically required for the performance of the user’s job or role in the organization should be assigned. All authorizations granted to a user are combined in the user’s profile.

The SAP Authorization Concept enables organizations to make certain policy decisions that help to control its system’s security.

**EXAMPLES OF AUTHORIZATIONS GRANTED**

- Only users X, Y, and Z can issue invoices for the company.
- Employees working in the company’s branch of one country (e.g. U.S.) cannot perform activities for the branch in another country (e.g. Ireland).
- A warehouse worker can only check inventory in their own warehouse.
In order to understand the SAP Authorization Concept, one needs to become familiar with the terminology.

**AUTHORIZATION OBJECT**

The Authorization Object is the basic element - or building block - of the SAP Authorization Concept. Every Authorization Object is a separate entity and, all have equal weight within the SAP environment. The term ‘Company’ (which can stand for a global branch, a department within a specific branch, or other segment within the organizational structure) is an example of a standard Authorization Object within the SAP concept. Other examples of standard SAP Authorization Objects are ‘Warehouse’, ‘Document Type’ and ‘Transaction Code’. In addition to standard SAP Authorization Objects, organizations can create their own unique Authorization Objects; whose names should always begin with either the letter ‘Y’ or ‘Z’.


**AUTHORIZATION = AUTHORIZATION OBJECT + FIELD VALUES**

**AUTHORIZATION FIELD**

An Authorization Field is a template that allows a Value to be linked to an Authorization Object. A Value can be a number representing a specific department within an enterprise (e.g., Accounting Dept.), a specific action (e.g., ‘Create’ or ‘Change’) or other. When the Authorization Field of an Authorization Object has been assigned a Value an Authorization is created. Without a Value in the Authorization Field, there is NO Authorization. Normally, an Authorization Object contains up to 10 Authorization Fields and an unlimited number of Values per field.

**AUTHORIZATION**

An Authorization (i.e. an access or activity privilege which has been granted) is created when all Authorization Fields of an Authorization Object are assigned Values.

**AUTHORITY CHECK**

An Authority Check is a check that runs automatically in SAP whenever a user tries to perform an action within the system (if the Authority Check has been included in the specific program). The Authority Check determines whether or not the user has the required authorization to perform the specific action. In order to pass the Authority Check for an Authorization Object, the user must pass all the checks for all the Authorization Fields in the Authorization Object.

An Authority Check is the only way to check authorizations in SAP. If authority check commands have not been inserted into the source code of a program, then that program can be accessed without needing any Authorization. Without Authority Checks, system users are free to use the program as they see fit, i.e. to freely view and perform actions at will.

2 For more information on ABAP command “AUTHORITY-CHECK”, see http://help.sap.com/abapdocu_70/en/ABAPAUTHORITY-CHECK.htm
NOTE: According to our observations, despite the potential for significant security breaches, most programs created in-house do not include Authority Checks. This is most likely due to the difficulties experienced by programmers in gathering the required information – or to their lack of awareness regarding the need for Authority Checks. XPANDION has developed a solution that will ease this problem for programmers.

 TRANSACTION / AUTHORIZATION FIELD ACTVT

The term “Transaction” in SAP, represents a series of related steps that are required in order to perform a particular task. In a common SAP installation, there are over 100,000 transaction names. Most Transactions fall into one of the following categories: ‘Create an Object’, ‘Change an Object’ and ‘Display an Object’.

EXAMPLES

• Create an Invoice (Ex: SAP Transaction FB60)
• Change a Bank Account (Ex: SAP Transaction FS02)
• Display Vendor Details (Ex: SAP Transactions XK03 and FK03)

In order to correlate between the purpose of the Transaction and the Authorization, the Standard SAP Authorization Field – ACTVT – is used. Typical values for these fields include 01 (Create), 02 (Change), and 03 (Display).

 TRANSACTION CODE

A Transaction Code, or T-code, is a sequence of characters which is the technical name of a Transaction in SAP. If a user wants to perform a Transaction, the system will first perform a check to determine whether or not they have the Authorization for the Transaction (T-code). FB60 is an example of a T-code - the Transaction of Creating a Vendor Invoice. If a user wants to create a vendor invoice, the system will check their authorization for FB60. However, it is not sufficient to give the user authorization for T-code FB60. The user must also be granted all Authorizations required for FB60, such as the vendor’s company codes, business areas and account types.

 TRANSACTION / ACTIVITY CHECKS

In order to allow a user to perform a Transaction, the system automatically carries out the necessary Authorization Checks. Each Transaction Code has certain required Authorizations. Typically, there are 10-15 Authorization Objects to check for each Transaction; though this number is actually unlimited and there can be 30 or more different authorization checks in a single Transaction! Without these checks, the transaction can be fully utilized by any user in the system.
The system checks whether or not the user has been granted the required Transaction (i.e. T-code) for any authorizations.

If the answer is yes, then the system goes through a series of further Authorization Checks.

At any point along the way, the user can be stopped if any of the Authorizations connected to the specific T-code are missing.

If the user becomes stuck (i.e., the system does not allow user to continue,) they can usually activate Transaction SU53* (the last Authorization Object that was checked), and then request the missing Authorization from the Authorization Manager. When this occurs, the user’s work is generally interrupted until the missing Authorization is granted.

* Transaction Code SU53 (Display Authorization Data) should be executed following the appearance of an error message. It enables retrieval of the required authorization data.

NOTE: According to our observations, Transactions created in-house by organizations include, at most, one or two Authorization Checks - and usually only for the most sensitive Transactions. Most Transactions created in-house do not include any checks whatsoever!

authorization profiles are usually collections of logically connected Authorizations, but are not as complex as Roles.

identifying the correct authorization for each transaction

Since there is no way to identify all the required Authorizations, Transaction SU24 is often used. SU24 is the basis for adding required authorizations when a Transaction is added to a Role (see below), using the Role Generator - PFCG. Though not perfect, it enables visibility of the checks required for each Transaction, as well as the associated Authorization Objects.

However, this is only a partial solution, since SU24 must be manually updated. If the required Authorizations for each Transaction have not been updated, they will not exist in the system. When an activity is added to a role through PFCG, SAP will automatically add all Authorization Objects required for the specific activity (or T-Code). It is critical to update SU24. If an Authorization Manager or Programmer has added a new Transaction Check to a Transaction, they must add it to the required checks for the Transaction in SU24. Unfortunately, most Programmers ARE NOT AWARE OF THIS CRUCIAL REQUIREMENT.
AUTHORIZATION ROLES

An Authorization Role* in SAP is usually a collection of logically connected authorizations. Roles can be assigned to multiple users, and users can be assigned multiple roles. Roles are usually assigned on a need-to-know basis. Only Roles (not Authorizations) can be assigned to users. A typical user may have 5 or 6 Authorization Roles, with each Role having several dozen Authorizations.

* The term “Authorization Role” is commonly referred to as “Role” among authorization-related or technical people. In this case, it is unrelated to “Job Role” of an employee within the organization.

A Role can actually include more objects, such as menu entries and mini-Apps, but this definition is the most commonly referred to, when speaking with Authorization people. More data about SAP roles can be found in SAP documentation for Transaction PFCG.

AUTHORIZATION PROFILES

Authorization Profiles are usually collections of logically connected Authorizations, but are not as complex as Roles. Roles can include T-codes, menu entries, validity periods or other, while Authorization Profiles include ONLY Authorizations. Authorization Profiles are no longer recommended by SAP for granting Authorizations. However, they are still being used due to issues of compatibility. When creating a Role in SAP via Transaction PFCG (Role Maintenance), a corresponding Authorization Profile is automatically created. Though SAP abandoned the Authorization Profile concept some time ago, several historical Authorization Profiles without related Roles still remain in the system. These Profiles, for example - SAP_ALL, FI_ALL, SAP_NEW, S_A. DEVELOPER and others - are all critical and high-risk, and represent significant potential security threats.

EXAMPLE

The Profile ‘SAP_ALL’ includes almost all the Authorization Objects in SAP. Users with a SAP_ALL profile can perform all tasks in the SAP system. Therefore, this should not be assigned to anyone, ever.

ROLE MAINTENANCE TRANSACTION PFCG

Role Maintenance (T-Code PFCG - also known by its original name, Profile Generator) automatically creates customizable Roles, thereby easing and simplifying the process of creating and maintaining Roles.
USER BUFFER

Every time a user logs into the system, SAP combines all a user’s Authorizations into a single location, called the User Buffer. The User Buffer resides in the SAP memory and not on a physical disk, so access to it is fast – much faster than retrieval from a hard-drive. Transaction Code SU56 shows the contents of the user’s User Buffer and the total number of authorizations in the user’s master record.

Authority Checks ONLY check the User Buffer. One of the problems with the User Buffer is that it cannot isolate transactions. When dynamically creating the User Buffer (and this happens each time a user logs into the system), the SAP application combines all the Authorization Roles of the user and allocates all granted Authorizations into the user’s User Buffer, while ignoring duplicate objects. Therefore, using the User Buffer can create a situation in which one Transaction is using another Transaction’s Values.

EXAMPLE

An organization has decided to grant a certain user Transaction Code FB60 (Vendor Invoice) - but only for Company 1000, and T-code FB50 (G/L Account Document) - but only for Company 2000. However, if these two transactions use the same Authorization Object, then a situation is created whereby the user has Authorizations for FB60 for BOTH Company 1000 AND Company 2000 - and has authorizations for FB50 for BOTH Company 1000 AND Company 2000. Without compensatory controls, the user can perform the right transactions for the wrong company.

NOTE: This problem creates a very high risk situation for organizations, but until now, it has not been monitored. Xpandion solves this problem by offering an alert regarding cross-transaction authorizations.
The SAP Authorization Concept guards the system against unauthorized access and use of the system. An Authorization is created ONLY after a Value has been attached to the Authorization Field of an Authorization Object.

According to the current view regarding security, users should be assigned only the minimum number of Authorizations required to perform their duties.

ABAP Command AUTHORITY-CHECK is the only method to check user Authorizations. If a program does not have Authorization Checks embedded in its code, anyone can access and use the program.

T-code SU24 must be manually updated. This factor is critical. T-Code SU24 must be manually updated on a regular basis to remain current as this particular T-code (SU24) contains all the required Authorization Objects for an SAP T-Code.

SAP_ALL and SAP_NEW Profiles should never be granted to anyone, since individuals with these Profiles have carte blanche to view and do whatever they like within the SAP system.

The User Buffer, an integral part of the SAP Authorization Mechanism, does not allow for the isolation of transactions, which can therefore result in unintended and sometimes high-risk cross-access to data.

**According to the current view regarding security, users should be assigned only the minimum number of Authorizations required to perform their duties**

Focused on the areas of SAP security and SAP licensing, Xpandion creates user-friendly, easily deployed, automatic management solutions for SAP’s global customers. Xpandion’s ProfileTailor™ suite of solutions delivers unprecedented visibility of actual, real-time SAP authorization usage - enabling significant improvements in enterprise security, including reduction of fraud and leakage of sensitive data. It is the first solution that detects and alerts to deviations in behaviour in real time - including deviations from SoD (Segregation of Duties) rules. ProfileTailor™ creates a thin and controllable SAP system that can be easily managed with substantially reduced effort and resources. Once the confusion regarding authorizations has been dispelled, enterprises can then maintain on-going control of their SAP licenses and authorization usage. Xpandion’s LicenseAuditor optimizes SAP investments, enabling considerable savings through the identification of dormant, underused, duplicate and misclassified users. The entire suite of solutions is available as classic enterprise software or as SAAS/Cloud.