Security Guide
SAP FS-PM

Release 3.0

Copyright

Symbols Used in this Text

Symbol	Meaning
	Caution
	Example
	Tip
	Recommendation
	Syntax

SAP documentation uses other symbols that show the type of information contained in the text. For more information, see the start page for each version of the SAP library under *Help* → *General Information Classes* and *Information Classes for Business Information Warehouse*.

Typographical Conventions

Format	Description
Sample text	Words or characters cited by the screen. This includes field labels, captions and button labels, as well as menu names, menu paths and menu entries.
	Cross-references to other documentation.
Sample text	Boldface words or phrases in the body text, titles of graphics and tables.
SAMPLE TEXT	Name of system objects. This includes report names, program names, transaction codes, table names and individual key terms for a programming language contained in the body text, such as SELECT and INCLUDE.
Sample text	Screen output. This includes file and folder names and their paths, messages, source text, names of variables and parameters, as well as names of installation tools, upgrade tools and database tools.
Sample text	Exact user input. This includes words or characters that you need to enter in the system, exactly as specified in the documentation.
<Sample text>	Variable user input. You are required to replace the words and characters in the brackets with the appropriate input before you can enter them in the system.
SAMPLE TEXT	Key on the keyboard, such as the function key F2 or the ENTER key.

Copyright ... 2
Typographical Conventions ... 3

1. Introduction ... 6
1.1 Target group ... 6
1.2 Why is security necessary? ... 6
1.3 About this document ... 6

2 Before You Begin ... 7
2.1 Underlying security guides ... 7
2.2 Additional information ... 8

3 Technical System Landscape ... 8
3.1 Use ... 8

4 User Administration and Authentication ... 9

5 User Administration ... 10
5.1 Use ... 10

6 Authorizations ... 10
6.1 Use ... 10
6.3 Authorization Class: J7OA (FS-PM Authorization) ... 15
6.4 Authorization objects ... 15
6.4.1 Authorization object J_7OABPOST ... 16
6.4.2 Authorization object J_7OABACTN ... 16
6.4.3 Authorization object J_7OABBSTK ... 16
6.4.4 Authorization object J_7OALFSV ... 16
6.4.5 Authorization object J_7OALFND ... 16
6.4.6 Authorization object J_7OABBPRO ... 17
6.4.7 Authorization object J_7OABBTX ... 17
6.4.8 Authorization object J_7OABCORR ... 17
6.4.9 Authorization object J_7OABCORE ... 17
6.4.10 Authorization object J_7OAPMPRT ... 17
6.5 Authorization fields ... 18

7 Network Security and Communication Security ... 18

8 Security of Communication Channels ... 20
8.1 Use ... 20

9 Network Security 20
9.1 Use 20
10 Communication Destinations 21
10.1 Use 21
11 Data Storage Security 21
11.1 Use 21
12 Security for Other Applications 22
12.1 Use 22
13 Trace Files and Log Files 22
13.1 Use 22

1 Introduction

This guide does not replace the manual for day-to-day use, which we recommend customers create for their specific requirements for live operation.

1.1 Target group

- *Technology consultants*
- *System administrators*

This document is not part of the installation guide, configuration guide, technical manuals or upgrade guide. These guides are relevant only for a specific phase of the software lifecycle, while the security guide presents information that is relevant for all phases of the lifecycle.

1.2 Why is security necessary?

The increasing use of distributed systems and the Internet to manage business data results in the need for more stringent security requirements. When working with a distribute system, you need to be sure that your data and processes support the requirements of your company without permitting unauthorized access to critical information. You cannot have errors made by users, negligence or attempts at manipulating data in your system resulting in loss of information or processing time. These security requirements also apply for **Financial Services - Policy Management** (FS-PM). We offer these security guides to help you make your FS-PM system secure.

The fact that FS-PM is an in-force business system requires it to have a high level of security. This is made all the more important due to the fact that the in-force business data contains personal information. Legal regulations (Federal Data Protection Act) themselves warrant great care with regard to guaranteeing sufficient security for FS-PM.

1.3 About this document

This security guide gives you an overview of security-relevant information specific to FS-PM. This document refers to the components used by FS-PM (FS-CD, FS-CS, FS-BP, FS-RI and msg.PM) only by referring to the respective security guide.

Overview of the main sections

This security guide is made up of the following main sections:

- *Before you begin*

  This section contains information about the reasons why security is required and how the document is used. It also contains references to other security guides that constitute the basis for this security guide.

- *Technical system landscape*

  This section gives you an overview of the technical components and communication paths that FS-PM uses.

- *User administration and authentication*

  This section gives you an overview of the following aspects related to user administration and authentication.

  - Tools recommended for user administration
  - User types required for FS-PM
  - Standard users delivered with FS-PM

- *Authorizations*

This section gives you an overview of the authorization concept that applies for FS-PM.

- *Network security and communication security*

  This section gives you an overview of the communication paths that FS-PM uses, as well as of the security mechanisms to be used. It also includes recommendations for the network topology for limiting access to the network level.

- *Data storage security*

  This section gives you an overview of all critical data that FS-PM uses, as well as of the security mechanisms to be used.

- *Security for applications from external developers or for additional applications*

  This section contains security information that applies to applications from external developers or to additional applications that are used in cooperation with FS-PM.

- *Trace files and log files*

  This section gives you an overview of the trace files and log files that contain security-relevant information, allowing you to reproduce certain activities in the case of a security violation.

- *Appendix*

  This section contains references to other information.

2 Before You Begin

2.1 Underlying security guides

As part of SAP for Insurance, FS-PM uses the following SAP components, which it calls using SAP systems:

- *SAP Web Application Server 6.40*

  SAP Web Application Server 6.40 represents the technological basis for FS-PM. It provides the underlying services for FS-PM.

- *FS-CD*

  FS-PM processes Collections/Disbursements requests using FS-CD.

- *FS-CS*

  FS-PM uses FS-CS to execute the commission calculation.

- *FS-BP*

  By means of the connection to BP, FS-PM can access the business partners in the connected BP system.

- *FS-RI*

  FS-PM uses this connection to integrate the reinsurance component FS-RI of SAP for Insurance.

Furthermore, FS-PM uses the component msg.PM from the company msg systems ag, which is called via a TCP/IP connection:

- *msg.PM*

  msg.PM (product manager) is the development and runtime environment for the insurance content for FS-PM.

FS-PM is based on these listed components. Therefore, the associated security guides also apply for the use of the components in FS-PM. You need to pay attention particularly to the important sections or specific restrictions specified in the following table.

Underlying security guides

Security guide for scenarios and applications or components	Important sections or specific restrictions
SAP ERP Central Component Security Guide	SAP Business Partner for Financial Services
SAP NetWeaver '04 Security Guide	SAP WEB AS Network and Communication Security, SAP WEB AS Security Guide for ABAP Technology
SAP NetWeaver '04 Network Guide	
SAP NetWeaver '04 DB and OS Platform Security Guides	Specific security guides fort he database management system used and the used operating system
SAP Web Application Server Security Guide (ABAP + Java)	
SAP NetWeaver Security Overview	

You can find a complete list of all available SAP security guides in SAP Service Marketplace under the quick link securityguide or under the following URL:

https://sapneth5.wdf.sap.corp/securityguide.

2.2 Additional information

For more information regarding special topics, see the quick links in the following table.

Quick links to other information

Contents	Quick link for SAP Service Marketplace
Security	service.sap.com/security
Security guide	service.sap.com/securityguide
Related SAP notes	service.sap.com/notes
Permitted platforms	service.sap.com/platforms
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager

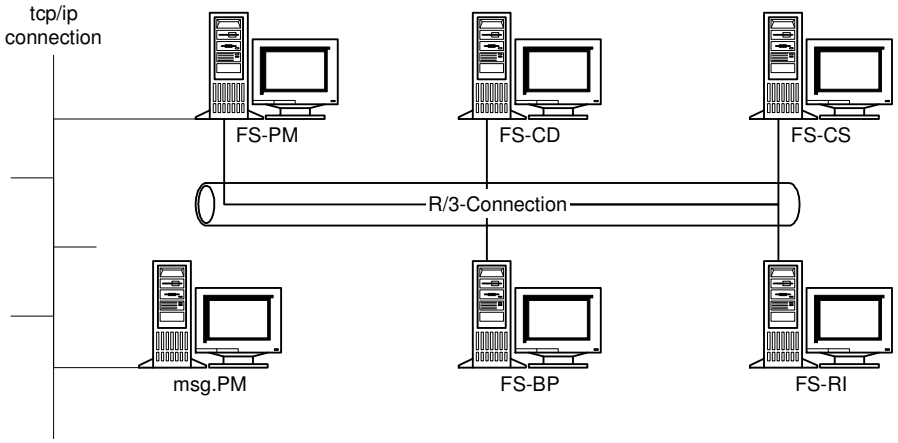
3 Technical System Landscape

3.1 Use

The following graphic gives you an overview of the technical system landscape for FS-PM.

As already described previously, FS-PM is connected via an R/3 connection to other required components in SAP for Insurance. FS-PM is connected to the msg.PM content server via a TCP/IP connection. The diagram represents a high-level distribution of components required

by FS-PM, each in its own system. The type of connection – R/3 or TCP/IP – is represented by different connection symbols.



This document does not address in further detail the physical network structure here. Here a reference is made to the detailed description in SAP Netweaver Security Guide (4.5.1 An Example Network Setup (with Client LAN) or the slide “Infrastructure Security – Secure Network Topology” in the PowerPoint presentation SAP Netweaver Security Overview). The chapter Network and Communication Security describes the aspects regarding the security of the network topology in more detail and refers to the appropriate chapter in the respective document.

You can find more information regarding the technical landscape in the sources listed in the following table.

More information regarding technical system landscape

Topic	Guide/tool	Quick link for SAP Service Marketplace
Technical description for FS-PM and the underlying technological components such as SAP Web AS 6.40	Master Guide	service.sap.com/instguides
Technical configuration High availability	Technical Infrastructure Guide	service.sap.com/ti
Security		service.sap.com/security

4 User Administration and Authentication

FS-PM uses these user administration and user authentication mechanisms of the platform SAP Web AS 6.40, particularly for the SAP Web Application Server ABAP. Therefore the security recommendations and guidelines for user administration and user authentication apply also to FS-PM as they are described in the *SAP Web AS Security Guide for ABAP Technology [External]* under service.sap.com/securityguide.

In addition to these guidelines, we give you information regarding user administration and user authentication that applies specifically to FS-PM in the following sections:

- *User Administration*

  This section lists the user administration tools, the required user types and the standard users delivered with FS-PM.

5 User Administration

5.1 Use

User administration for FS-PM uses the mechanisms offered by SAP Web Application Server ABAP, such as tools, user types and the password concept. An overview of how these mechanisms affect FS-PM can be found in the following sections. Furthermore, you receive a list of sample roles and users delivered with FS-PM.

5.2 User administration tools

The following table lists the tools for user administration in FS-PM.

Tool	Description	Prerequisites
Mandatory transactions		
User and roll maintenance for SAP Web AS ABAP (transactions SU01 and PFCG)	For more information, see Users and Roles (BC-SEC-USR) [External].	
Maintenance of structural and quantitative authorization checks in the Business Rule Framework (transaction BRF)	Using BRF you define rules for the authorization of characteristics such as the postal code, the sum insured, the subcoverage total, the premium and the endowment total.	In BRF you first define the events, expressions and actions using the maintenance and implementing classes.
Facultative transactions		
Maintain the authorization objects (transaction SU21)	You can use this transaction to create authorization objects or to display/change existing objects. Furthermore, you can check where in the program an authorization object is used.	
Maintenance for authorization fields (transaction SU20)	You define the authorization fields in this transaction. Here you assign data elements, search helps and packages to the fields.	

6 Authorizations

6.1 Use

FS-PM uses the authorization provided by SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines apply also to FS-PM as they are described in the security guide SAP Web AS ABAP.

The authorization concept for SAP Web Application Server ABAP is based on the assignment of authorizations to users based on roles. Use the profile generated for maintaining roles for SAP Web AS ABAP (transaction PFCG).

6.2 Sample roles

The following table lists the sample roles and the sample authorizations assigned to them.

The roles were defined for the line of business P&C/non-life and life. Additionally, there are cross-line-of-business roles.

P&C/non-life line of business:

Role	Role name
/MSG/AP_SHUSB	FS-PM P&C/non-life processor
/MSG/AP_SHUSB2	FS-PM P&C/non-life processor – PC 10001 - 20000
/MSG/AP_SHUSU	FS-PM P&C/non-life superuser

Role	/MSG/AP_SHUSB	/MSG/AP_SHUSB2	/MSG/AP_SHUSU
Authorization check (AC)			
AC select sales product New Business	Only sales products for P&C/non-life LoB	Only sales products for P&C/non-life LoB	Only sales products for P&C/non-life LoB
AC enter sales product New Business	As above	As above	As above
AC input policy number	As above	As above	As above
AC input application number	As above	As above	As above
AC sales product business process	As above	As above	As above
AC product-dependent business transactions navigation tree	Only contracts, coverage packages, coverages assigned to P&C/non-life LoB	Only contracts, coverage packages, coverages assigned to P&C/non-life LoB	Only contracts, coverage packages, coverages assigned to P&C/non-life LoB
AC address of policyholder (New Business)	All PCs	Only PC area 10001-20000 (PC for domicile of PH)	All PCs
AC address of policyholder (non-New Business)	As above	As above	As above
AC object category object management	Home contents, building, pet	Home contents, building, pet	Home contents, building, pet
QAC sums insured (New Business)	Contracts with sum insured up to EUR 500,000	Contracts with sum insured up to EUR 500,000	No restriction
QAC sums insured (non-New Business)	As above	As above	As above
QAC premium New Business	Contracts with yearly premium up to EUR 5,000	Contracts with yearly premium up to EUR 5,000	No restriction
QAC premium New Business	As above	As above	As above
AC BP in central access	New Business, Change, Inquiry	New Business, Change, Inquiry	No restriction
AC BT navigation tree context menu	No restriction	No restriction	No restriction
AC default BT navigation tree	As above	As above	As above

AC action	All except create subclaim, posting, reverse payment	All except create subclaim, posting, reverse payment	All except create subclaim, posting, reverse payment

Life line of business:

Role	Role name
/MSG/AL_LVSB	FS-PM life processor
/MSG/AL_LVSB2	FS-PM life processor – PC 10001 - 20000
/MSG/AL_LVSU	FS-PM life superuser
/MSG/AL_LVLB	FS-PM life benefit case processor
/MSG/AL_FONDS	FS-PM life authorizations for fund management and fund range

The role /MSG/AL_FONDS is used solely for the assignment of authorizations to actions in the fund management component. This provides the standard system with maximum authorization. However, you can change these as needed.

Role	/MSG/AL_LVSB	/MSG/AL_LVSB2	/MSG/AL_LVLB	/MSG/AL_LVSU
Authorization check (AC)				
AC select sales product New Business	Only sales products for life LoB	Only sales products for life LoB	Only sales products for life LoB	Only sales products for life LoB
AC enter sales product New Business	As above	As above	As above	As above
AC input policy number	As above	As above	As above	As above
AC input application number	As above	As above	As above	As above
AC sales product business process	As above	As above	As above	As above
AC product-dependent business transactions navigation tree	Only contracts, coverage packages, coverages assigned to the life LoB	Only contracts, coverage packages, coverages assigned to the life LoB	Only contracts, coverage packages, coverages assigned to the life LoB	Only contracts, coverage packages, coverages assigned to the life LoB
AC address of policyholder (New Business)	All PCs	Only PC area 10001-20000 (PC for domicile of PH)	-	All PCs

AC address of policyholder (non-New Business)	As above	As above	No restriction	As above
AC object category object management	Person	Person	Person	Person
QAC sums insured (New Business)	Sum insured over all coverages up to EUR 200,000 Contracts with yearly annuity up to EUR 40,000	Sum insured over all coverages up to EUR 200,000 Contracts with yearly annuity up to EUR 40,000	-	No restriction
QAC sums insured (non-New Business)	As above	As above	-	As above
QAC premium New Business	Contracts with yearly premium up to EUR 5,000	Contracts with yearly premium up to EUR 5,000	-	No restriction
QAC premium New Business	As above	As above	-	As above
BAC totals within benefit case processing	-	-	Total of all benefit values up to EUR 200,000 Total of all disbursements up to EUR 200,000	No restriction
AC BP in central access	New Business, Change, Inquiry	New Business, Change, Inquiry	Benefit, Inquiry	No restriction
AC BT navigation tree context menu	No restriction	No restriction	No restriction	No restriction
AC default BT navigation tree	As above	As above	No restriction	As above
AC action	All except create subclaim, posting, reverse payment	All except create subclaim, posting, reverse payment	All actions in BP Inquiry and life benefit except reverse payment	No restriction

Cross-line-of-business roles:

Role	Role name
/MSG/AB_FSPMSU	FS-PM superuser
/MSG/AB_FSPMCC	FS-PM call center employee (CC)
/MSG/AB_BASICS	FS-PM basis user role for cross-application transactions

/MSG/AB_FSPMAE	FS-PM accounting expert

The role /MSG/AB_BASICS includes the cross-application authorizations for use by FS-PM. Assign this role to the user in addition to the roles mentioned above.

Use the role /MSG/AB_FSPMAE to grant a user the authorization, so that he/she can change the accounting periods in FS-PM Customizing.

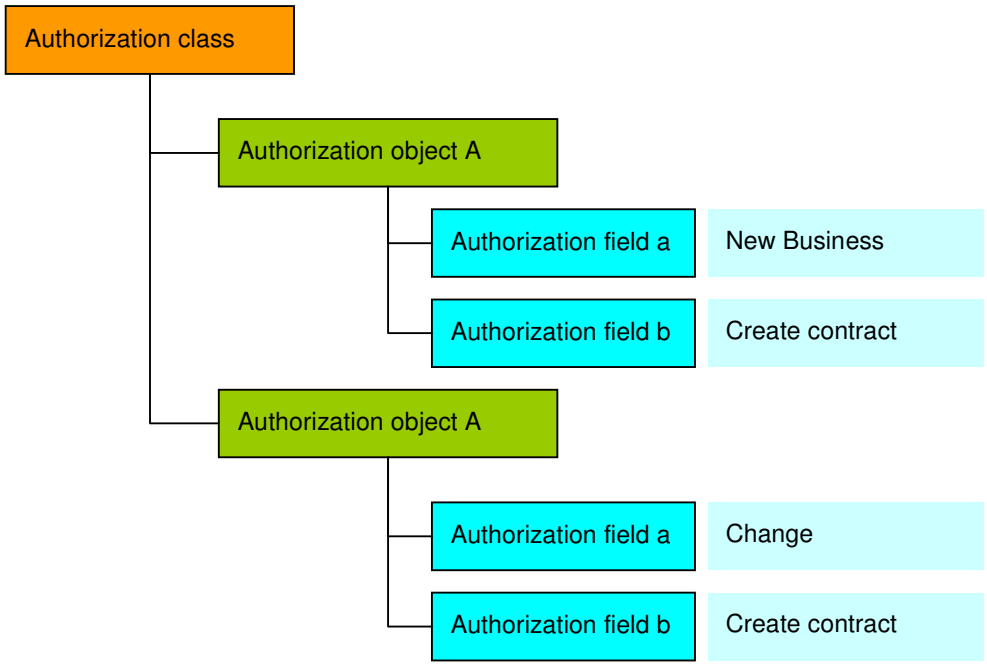
Role	**/MSG/AB_FSPMCC**	**/MSG/AB_FSPMSU**
Authorization check (AC)		
AC select sales product New Business	No restriction	No restriction
AC enter sales product New Business	As above	As above
AC input policy number	As above	As above
AC input application number	As above	As above
AC sales product business process	As above	As above
AC product-dependent business transactions navigation tree	No restriction	No restriction
AC address of policyholder (New Business)	All PCs	All PCs
AC address of policyholder (non-New Business)	As above	As above
AC object category object management	All object categories (display only)	No restriction
QAC sums insured (New Business)	-	No restriction
QAC sums insured (non-New Business)	-	As above
QAC premium New Business	-	No restriction
QAC premium New Business	-	As above
AC BP in central access	Inquiry	No restriction
AC BT navigation tree context menu	Display mode only	No restriction
AC default BT navigation tree	As above	As above
AC action	The actions within the Inquiry BP	No restriction

6.3 Authorization Class: J7OA (FS-PM Authorization)

Authorization classes are used to improve the management of authorization objects. By dividing the authorization objects into different authorization classes, you can make finding the objects easier. You can assign one or more authorization classes to an application.

The authorization objects have at least one or more authorization fields, depending on their use. These fields are assigned different values depending on the roles of the users. In this way, you can define different authorizations within the roles.

If an authorization object contains more than one authorization field, the authorization to be checked depends on several factors. The execution of a business transaction may be permitted in the *New Business* business process, while the user is not permitted to execute the same business transaction in the *Change* business process. This behavior is attained through the authorization object for checking the business transaction containing, in addition to a field for the business transaction ID, a field for the business process ID. In the Customizing of the authorization data for a role, several authorization objects of the same type with different authorization field characteristics are created for the individual authorizations. The following graphic represents this configuration:



6.4 Authorization objects

The authorization fields of the authorization objects are listed. For authorization objects that contain more than one field, you can make it so that no check takes place for the associated

authorization field by assigning a "dummy." In Customizing, you need to process each action for which a user is to be authorized. As outlined in the SAP standard system, you do not have authorization for all combinations of values for the authorization fields that are not entered. Generate a new authorization object if you have changed the values for the authorization fields.

6.4.1 Authorization object J_7OABPOST

Name	Short text	Authorization fields
J_7OABPOST	Accounting delimitation	ACTVT (activity) BILEXP (accounting expert flag)

Table 1: authorization object J_7OABPOST

6.4.2 Authorization object J_7OABACTN

Name	Short text	Authorization fields
J_7OABACTN	FS-PM action	ACTN_ID (action ID) ITEM_ID (object category)

Table 2: authorization object J_7OABACTN

6.4.3 Authorization object J_7OABBSTK

Name	Short text	Authorization fields
J_7OABBSTK	FS-PM in-force business range	BSTKNR (in-force business range number)

Table 3: authorization object J_7OABBSTK

6.4.4 Authorization object J_7OALFSV

Name	Short text	Authorization fields
J_7OALFSV	FS-PM Finance Service	AUTH_FIELD (field name) ACTVT (activity)

Table 3: authorization object J_7OALFSV

6.4.5 Authorization object J_7OALFND

Name	Short text	Authorization fields
J_7OALFND	FS-PM fund management	FUND_ID (fund number)

Table 4: authorization object J_7OALFND

6.4.6 Authorization object J_7OABBPRO

Name	Short text	Authorization fields
J_7OABBPRO	FS-PM business process	BPRC_ID (business process)

Table 5: authorization object J_7OABBPRO

6.4.7 Authorization object J_7OABBTX

Name	Short text	Authorization fields
J_7OABBTX	FS-PM business transaction	BPRC_ID (business process) MSG_PM_ID (product manager key) BTX_ID (business transaction)

Table 6: authorization object J_7OABBTX

6.4.8 Authorization object J_7OABCORR

Name	Short text	Authorization fields
J_7OABCORR	FS-PM correspondence documents	CORR_ID (correspondence type) ACTVT (activity)

Table 7: authorization object J_7OABCORR

6.4.9 Authorization object J_7OABCORE

Name	Short text	Authorization fields
J_7OABCORE	FS-PM correspondence - copies	CORR_ID (correspondence type) ACTVT (activity)

Table 8: authorization object J_7OABCORE

6.4.10 Authorization object J_7OAPMPRT

Name	Short text	Authorization fields
J_7OAPMPRT	msg.PM product element	BPRC_ID (business process) MSG_PM_ID (product manager key)

Table 9: authorization object J_7OAPMPRT

You can assign the following authorization objects of the authorization class J7OA to a role and characterize them as needed. Note that you do not have to make modifications to the

program when using these authorization objects, which are used in the standard delivery. In other words, you need to implement these when calls to the authorization check are made.

- *J_7OABACTV (FS-PM action)*
- *J_7OALFSRV (FS-PM finance service)*
- *J_7OALFNP (FS-PM fund range)*
- *J_7OALFNDP (FS-PM fund range)*
- *J_7OABBOBJ (FS-PM business object)*
- *J_7OABPOL (FS-PM policy)*
- *J_7OALPOL (FS-PM policy)*
- *J_7OABPAC (for BPAC (Business Process Administration Console))*
-

6.5 Authorization fields

Field name	Data element	F4 help	Table name for maintenance dialog/package
ACTVT	ACTIV_AUTH	TACT	SUSR
BILEXP	/MSG/ABD_BALEXP_FG	-	J7OAB_AUTH
ACTN_ID	/MSG/ABU_ACTN_ID	/MSG/ABUUACTIONT	J7OAB_AUTH
ITEM_ID	/MSG/ABU_OBJCAT_ID	/MSG/ABU_POBJCAT	J7OAB_AUTH
BSTKNR	/MSG/ABU_IFBR_ID	/MSG/ABUAIFBROP	J7OAB_AUTH
AUTH_FIELD	FIELDNAME	AUTHX	S_PROFGEN
FUND_ID	/MSG/ALD_INTNAME_TT	/MSG/ALDLFUND	J7OAL_AUTH
BPRC_ID	/MSG/ABU_BIZPRC_ID	/MSG/ABUUBIZPROT	J7OAB_AUTH
MSG_PM_ID	/MSG/ABU_PM_ID	-	J7OAB_AUTH
BTX_ID	/MSG/ABU_BTX_ID	/MSG/ABUUBTXT	J7OAB_AUTH
CORR_ID	COTYP_KK	TFK070A	J7OAB_AUTH

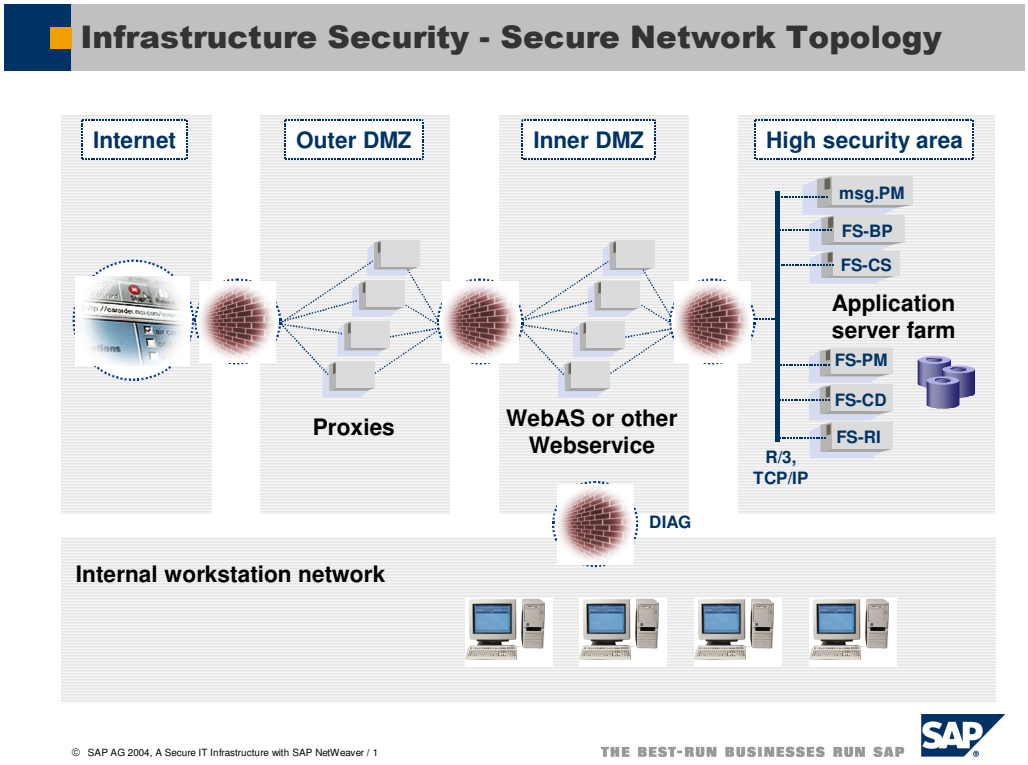
Table 10: authorization fields

7 Network Security and Communication Security

Your network infrastructure is very important for the protection of your system. Your network must support the required communication for your company and for your requirements

without permitting unauthorized access. A clearly defined network topology can preclude many security risks (for the operating system and at the application level) based on software errors and can thwart infiltration of the network such as tapping. If users are unable to log on to your application or database server at the operating-system level or the database level, unwanted guests will not be able to misuse the servers and will not be able to access the data base or the files on the back-end system. If the user cannot connect using the Server-LAN (local area network), he/she cannot take advantage of the known errors and security gaps in the network services on the server either.

The following graphic from SAP Netweaver Security Overview represents in a clear manner a network topology optimized for security purposes.



The network topology for FS-PM is based on the topology used for the SAP NetWeaver Platform. The (server) components shown in the technical system landscape section communicate via R/3 connections (exception: msg.PM). msg.PM communicates with FS-PM via TCP/IP. These components are located at the very farthest from one another within the inner demilitarized zone. The aim is to place all represented components in the high-security area.

The security guidelines and recommendations described in the security guide for SAP NetWeaver apply to FS-PM as well. Details that affect FS-PM in particular are described in the following sections:

- *Security of communication channel* [page 3]

  This section describes the communication paths and protocol that FS-PM uses.

- *Network security [page 3]*

  This section describes the network topology recommended for FS-PM. It shows the appropriate network segments of the different client and server components and where fire walls should be used to protect against unwanted access. Furthermore, it contains a list of ports that are required for the operation of FS-PM.

- *Communication destinations [page 3]*

This section describes the data required for the different communication paths, such as which user is used for which communication.

You can find more information in the following sections of the security guide for SAP NetWeaver:

- *Network and communication security [external]*
- *Security aspects for connectivity and interoperability [external]*

8 Security of Communication Channels

8.1 Use

The following table lists the communication path used by FS-PM, as well as the protocol used for the connection and the type of data transferred.

Communication paths

Communication paths	Protocol used	Type of data transferred	Data requiring particular protection
Front-end client with SAP GUI for Windows for application server	DIAG	All application data	Passwords, personal information, account information
Application server to application server	RFC between two SAP systems	All application data	Payment transaction data, account information, personal information
Application server for external application msg.PM	RFC on TCP/IP basis	in-force business data relevant for product manager	Personal data such as answers to health questions

You can protect DIAG and RFC connections using secure network communications (SNC). HTTP connections are protected using the secure sockets layer protocol (SSL protocol).

The TCP/IP communication between FS-PM and msg.PM can and should only be protected when needed using IPSec or a similar security service that is transparent for the system. This applies particularly to the following topologies:

- *FS-PM and msg.PM are located in different security zones*
- *FS-PM and msg.PM communicate using less secure zones*
- *The security requirements for the zone(s) in which FS-PM components and msg.PM are run are so high that the communication between the components must satisfy the highest security requirements.*

You can find more information in the security guide for SAP NetWeaver under *transport layer security* [external].

9 Network Security

9.1 Use

Regarding the network security for FS-PM, the following sections in the SAP NetWeaver security guide apply without restriction. Especially the sections regarding SAP NetWeaver ABAP (chapter Network Security for SAP Web ASABAP) are relevant for FS-PM. The

structure of a network topology optimized for security purposes is represented graphically in the previous chapter.

- The individual components can be run both in a network segment/security zone as well as in a distributed fashion across more than one network segment/security zone, as described above. You can find documentation regarding the security of individual network segments in the SAP NetWeaver security guides.
- For more information regarding services and ports used by SAP NetWeaver, see the security guide for SAP NetWeaver under *network services* [external].
- Information regarding the configuration of firewalls activated between the individual R/3 systems in a complex FS-PM network topology can be found in the security guide for SAP NetWeaver under *using firewall systems for access control* [external].
- We recommend that you place all participating server components in the high-security network segment for the network topology. This is also the recommended placement for performance reasons.

  You can find more information in the security guide for SAP NetWeaver under *using multiple network zones* [external].

10 Communication Destinations

10.1 Use

FS-PM users must have authorization for the required external systems such as FS-CD, FS-CS, FS-BP and FS-RI.

Generally there are three options for allowing a user to access a different destination from within FS-PM.

- FS-PM remote users: define an FS-PM remote user who has the appropriate authorizations for reading and writing in other destinations.
- Single sign on: for access to a different destination, an authorization check is necessary that uses the input for the username and the password. However, the user is not recognized in the destination.
- The user is recognized in the destination. When you log on to the RFC destination, all authorizations are automatically copied by the calling application.

11 Data Storage Security

11.1 Use

The in-force business data and the master data are stored in FS-PM in the SAP Systems database.

Individual user data is not used, only user data from SAP Business Partner is used.

External configuration data is not used either.

- *Master data is stored in the database during the Customizing of the FS-PM system. The in-force business data is written to the database when the user saves when creating or changing a policy or when he/she releases the application after processing.*
- *Until the time when a COMMIT is run (that is, until the information is written to the database), the application holds the data in the main memory. It does not store it temporarily as a file.*

- *In client maintenance, the protection level 0 (no restriction) is sufficient for FS-PM.*

12 Security for Other Applications

12.1 Use

As described above, FS-PM uses msg.PM to check the actuarial make-up of the policy and to calculate it. You can guarantee the security of the msg.PM system using suitable user authorization at the operating-system level. You can rule out the influence of msg.PM runtime and the used content by restricting access to the msg.PM system appropriately. Here we refer again to the placing of the msg-PM system in the inner security zone.

msg.PM does not save any in-force business data. It calculates and returns new application data from the application data delivered by FS-PM. msg.PM therefore does not change the in-force business data directly. This, and the journal management and history management provided by FS-PM ensures to a wide extent that the application data cannot be corrupted by means of msg.PM.

13 Trace Files and Log Files

13.1 Use

FS-PM produces trace/log files depending on the settings that can contain information relevant to security and data protection.

Use the entry /**MSG/3FJTRACE in the TRMAC table for activating and deactivating the trace function.** Use the transaction /**MSG/3FL_TRACE** to display the trace result. You can use the transaction **SLG1** to query the application log at the user level. Additionally, the system logs the user data in the journal.

For example, by using the trace function, you could determine which user performed which processing in which period (monitoring function).

When defining, executing and evaluating authorizations, be sure to consider the relevant national and international data protection regulations.