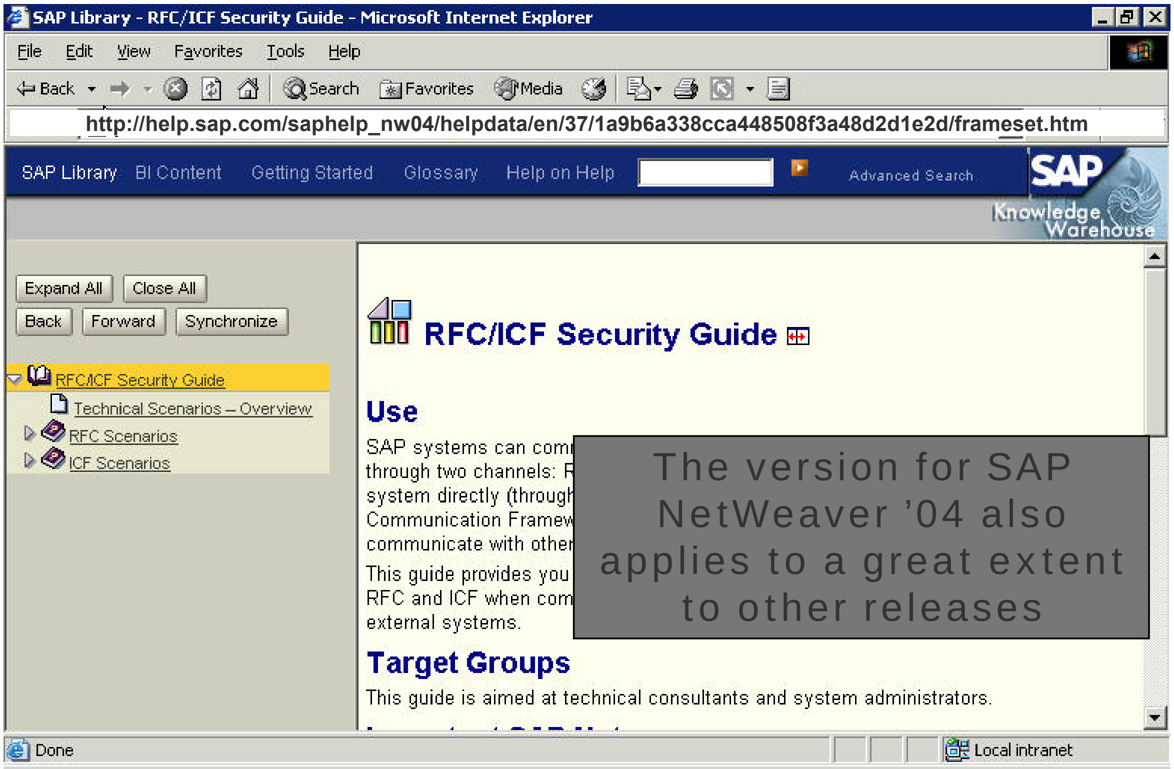
RFC Security

Tips & Tricks for setting up an authorization concept to secure the RFC connections in an SAP system landscape

SAP AG, Product Security

THE BEST-RUN BUSINESSES RUN SAP

RFC/ICF Security Guide (Online Documentation)


SAP Library - RFC/ICF Security Guide - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
http://help.sap.com/saphelp_nw04/helpdata/en/37/1a9b6a338cca448508f3a48d2d1e2d/frameset.htm
SAP Library BI Content Getting Started Glossary Help on Help Advanced Search
SAP Knowledge Warehouse
Expand All Close All
Back Forward Synchronize
RFC/ICF Security Guide
Technical Scenarios – Overview
RFC Scenarios
ICF Scenarios
Done
Local intranet

RFC/ICF Security Guide

Use

SAP systems can comm
through two channels: R
system directly (through
Communication Framew
communicate with other

This guide provides you
RFC and ICF when com
external systems.

Target Groups

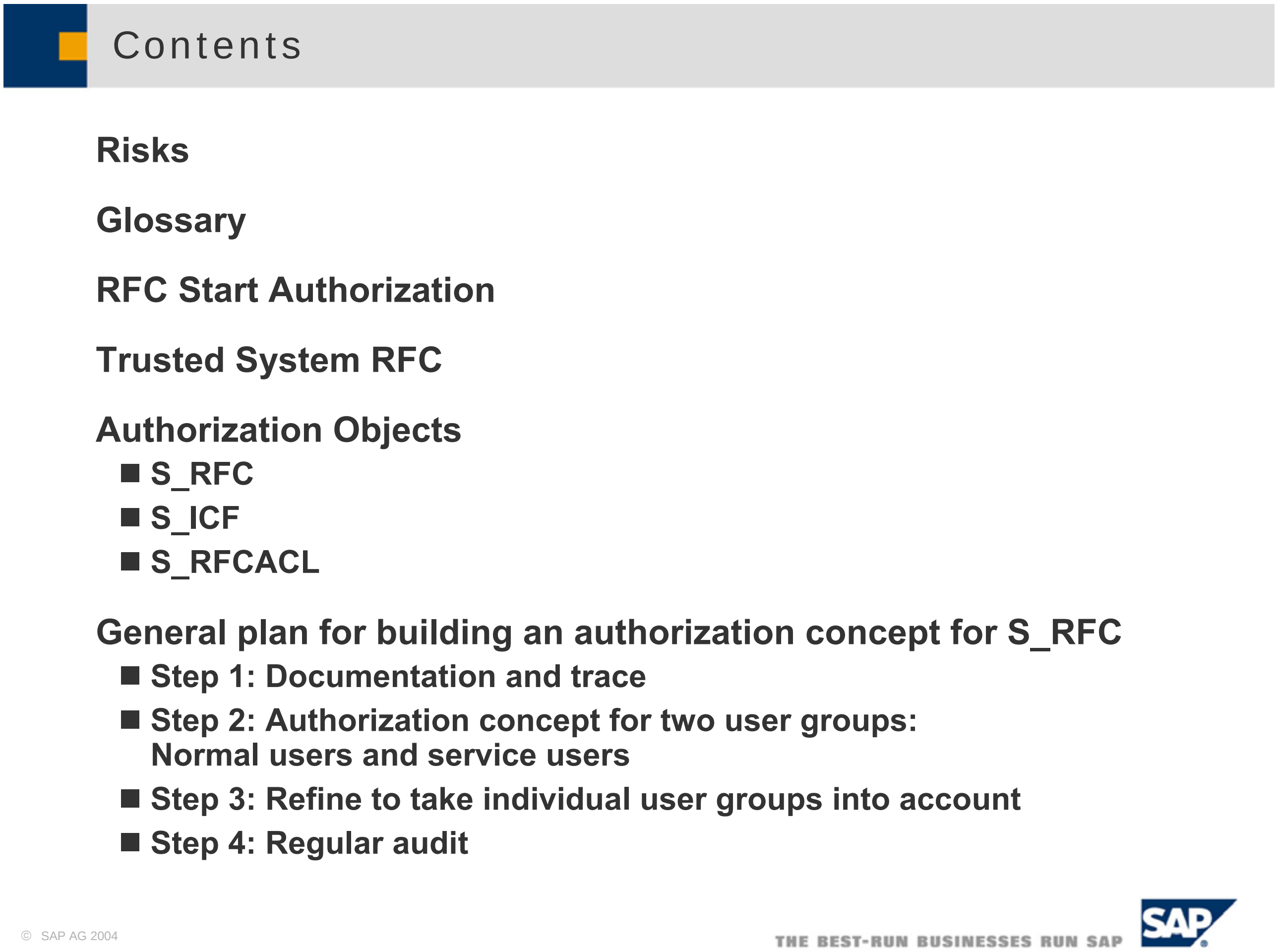
This guide is aimed at technical consultants and system administrators.

The version for SAP NetWeaver '04 also applies to a great extent to other releases

© SAP AG 2004

THE BEST-RUN BUSINESSES RUN SAP

- This presentation gives an overview about setting up secure RFC-connections in an SAP landscape. It also provides you with a guideline of how to build an authorization concept for RFC.
- Additional information is available on http://help.sap.com/saphelp_nw04/helpdata/en/37/1a9b6a338cca448508f3a48d2d1e2d/frameset.htm. Under this link you will find the security guide for RFC/ICF security that includes all related information.



Contents

Risks

Glossary

RFC Start Authorization

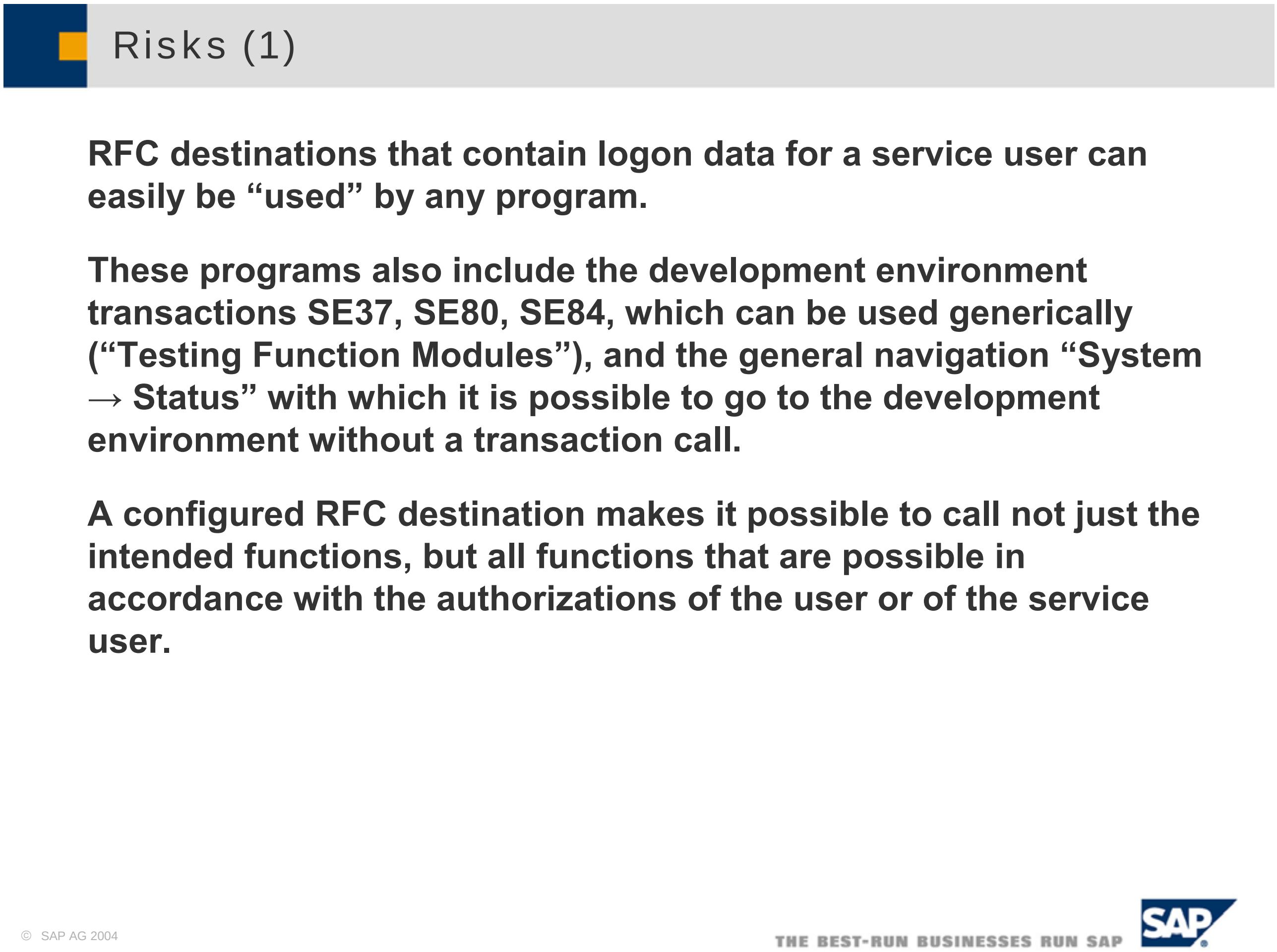
Trusted System RFC

Authorization Objects

- **S_RFC**
- **S_ICF**
- **S_RFCACL**

General plan for building an authorization concept for S_RFC

- **Step 1: Documentation and trace**
- **Step 2: Authorization concept for two user groups: Normal users and service users**
- **Step 3: Refine to take individual user groups into account**
- **Step 4: Regular audit**



Risks (1)

RFC destinations that contain logon data for a service user can easily be “used” by any program.

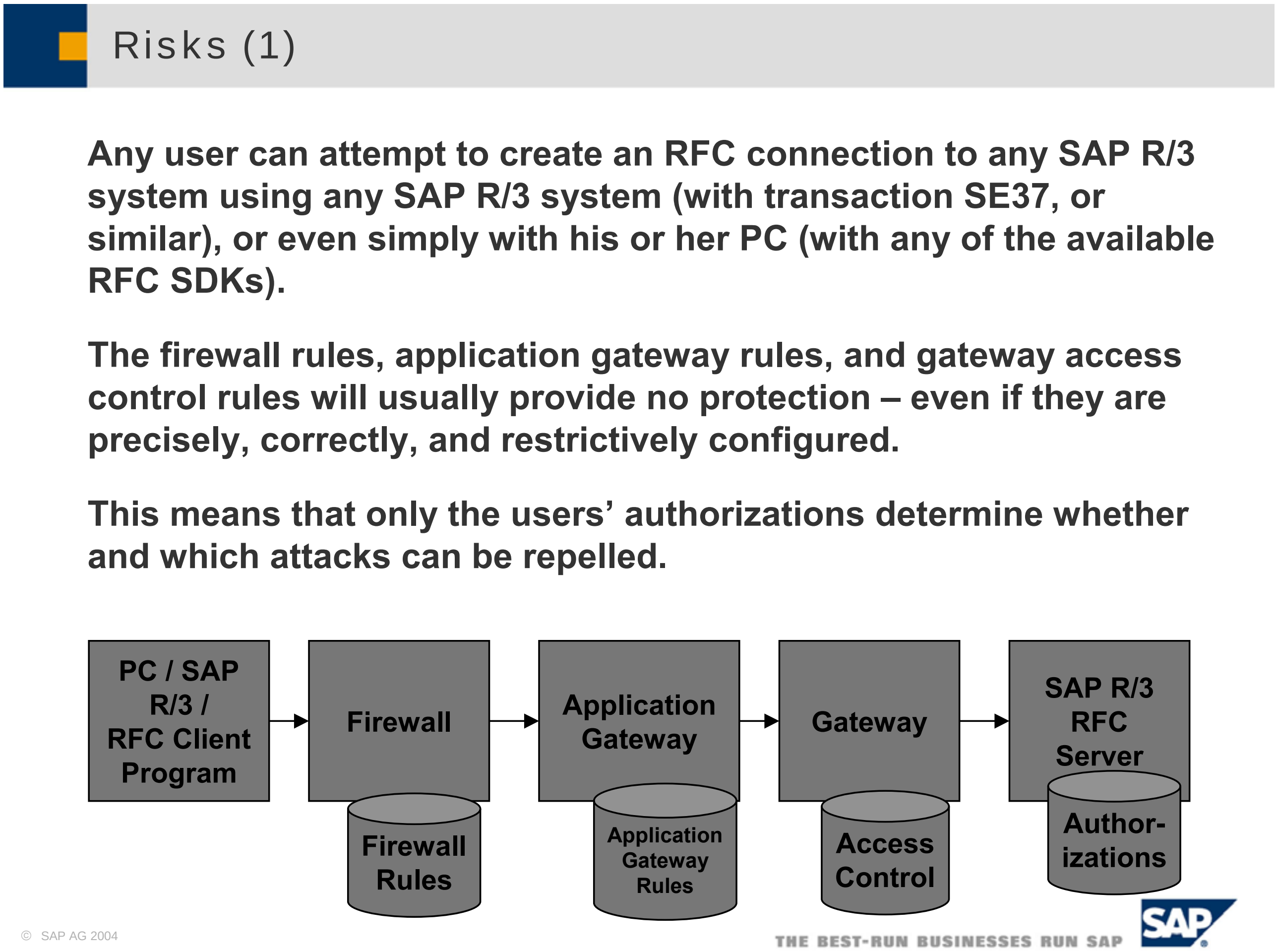
These programs also include the development environment transactions SE37, SE80, SE84, which can be used generically (“Testing Function Modules”), and the general navigation “System → Status” with which it is possible to go to the development environment without a transaction call.

A configured RFC destination makes it possible to call not just the intended functions, but all functions that are possible in accordance with the authorizations of the user or of the service user.

© SAP AG 2004

THE BEST-RUN BUSINESSES RUN SAP

- If you do not want to roll out each user in the whole SAP landscape, you are able to configure a service user for each RFC destination. In that case, the logon data for that service user is stored in the RFC destination. If any other program calls the RFC destination, the stored logon data is used for user authorization. So each caller is identified as the stored service user and his identity in the application or program that is used to establish the RFC connection does not matter. No further authentication is needed in that case.
- When calling a RFC destination, the calling program gets access to all functions that match the authorizations of the service user. That means, that you have to be very careful with the authorizations configured for the RFC destinations. These authorizations should just allow the functions that are really necessary to handle RFC.



Risks (1)

Any user can attempt to create an RFC connection to any SAP R/3 system using any SAP R/3 system (with transaction SE37, or similar), or even simply with his or her PC (with any of the available RFC SDKs).

The firewall rules, application gateway rules, and gateway access control rules will usually provide no protection – even if they are precisely, correctly, and restrictively configured.

This means that only the users' authorizations determine whether and which attacks can be repelled.

© SAP AG 2004

THE BEST-RUN BUSINESSES RUN SAP

- In a SAP landscape, any user may attempt to create a RFC connection to any SAP system if the RFC SDKs are available. As RFC connections normally are widely used in SAP landscapes, any firewall rule, application gateway rule or gateway access control rule would not prevent a user to create a RFC connection. The only access limitation is given by the users authorization. So if any user tries to use RFC connections to attack a SAP System, the users authorizations should be configured well in the whole system. That also includes the authorizations of service users, if they are used to establish RFC connections.

RFC SDK

The RFC SDK can be installed as part of SAP GUI.

Some example programs:

sapinfo(.exe)

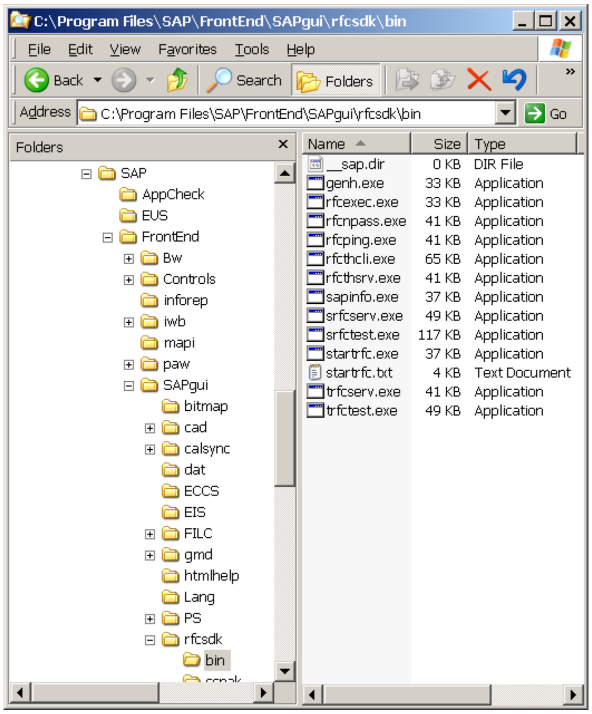
- **RFC client program, provides system information**

startrfc(.exe)

- **RFC client program with which any RFC function module can be started**

rfcexec(.exe)

- **RFC server program that can be started by the SAP system for file and pipe access**



Name	Size	Type
__sap.dir	0 KB	DIR File
genh.exe	33 KB	Application
rfcexec.exe	33 KB	Application
rfcnpass.exe	41 KB	Application
rfcping.exe	41 KB	Application
rfcthcli.exe	65 KB	Application
rfcthsrv.exe	41 KB	Application
sapinfo.exe	37 KB	Application
srfcserv.exe	49 KB	Application
srfctest.exe	117 KB	Application
startrfc.exe	37 KB	Application
startrfc.txt	4 KB	Text Document
trfcserv.exe	41 KB	Application
trfctest.exe	49 KB	Application

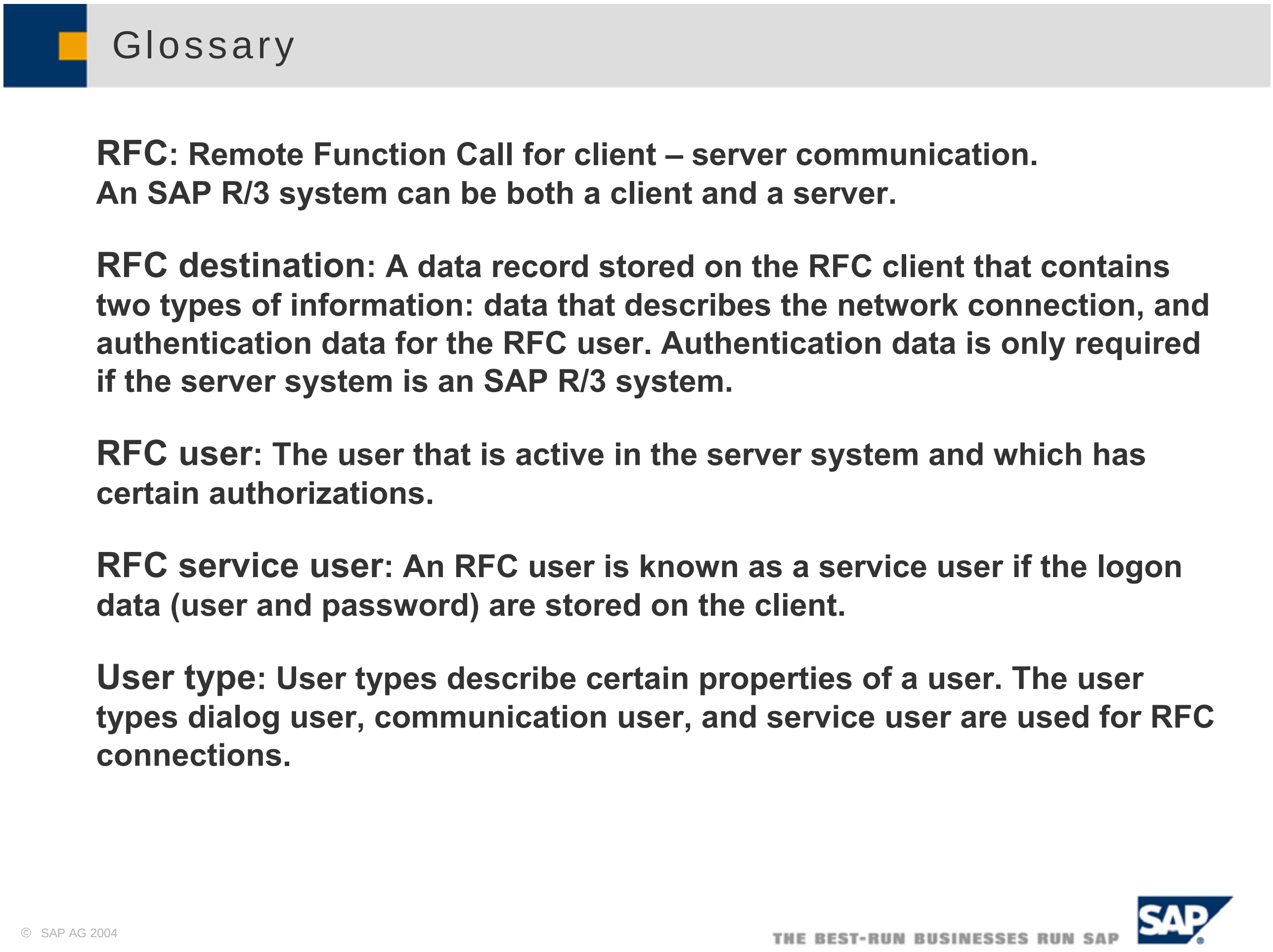
THE BEST-RUN BUSINESSES RUN SAP

- Here are some example programs of the RFC SDK that may be installed as a part of SAP GUI on each PC in a SAP landscape. The following description of the RFC command line interfaces includes the complete information anyone needs to establish a RFC connection:
- RFC command line interface
- Syntax :
- startrfc [connect options] <function options>
- with function options =
- -F <function module
- -E <parameter>=<value>
- -T <table name>,<width>,[r=<file>][,w=<file>]
- where <file> is a path name to read from (r)
- or write to (w) the internal table.
- If <file> is -, stdin or stdout is used.

- RFC connection options:
- -d <destination>   name of the RFC destination.
- Necessary, if you are using a 'sideinfo' file.

- -2   SNA mode on.
- You must set this if you want to connect to R/2.
- All other connection data must be supplied by a
- sideinfo file.

```
  -3      R/3 mode on.
■          You must set this if you want to connect to R/3.
■          Specify the following options:
■     -h <hostname>         hostname of the R/3 target system.
■     -s <system number>    system number of the target system.
■          this determines the TCP/IP service to be used to connect
■          to the R/3 system. The default value is 0 and the default
■          service being used then is sapgw00.
■     -gui               start sapgui
■          to allow dynpro and graphics processing
■          (3.0C or later required on the target system).
■     Using an intermediate SAP gateway, specify:
■          -g <gateway host>
■          -x <gateway service>
■          (must not be used with -gui or -debug option).

■  -balanced             load balancing mode.
■          Another way to connect to R/3, if the R/3 system is 3.0C
■          or later and workload balancing is active on that system.
■          Requests are automatically routed to the application server
■          having the best response times in the moment.
■          Specify the following options:
■     -h <host name>     hostname of R/3's message server.
■     -s <system name>   name of the target system.
■          This determines the TCP/IP service to be used to connect
■          to the R/3 system.
■          The system name is a 3 letter word. If the system name
■          is XXX, the service being used is sapXXX.
■     -g <group name>    name of application server group.
■          The default is PUBLIC.
■     -gui               start sapgui
■          to allow dynpro and graphics processing.

■additional options:
■  -t              turn trace on.
■          all operations are written to the trace file 'dev_rfc'
■  -debug          turn ABAP/4 debugging mode on.
■          this can only be done, if sapgui is installed on the client
■          system and the target system has version 3.0C or later.

■Using the 'saprfc.ini'-file:
■  -D <destination>    name of the RFC destination in saprfc.ini
■          Instead of using the connection and additional options
■          defined above, you can also work with the 'saprfc.ini'-file
■          and all needed options must be defined in this file.
■          Using this feature, this program can run in an SNC
■          environment.

■RFC logon data:
■  -u <userid>      SAP userid.
■  -p <password>    password.
■  -c <client>      client.
■  -l <language>    logon language.

■further options:
■        -i <input file for argv>
■        -o <output file for argv>
■        -?                        this text
```



Glossary

RFC: Remote Function Call for client – server communication.
An SAP R/3 system can be both a client and a server.

RFC destination: A data record stored on the RFC client that contains two types of information: data that describes the network connection, and authentication data for the RFC user. Authentication data is only required if the server system is an SAP R/3 system.

RFC user: The user that is active in the server system and which has certain authorizations.

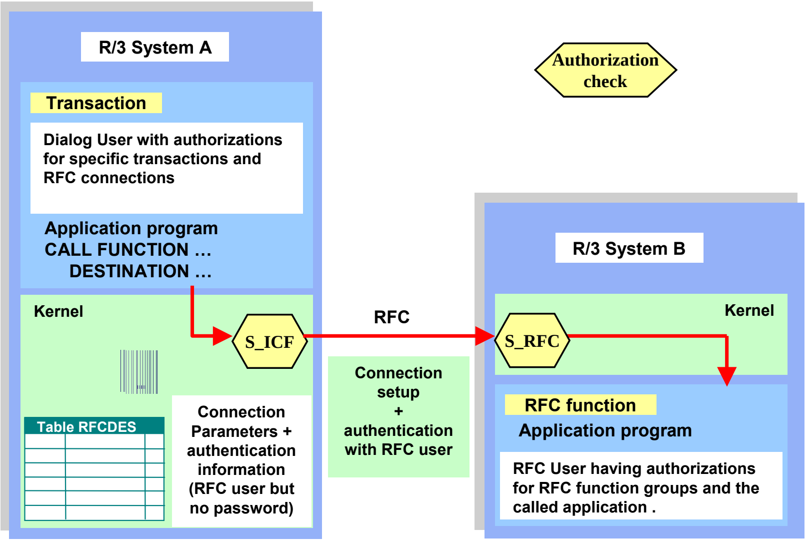
RFC service user: An RFC user is known as a service user if the logon data (user and password) are stored on the client.

User type: User types describe certain properties of a user. The user types dialog user, communication user, and service user are used for RFC connections.

RFC Function Module Start Authorization

The RFC user’s authorizations for S_RFC in the server system define which function groups can start RFC functions.

The user’s authorizations for S_ICF in the client system define which RFC destinations can be used.



R/3 System A
Transaction
Dialog User with authorizations for specific transactions and RFC connections
Application program
CALL FUNCTION …
DESTINATION …
Kernel
S_ICF
Table RFCDES
Connection Parameters + authentication information (RFC user but no password)
RFC
Connection setup + authentication with RFC user
Authorization check
R/3 System B
Kernel
S_RFC
RFC function
Application program
RFC User having authorizations for RFC function groups and the called application .

■If any SAP System wants to establish a RFC connection to another SAP System, a check if the calling system is allowed to use the RFC destination is performed. This is done on the calling system using the authorization object S_ICF. This object could be found in the authorization profile of the user that is logged into the calling system. The user is able to use only those RFC destinations that are configured in the S_ICF object.

■On the other hand, the RFC destination uses the authorization object S_RFC to determine, which actions could be performed by any caller in a RFC connection. The authorization object S_RFC has the following three fields:

■RFC_NAME	name of the function group
ACTVT	only possible value is 16 (execute)
RFC_TYPE	only possible value is FUGR (function group)

■As this object is not linked to the profile generator, administrators have to create authorizations for this object manually.

■To configure this authorization object well, administrators need to be aware to the fact, that certain function groups are needed for a certain scenario. They need exact documentation of the function modules needed in these scenarios.

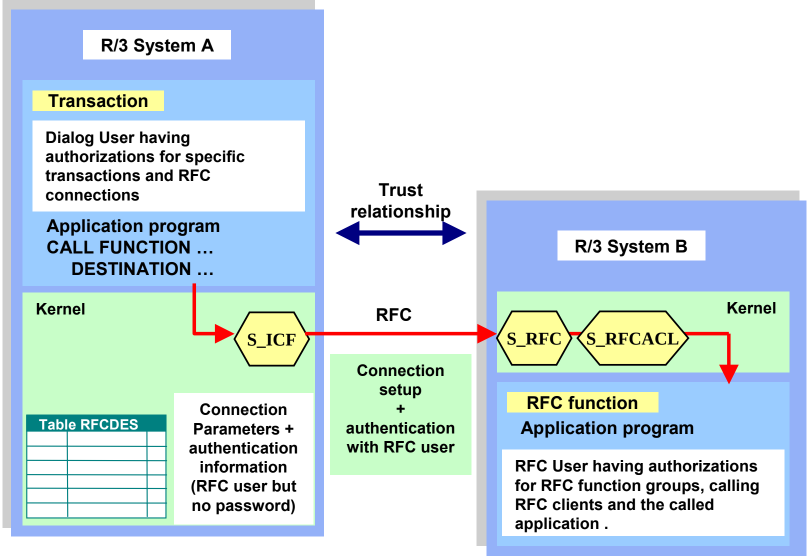
■Application developers need to provide a standard role for the scenario: They should trace, which authorizations are needed exactly, to perform the function, and put these authorizations into the standard role. As note 0543164 states, authorizations are now also traced for RFC function modules, if the profile parameter auth/authorization_trace is set to y.

■As you my see in the description above, the authorization object S_RFC just controls which actions may be performed. It does not check, if the calling system is allowed to use the RFC destination. If the authentication using username and password of the RFC user does not fail. The RFC connection is established.

Trusted System RFC

You can link different SAP R/3 systems for the RFC context. To do this, you designate a calling system with the target system as a “trusted system”. Trusted systems can log on to a trusting system without a password.

An additional authorization check is performed in the server system for S_RFCACL.


R/3 System A
Transaction
Dialog User having authorizations for specific transactions and RFC connections
Application program
CALL FUNCTION ...
DESTINATION ...
Kernel
S_ICF
Table RFCDES
Connection Parameters + authentication information (RFC user but no password)
Trust relationship
RFC
Connection setup + authentication with RFC user
R/3 System B
Kernel
S_RFC
S_RFCACL
RFC function
Application program
RFC User having authorizations for RFC function groups, calling RFC clients and the called application .

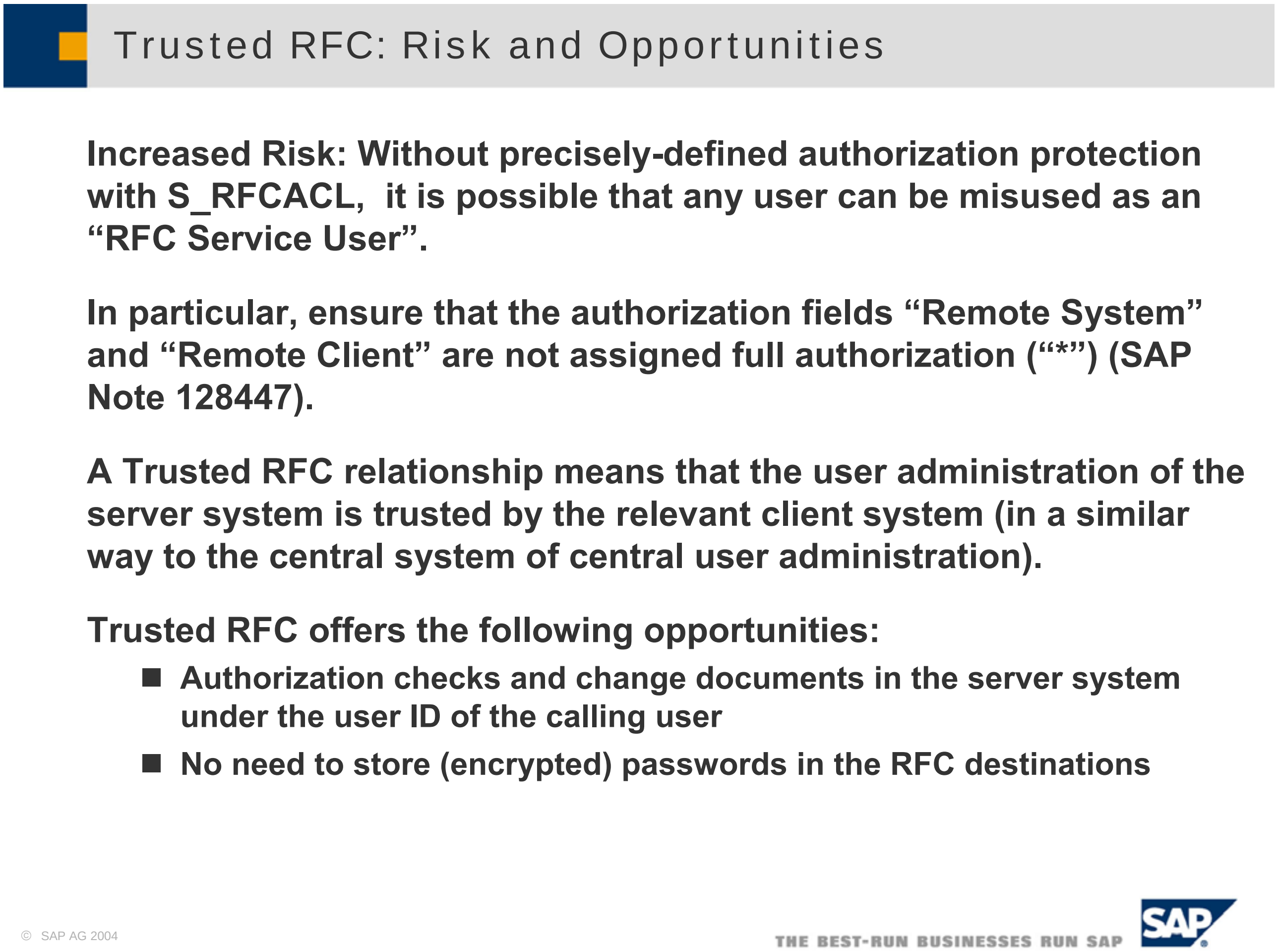
■To mitigate the risk of unauthorized using of RFC destinations, SAP allows to establish a trust relationship between the calling system and the called system. In that scenario the RFC destination, which is called trusting system, does only accept connections form dedicated calling systems, the so called trusted systems. The trust relationship is build using the authorization object S_RFCACL. To log on a trusting system, no password is needed, because the trusting system trusts the authentication performed by the trusted system.

■The authorization object S_RFCACL, that is only used in trust relationships, contains 7 fields:

■RFC_SYSID	ID of the calling system
RFC_CLIENT	Client of the calling system
RFC_USER	ID of the calling user
RFC_EQUSER	Indicator of whether the RFC user may be called by a user with the same ID
RFC_TCODE	Calling transaction code
RFC_INFO	Additional information from the calling system (currently inactive)
ACTVT	Can currently have the value 16 (execute)

■Using the fields RFC_USER and RFC_EQUSER, you are able to map the user and authorizations in the calling system to any user of the called system. That makes it very easy to control the users authorizations in the trusting system and it is also possible to get information about the user that performed an action over RFC in the trusted system from the log files. Therefore you have to implement a one by one mapping of the users in the trusted and the trusting system.

■As this authorization object is implemented in the profile generator, the administrator must create authorizations for his object manually.



Trusted RFC: Risk and Opportunities

Increased Risk: Without precisely-defined authorization protection with S_RFCACL, it is possible that any user can be misused as an “RFC Service User”.

In particular, ensure that the authorization fields “Remote System” and “Remote Client” are not assigned full authorization (“*”) (SAP Note 128447).

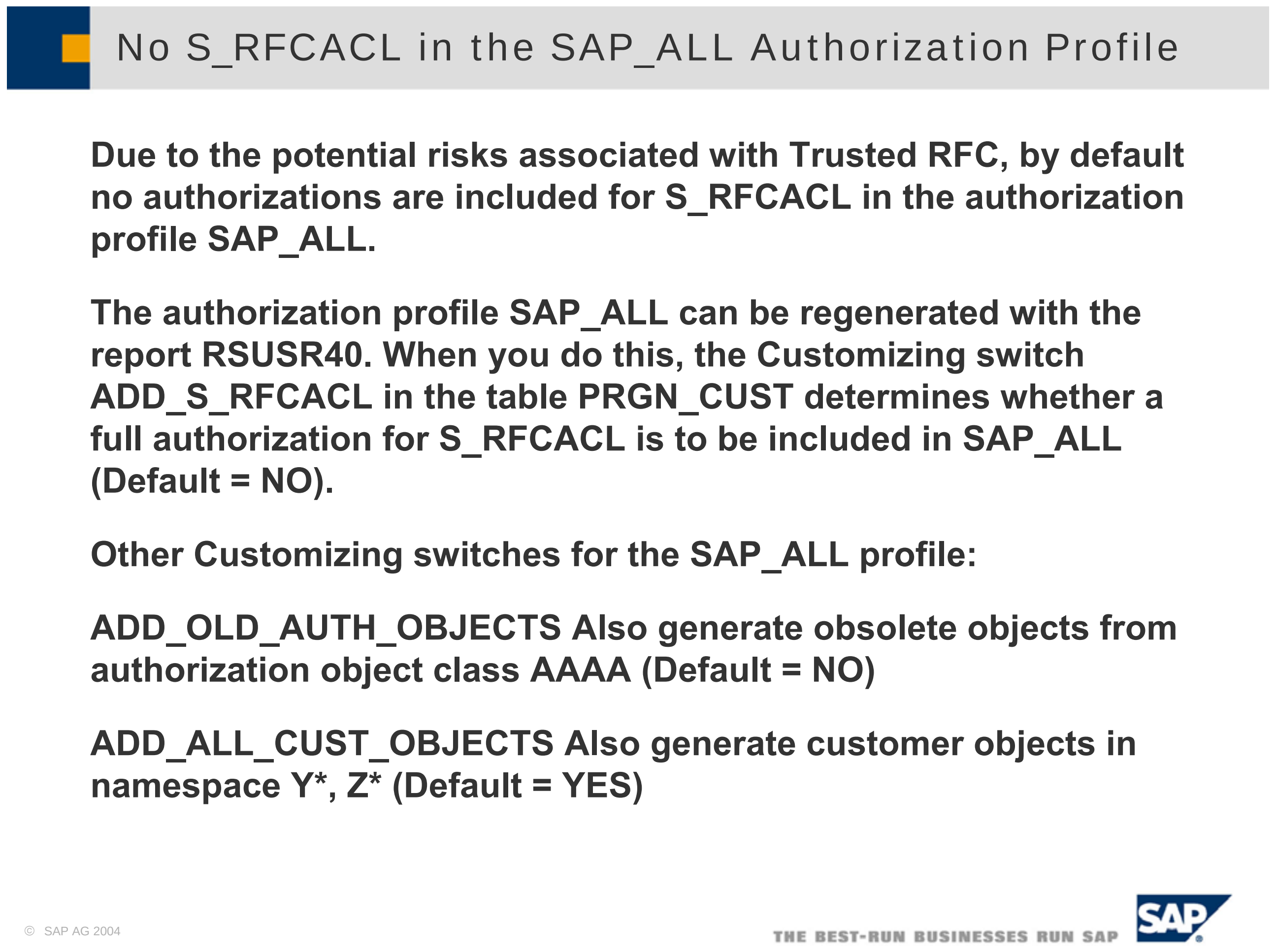
A Trusted RFC relationship means that the user administration of the server system is trusted by the relevant client system (in a similar way to the central system of central user administration).

Trusted RFC offers the following opportunities:

- Authorization checks and change documents in the server system under the user ID of the calling user
- No need to store (encrypted) passwords in the RFC destinations

THE BEST-RUN BUSINESSES RUN SAP

- Using trust relationships in RFC connections gives you a good security opportunity, but also contains risks. In a trusted RFC relationship, the RFC destinations trusts the user management and administration of the calling system. So, with a trustworthy user managements, you may earn a higher level of security, because there is no need to store passwords in the RFC destinations any more. It is also possible to perform authorization checks and produce change documents under the user ID of the calling user in the RFC destination. That allows you to control and audit the RFC connections with a scope on the users of the system. On the other hand, these security advantages turn to security risks, if the S_RFCACL object is not configured well or the users are managed and administered in a careless way. It might be possible that any user could be misused as an „RFC Service User“.



No S_RFCACL in the SAP_ALL Authorization Profile

Due to the potential risks associated with Trusted RFC, by default no authorizations are included for S_RFCACL in the authorization profile SAP_ALL.

The authorization profile SAP_ALL can be regenerated with the report RSUSR40. When you do this, the Customizing switch ADD_S_RFCACL in the table PRGN_CUST determines whether a full authorization for S_RFCACL is to be included in SAP_ALL (Default = NO).

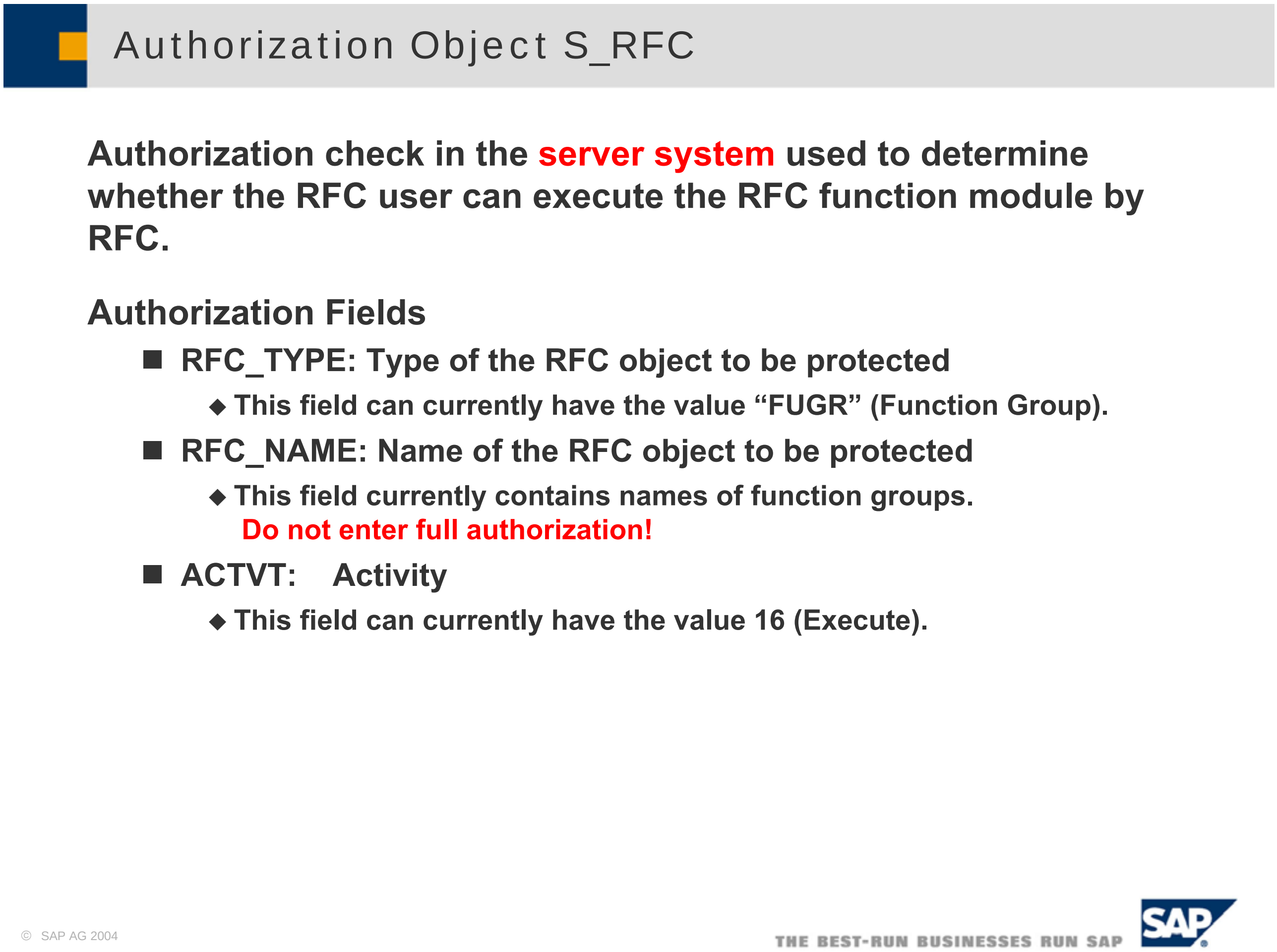
Other Customizing switches for the SAP_ALL profile:

ADD_OLD_AUTH_OBJECTS Also generate obsolete objects from authorization object class AAAA (Default = NO)

ADD_ALL_CUST_OBJECTS Also generate customer objects in namespace Y*, Z* (Default = YES)

THE BEST-RUN BUSINESSES RUN SAP

- As wrong configuration of S_RFCACL may cause security leaks, this authorization object is not included in the SAP_ALL profile. To include it, you can regenerate profile SAP_ALL using report RSUSR40. The customizing switch ADD_S_RFCACL in table PRGN_CUST determines whether full authorizations should be included in the SAP_ALL profile. As the default value is NO, you have to set value YES to include full authorizations for S_RFCACL. Table PRGN_CUST contains some other customizing switches for the SAP_ALL profile. If you set ADD_OLD_AUTH_OBJECTS, obsolete objects from object class AAAA will be generated in SAP_ALL. You might need this, if you still run older components that check these objects. The default value of ADD_OLD_AUTH_OBJECTS is NO. If you use customized objects in the customer namespace Y* and Z* and you want to include those in the SAP_ALL profile, you have to ensure that the value of ADD_ALL_CUST_OBJECTS is set to YES, which is the default value.



Authorization Object S_RFC

Authorization check in the server system used to determine whether the RFC user can execute the RFC function module by RFC.

Authorization Fields

- **RFC_TYPE: Type of the RFC object to be protected**
  - ◆ This field can currently have the value “FUGR” (Function Group).
- **RFC_NAME: Name of the RFC object to be protected**
  - ◆ This field currently contains names of function groups.
    Do not enter full authorization!
- **ACTVT: Activity**
  - ◆ This field can currently have the value 16 (Execute).

THE BEST-RUN BUSINESSES RUN SAP

- Authorization check in the server system is performed with authorization object S_RFC. This object checks, if the it is allowed to execute the function that is called over RFC. To determine whether the function could be called, three authorization fields are checked. The field ACTVT contains the activities that are allowed on the called function. The value of that field should be set to 16 for execute. The field RFC_TYPE specifies the RFC object that should be protected. The value of that field should be set to „FUGR“, which means Function Group. The dedicated function groups itself are specified in field RFC_NAME that should contain the names of the function group. Make sure not to enter full authorizations in that field! If you do so, a caller is allowed to access each function of the server system.

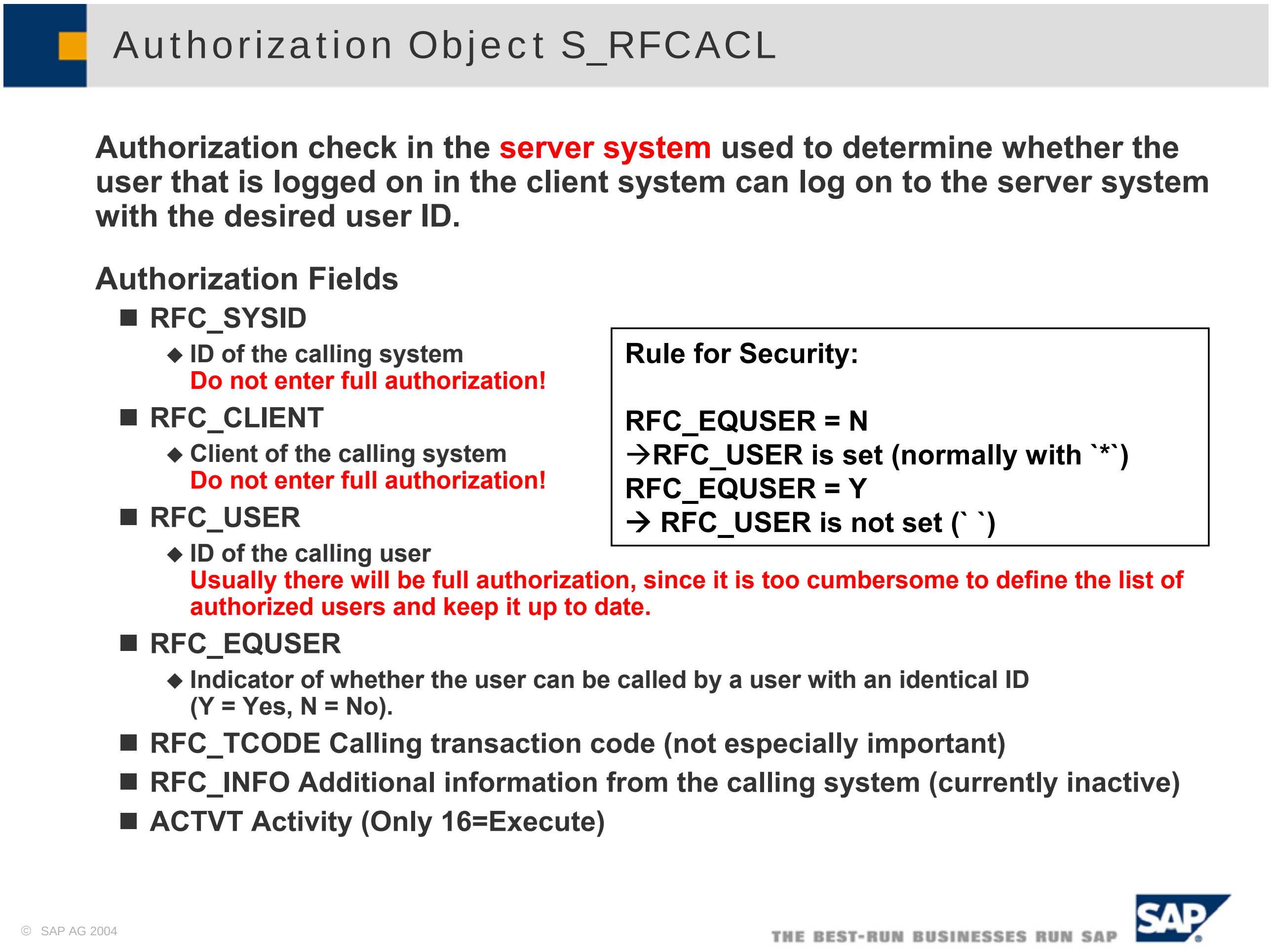
Authorization Object S_ICF

Authorization check in the client system used to determine whether the logged-on user is permitted to use the RFC destination to call function modules by RFC.

Authorization Fields

- **ICF_FIELD: Type of the object to be protected.**
  - ◆ This field can have the following values:
  - ◆ SERVICE: For the use of ICF services
  - ◆ DEST: For the use of RFC destinations (as of SAP Web AS 6.20)
- **ICF_VALUE: Value of the ICF object to be protected.**
  - ◆ This field contains the value of the corresponding object. The values that are to be protected are maintained in transaction SICF for ICF services and in transaction SM59 for RFC destinations.

- On the client system, a authorization check is performed to determine whether the logged-on user is allowed to use the requested RFC destination. The authorization object S_ICF is used to perform that authorization check. It includes two authorization fields. The authorization field ICF_FIELD specifies the type of the object that should be protected. To protect RFC destinations, it should contain the value DEST, for the usage of ICF services, it should contain the value SERVICE. The field ICF_VALUE contains the corresponding objects. The values that should be protected are maintained using transaction SM59 for RFC destinations and SICF for IFC services.



Authorization Object S_RFCACL

Authorization check in the server system used to determine whether the user that is logged on in the client system can log on to the server system with the desired user ID.

Authorization Fields

- RFC_SYSID
  - ID of the calling system
    Do not enter full authorization!
- RFC_CLIENT
  - Client of the calling system
    Do not enter full authorization!
- RFC_USER
  - ID of the calling user
    Usually there will be full authorization, since it is too cumbersome to define the list of authorized users and keep it up to date.
- RFC_EQUSER
  - Indicator of whether the user can be called by a user with an identical ID (Y = Yes, N = No).
- RFC_TCODE Calling transaction code (not especially important)
- RFC_INFO Additional information from the calling system (currently inactive)
- ACTVT Activity (Only 16=Execute)

Rule for Security:

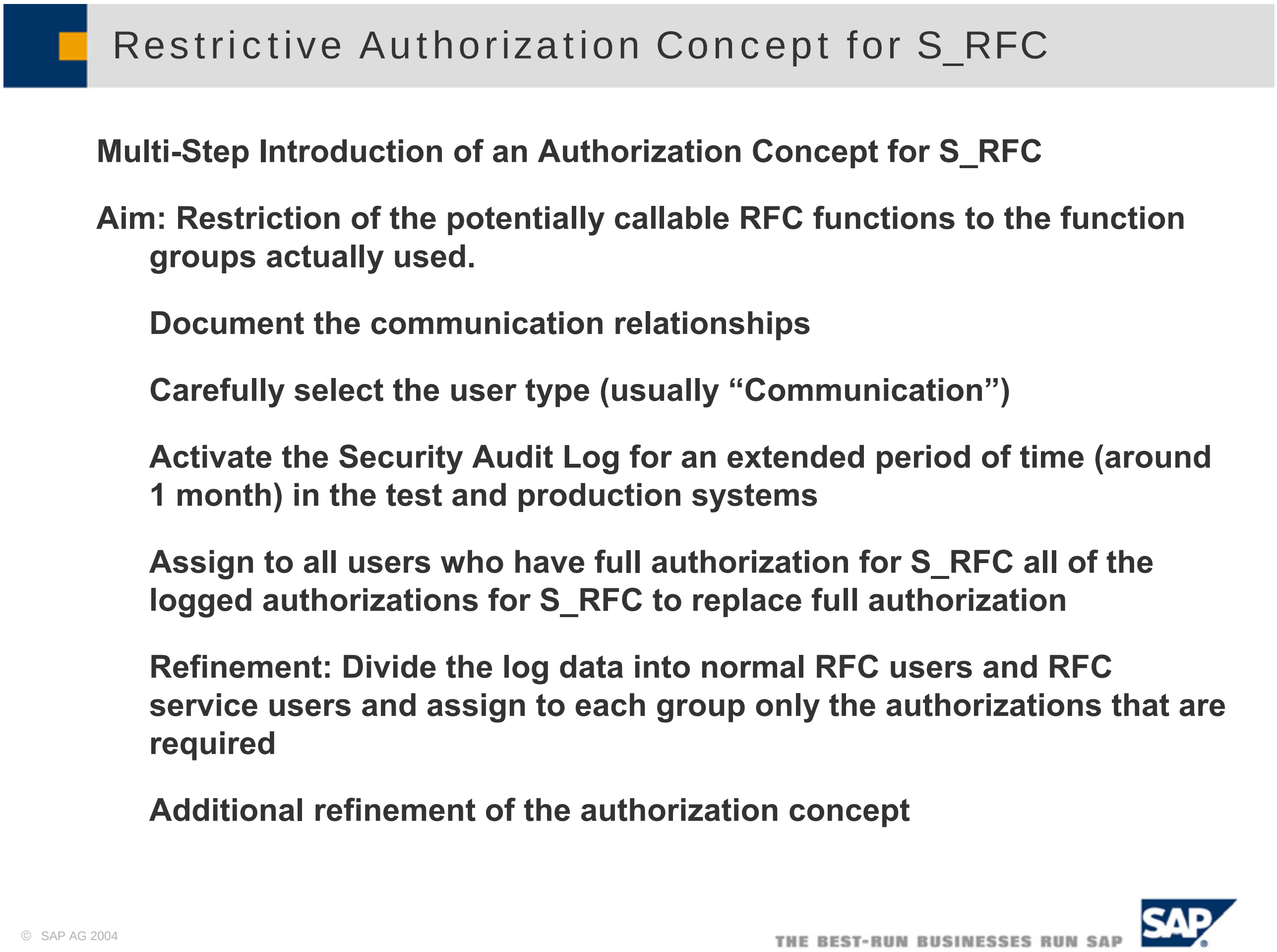
RFC_EQUSER = N
→RFC_USER is set (normally with `*`)
RFC_EQUSER = Y
→ RFC_USER is not set (` `)

THE BEST-RUN BUSINESSES RUN SAP

- To restrict access to the server system for dedicated users, the authorization object S_RFCCACL is used in the server system. This authorization object specifies if the user logged in the client system is allowed to establish a RFC connection to the server system. Remember, that the check on authorization object S_ICF is performed on the client site. The authorization check on object S_RFCACL is performed on server side. Both checks are necessary. The check on client side using object S_ICF prevents network traffic in normal processing. The check on server site is necessary for security reasons, because the server is not able to check if the calling system has performed authorization check on field S_ICF. Therefore the server system itself has to check the users authorization. To do so, the user username is transferred in the RFC request. The server system then is able to perform an own authorization check regarding to the logged on user.

- As you can see now, it is not possible that an attacker uses any program that passes check on S_ICF to access functions on the server system over a RFC connection as it was possible in an un-trusted scenario that in which check on S_RFCACL is not perform. Nevertheless you have to keep in mind, that each user that is allowed to establish RFC connections must exist in both, the client and the server system or at least has a user assigned in the server system.

- You also have to configure the object S_RFCACL well to earn the security described above. Therefore you have to be careful by setting the values of the authorization fields. The field RFC_SYSID gives you control on the systems that are allowed to call this RFC destination. Therefore it should contain the corresponding IDs of the client systems. If you want also control the client on the calling system, you can do this by setting the value of field RFC_CLIENT. To control, what user is allowed to access the RFC destination, list the users in field RFC_USER. Make sure not to enter full authorization. If you do so, every user is able to access the RFC destination. To ensure, that a the users on client and server system are the same, set RFC_EQUSER to YES. If you have to allow to change user while accessing the RFC destination, e. g. if you do not want do roll out users on client and server systems, set RFC_EQUSER to NO. It is recommended to use same user on client and server system. Only in that case it is possible to log which user did what on the RFC destination. The last three fields RFC_TCODE, RFC_INFO and ACTVT are not important for a secure RFC connection. RFC_INFO is currently not in use and ACTVT is set to 16 by default.



Restrictive Authorization Concept for S_RFC

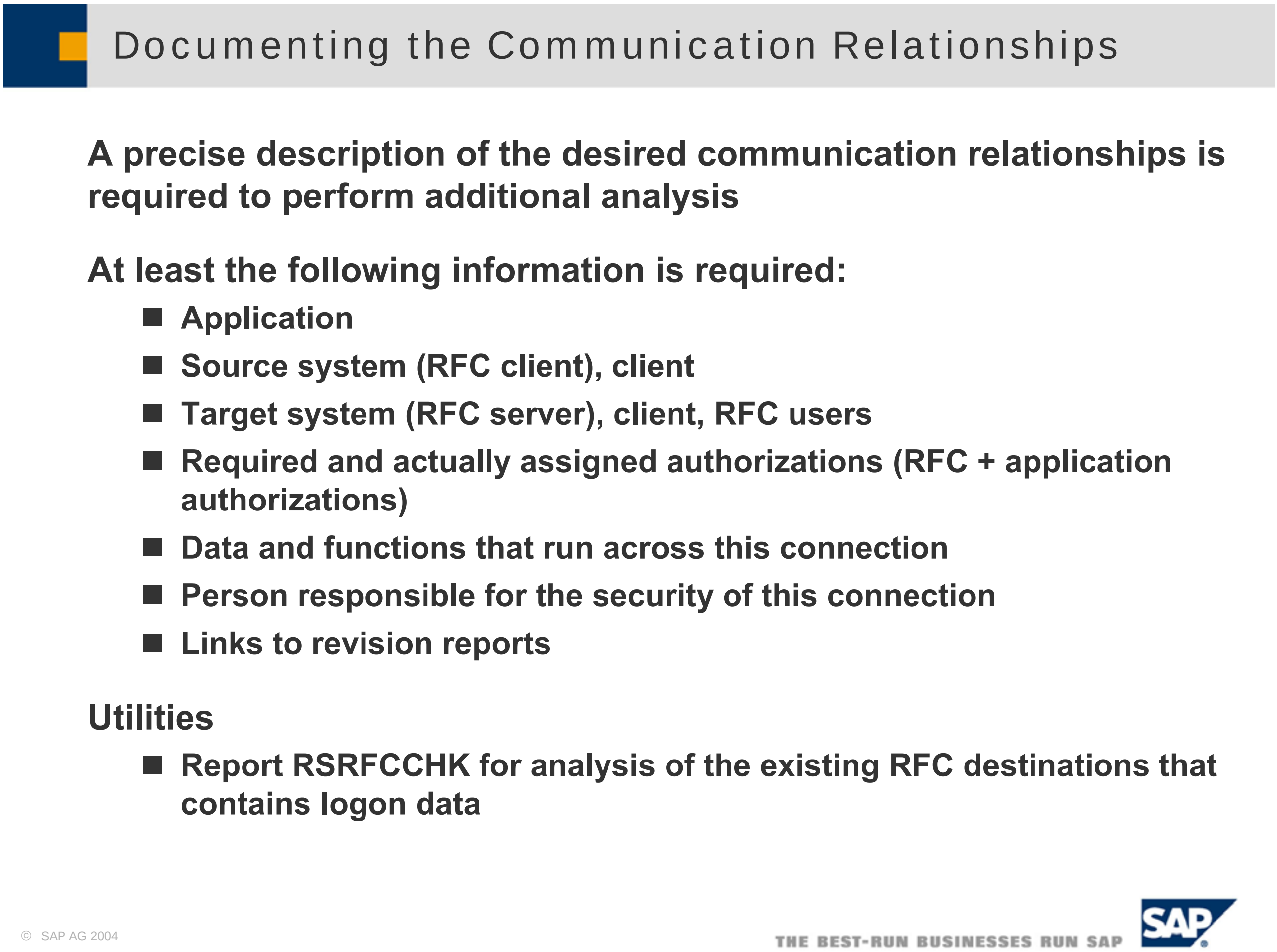
Multi-Step Introduction of an Authorization Concept for S_RFC

Aim: Restriction of the potentially callable RFC functions to the function groups actually used.

- **Document the communication relationships**
- **Carefully select the user type (usually “Communication”)**
- **Activate the Security Audit Log for an extended period of time (around 1 month) in the test and production systems**
- **Assign to all users who have full authorization for S_RFC all of the logged authorizations for S_RFC to replace full authorization**
- **Refinement: Divide the log data into normal RFC users and RFC service users and assign to each group only the authorizations that are required**
- **Additional refinement of the authorization concept**

THE BEST-RUN BUSINESSES RUN SAP

- Now, after we saw, how important it is to restrict the RFC functions that could be called, the question is, how to do this. At first, you should clearly understand, how your SAP system landscape looks like and which RFC destinations exist in your system. Therefore you have to document the communication relationship. The second point is, that you have to make sure, that the user for RFC users is selected carefully. Normally the user type should be „Communication“.
- In a existing system, you will normally find that the RFC users have full authorizations. As we saw before, this is not very secure. The user should be assigned only those authorizations he really needs. That is not easy to do, because you do not really know which authorizations that are. To figure that out, a good way is to activate the security audit log for a extended period of time. The time to choose depends on the customers business. On one hand, the time period should be long enough to ensure that each transaction is called at least one time during normal business. On the other hand the time period should not be too long. A time period of about three month might be a good choice. After that time period, you can examine the log file and filter the authorizations that are logged. These authorizations should be assigned to the authorization object S_RFC. Now the system should run as before.
- After that you can perform a first refinement step. Divide the logged data into normal RFC users and RFC service users and assign to each group the required authorization. In a additional refinement step you can divide RFC users and service users in several groups depending on function groups that are used.
- The steps described above, starting with the second step, must be performed for each RFC destination.



Documenting the Communication Relationships

A precise description of the desired communication relationships is required to perform additional analysis

At least the following information is required:

- **Application**
- **Source system (RFC client), client**
- **Target system (RFC server), client, RFC users**
- **Required and actually assigned authorizations (RFC + application authorizations)**
- **Data and functions that run across this connection**
- **Person responsible for the security of this connection**
- **Links to revision reports**

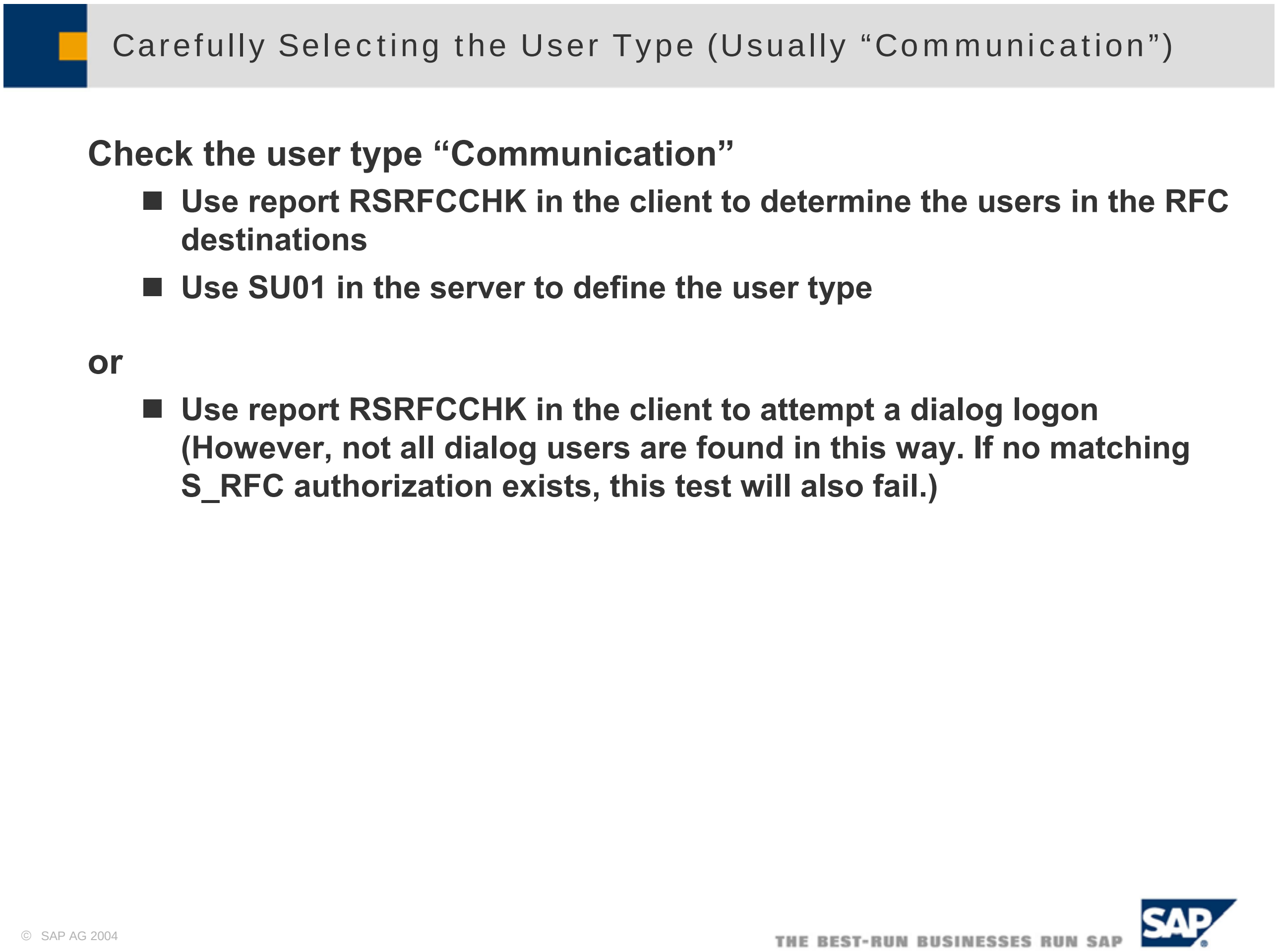
Utilities

- **Report RSRFCCHK for analysis of the existing RFC destinations that contains logon data**

- As said before, the communication relationships have to be documented. This documentation should be a precise description of the desired communication relationships. This is needed to perform additional analysis. At least the following information is required:

- Application
- Source System, that is the RFC client
- Target System, that is the RFC Server
- The required and the actually assign authorizations for RFC and the application
- The data and the functions that run across this connection
- The responsible person for the security of this connection
- Links to any revision reports if exist

- The report RSRFCCHK informs you about existing RFC destinations that contain logon data.



Carefully Selecting the User Type (Usually “Communication”)

Check the user type “Communication”

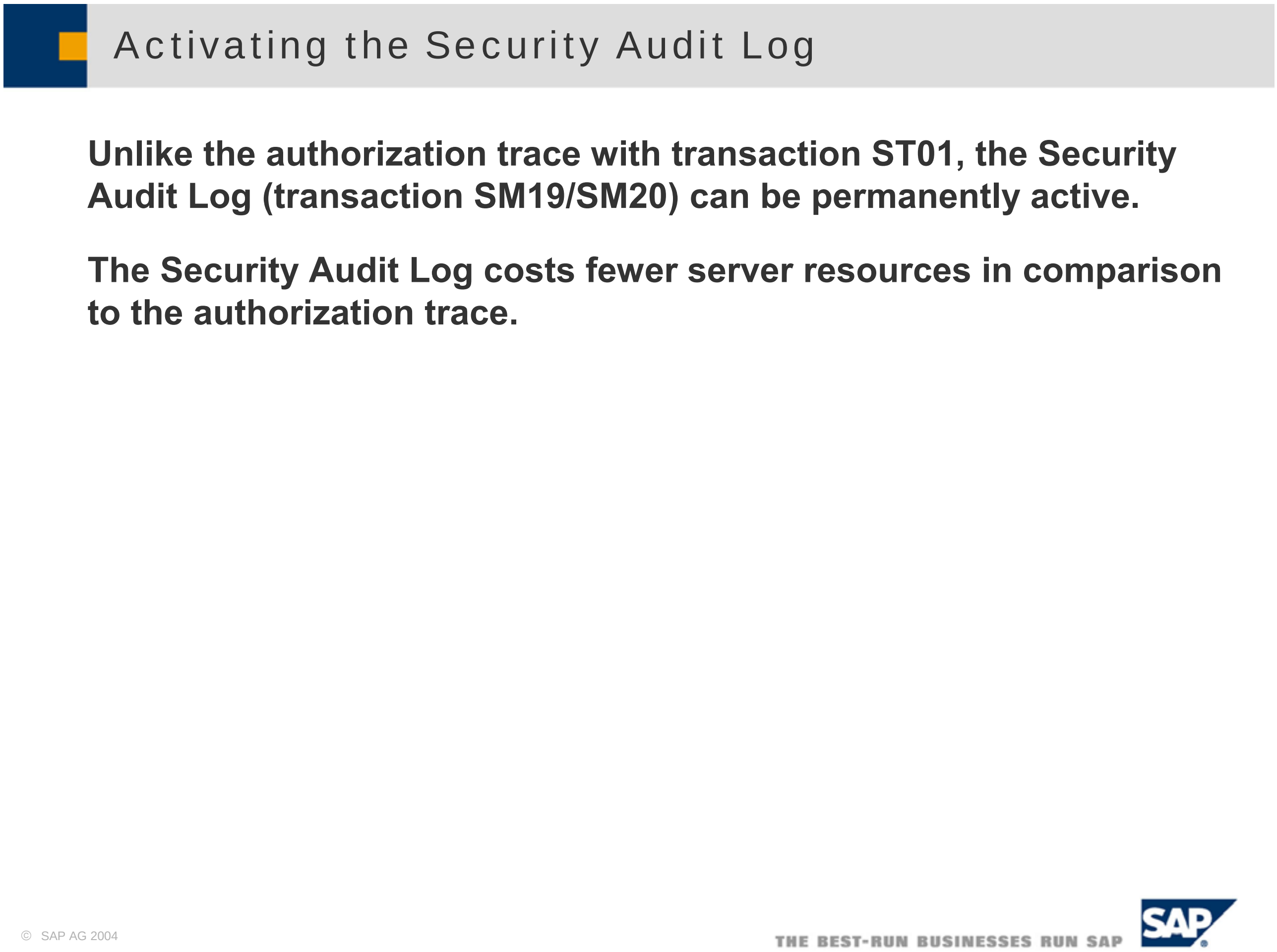
- **Use report RSRFCCHK in the client to determine the users in the RFC destinations**
- **Use SU01 in the server to define the user type**

or

- **Use report RSRFCCHK in the client to attempt a dialog logon (However, not all dialog users are found in this way. If no matching S_RFC authorization exists, this test will also fail.)**

THE BEST-RUN BUSINESSES RUN SAP

- To check the user type and change it to communication if necessary, you can also use the report RSRFCCHK in the client to determine the users in the RFC destinations. Then you can check and change the user type using transaction SU01 on the server. Another possible way is to use report RSRFCCHK in the client to try a dialog logon. But you will not find all dialog users. If no matching S_RFC authorization exists, this test will also fail.



Activating the Security Audit Log

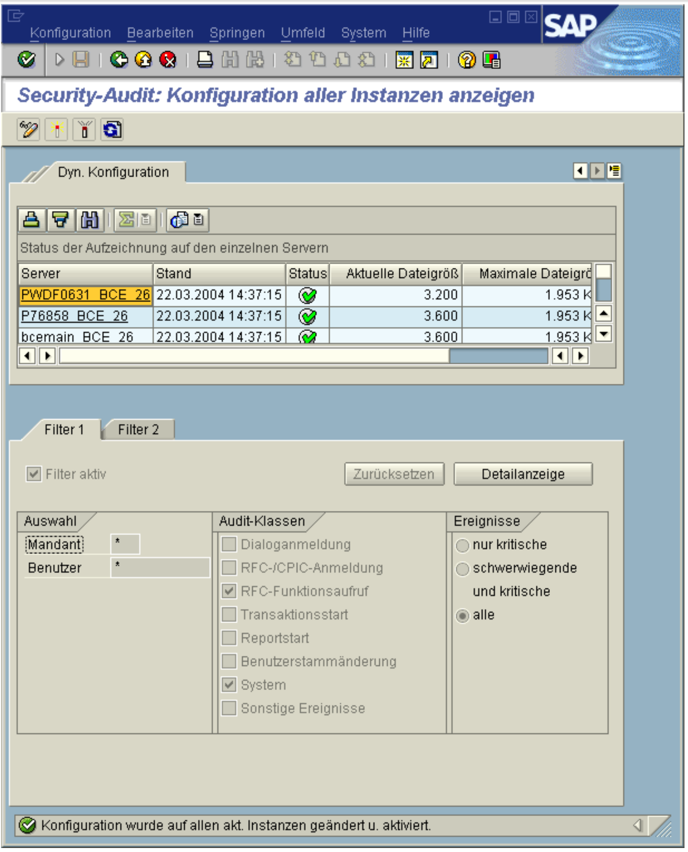
Unlike the authorization trace with transaction ST01, the Security Audit Log (transaction SM19/SM20) can be permanently active.

The Security Audit Log costs fewer server resources in comparison to the authorization trace.

THE BEST-RUN BUSINESSES RUN SAP

- The Security audit Log is activated with transactions SM19 or SM20. Instead of using the security audit log, you might also use the authorization trace that is enabled with transaction ST01. In that case you should remember that the authorization trace costs much more server resources than the security audit log and therefore should not be active permanent.

Security Audit Log Configuration (SM19)



Security-Audit: Konfiguration aller Instanzen anzeigen

Dyn. Konfiguration

Status der Aufzeichnung auf den einzelnen Servern

Server	Stand	Status	Aktuelle Dateigröß	Maximale Dateigrö
PWDF0631_BCE_26	22.03.2004 14:37:15	✓	3.200	1.953 K
P76858_BCE_26	22.03.2004 14:37:15	✓	3.600	1.953 K
bcemain_BCE_26	22.03.2004 14:37:15	✓	3.600	1.953 K

Filter 1 | Filter 2

☑ Filter aktiv

Zurücksetzen | Detailanzeige

Auswahl		Audit-Klassen	Ereignisse
Mandant	*	□ Dialoganmeldung	○ nur kritische
Benutzer	*	□ RFC-/CPIC-Anmeldung	○ schwerwiegende und kritische
		☑ RFC-Funktionsaufruf	● alle
		□ Transaktionsstart	
		□ Reportstart	
		□ Benutzerstammänderung	
		☑ System	
		□ Sonstige Ereignisse	

✓ Konfiguration wurde auf allen akt. Instanzen geändert u. aktiviert.

A filter is activated for:

•All clients

•All users

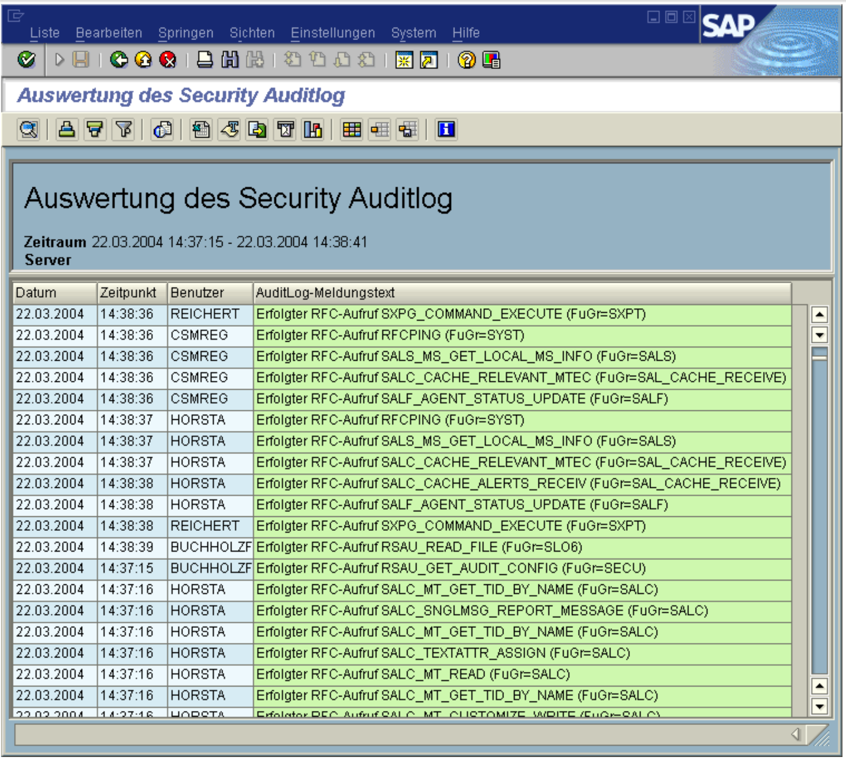
•The audit class RFC function calls

•All events

THE BEST-RUN BUSINESSES RUN SAP

- If you enable security audit log, you should set some filters to get appropriate results. Set filter for all clients, so connections from all clients are logged. The same for the filter all users to log access form all users. To log only RFC calls set the filter for audit class RFC function calls. The event filter should be set to all. With this settings you will get a security audit log only for all RFC calls from each client and each user.

Security Audit Log Evaluation SM20 or SM20N



Auswertung des Security Auditlog

Zeitraum 22.03.2004 14:37:15 - 22.03.2004 14:38:41
Server

Datum	Zeitpunkt	Benutzer	AuditLog-Meldungstext
22.03.2004	14:38:36	REICHERT	Erfolgter RFC-Aufruf SXPG_COMMAND_EXECUTE (FuGr=SXPT)
22.03.2004	14:38:36	CSMREG	Erfolgter RFC-Aufruf RFCPING (FuGr=SYST)
22.03.2004	14:38:36	CSMREG	Erfolgter RFC-Aufruf SALS_MS_GET_LOCAL_MS_INFO (FuGr=SALS)
22.03.2004	14:38:36	CSMREG	Erfolgter RFC-Aufruf SALC_CACHE_RELEVANT_MTEC (FuGr=SAL_CACHE_RECEIVE)
22.03.2004	14:38:36	CSMREG	Erfolgter RFC-Aufruf SALF_AGENT_STATUS_UPDATE (FuGr=SALF)
22.03.2004	14:38:37	HORSTA	Erfolgter RFC-Aufruf RFCPING (FuGr=SYST)
22.03.2004	14:38:37	HORSTA	Erfolgter RFC-Aufruf SALS_MS_GET_LOCAL_MS_INFO (FuGr=SALS)
22.03.2004	14:38:37	HORSTA	Erfolgter RFC-Aufruf SALC_CACHE_RELEVANT_MTEC (FuGr=SAL_CACHE_RECEIVE)
22.03.2004	14:38:38	HORSTA	Erfolgter RFC-Aufruf SALC_CACHE_ALERTS_RECEIV (FuGr=SAL_CACHE_RECEIVE)
22.03.2004	14:38:38	HORSTA	Erfolgter RFC-Aufruf SALF_AGENT_STATUS_UPDATE (FuGr=SALF)
22.03.2004	14:38:38	REICHERT	Erfolgter RFC-Aufruf SXPG_COMMAND_EXECUTE (FuGr=SXPT)
22.03.2004	14:38:39	BUCHHOLZF	Erfolgter RFC-Aufruf RSAU_READ_FILE (FuGr=SLO6)
22.03.2004	14:37:15	BUCHHOLZF	Erfolgter RFC-Aufruf RSAU_GET_AUDIT_CONFIG (FuGr=SECU)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_MT_GET_TID_BY_NAME (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_SNGLMSG_REPORT_MESSAGE (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_MT_GET_TID_BY_NAME (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_TEXTATTR_ASSIGN (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_MT_READ (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_MT_GET_TID_BY_NAME (FuGr=SALC)
22.03.2004	14:37:16	HORSTA	Erfolgter RFC-Aufruf SALC_MT_CUSTOMIZE_WRITE (FuGr=SALC)

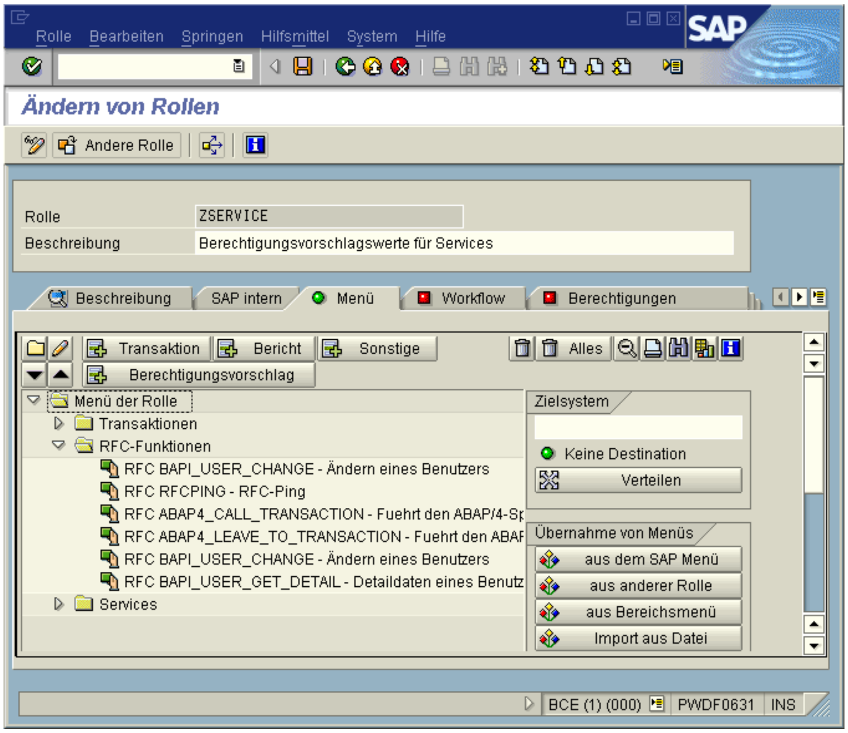
The function group names of the started RFC function modules are displayed.

You can extract the required information by downloading this data and processing it, for example with Microsoft Excel.

SAP plans to make available an evaluation report optimized for the purpose of assigning authorizations.

- After the security audit log was active for the desired time period, you have to analyze it. Transactions are used to show the Security Audit Log. The Log contains the time when the RFC connection was established, the user and the name of the requested function group. The Log could be downloaded an further processed with Microsoft Excel or any other tool to get extract the names of the function modules. SAP plans to make available a optimized report, so that further processing with any external tool is not necessary any more.

RFC Authorizations/Entering Functions in Roles



Rolle: ZSERVICE
Beschreibung: Berechtigungsvorschlagswerte für Services

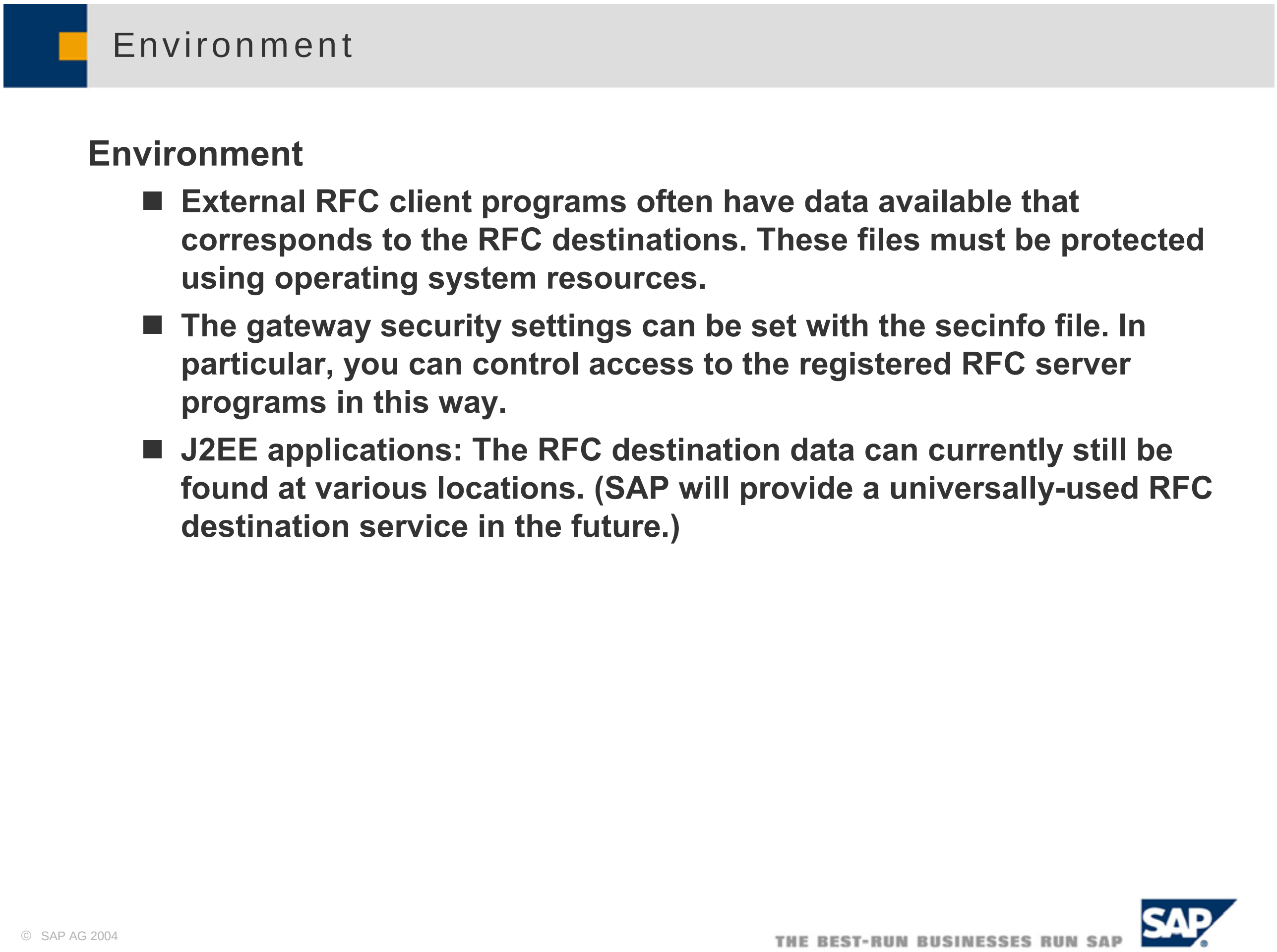
- Menü der Rolle
  - Transaktionen
  - RFC-Funktionen
    - RFC BAPI_USER_CHANGE - Ändern eines Benutzers
    - RFC RFCPING - RFC-Ping
    - RFC ABAP4_CALL_TRANSACTION - Fuehrt den ABAP/4-Sp
    - RFC ABAP4_LEAVE_TO_TRANSACTION - Fuehrt den ABAP
    - RFC BAPI_USER_CHANGE - Ändern eines Benutzers
    - RFC BAPI_USER_GET_DETAIL - Detaildaten eines Benutz
  - Services

Before SAP Web AS 6.20, the function groups found with the Security Audit Log are directly entered into the authorization data for the role.

As of SAP Web AS 6.20, you can alternatively enter the RFC functions in the menu of the role.

THE BEST-RUN BUSINESSES RUN SAP

- After you have analyzed what authorization objects are needed, you now have to build roles that contain that authorizations. Before SAP Web AS 6.20 the authorization objects had to be entered manually in the role using transaction PFCG. As of SAP Web AS 6.20 it is also possible to enter the RFC functions in the menu tab of PFCG.



Environment

Environment

- External RFC client programs often have data available that corresponds to the RFC destinations. These files must be protected using operating system resources.
- The gateway security settings can be set with the secinfo file. In particular, you can control access to the registered RFC server programs in this way.
- J2EE applications: The RFC destination data can currently still be found at various locations. (SAP will provide a universally-used RFC destination service in the future.)

- After the configuration of the RFC connections is secured as described before, there are still some security issues. External RFC clients often store data that corresponds to the RFC destinations. To avoid an attacker form using this information the files that contain the data should be protected. A minimum of protection is normally given by the operating system. There you can configure the access conditions for these files, so that only the RFC client is able to access the file. If the information is stored in clear text, you might wish to implement some security functions such as file encryption in addition to access control functions delivered by the operating system. In that case you should choose a file encryption tool that is implemented as a I/O driver for the file system and so performs transparent data encryption.
- To control access to the registered RFC server programs, you can edit the gateway security settings in the secinfo file.
- In addition, you have to be careful with J2EE applications. In various applications, the RFC destination data can still be found. So you should configure the access conditions of the applications well. SAP will provide a universal RFC destination service in the future which solves the security issue with J2EE applications.

RFC Security

Questions?

security@sap.com

URL: http://service.sap.com/security

© SAP AG 2004

THE BEST-RUN BUSINESSES RUN SAP

Copyright 2004 SAP AG. All Rights Reserved

THE BEST-RUN BUSINESSES RUN SAP