

Externer Zugriff auf SAP R/3-Systeme über RFC

Von Dipl.-Betriebswirt Christoph Wildensee, CISM, CIFI, IV-Revisor Stadtwerke Hannover AG

Einleitung

Der ‚Remote Function Call‘ (RFC) bildet die Grundlage für die Integration mehrerer SAP-Systeme, aber auch die bidirektionale Anbindungsmöglichkeit weiterer Systeme mit entsprechender Datenversorgung. Somit bietet diese Technik des entfernten Funktionsaufrufes als Standardschnittstelle die Möglichkeit, Funktionsbausteine in entfernten SAP-Systemen auszuführen – Funktionen und Daten werden für die Verwendung in und aus anderen Systemen verfügbar gemacht. Über RFC wird auch die Kommunikation mit anderen Mandanten desselben Systems hergestellt.

Standardmäßig sind in jedem SAP-System bereits RFC-Verbindungen vorhanden, z.B. für das Transport Management System und die Verbindungen zu allen Applikationsservern. Hinzu kommen naturgemäß die Konsolidierungsverbindungen zwischen den Systemen untereinander wie z.B. IS-U und Classic sowie HR und Classic, sofern die Systeme getrennt gefahren werden.

Risiken

Der Mechanismus des Datenzugriffs in SAP-Systemen ist zweigeteilt. Zum einen wird die Transaktion, d.h. der Aufruf des SAP-Programmpaketes, das einen Arbeitsabschnitt eines Prozesses darstellt, geschützt. Zum anderen werden die Zugriffe auf die eigentlichen Schlüsselinformationen und zumeist der damit verbundene Manipulationsgrad innerhalb der Transaktion über Berechtigungsobjekte gesteuert. Das Gewähren einer Transaktion bedeutet somit nur in Kombination mit den ausgeprägten Berechtigungsobjekten, dass der betriebswirtschaftliche Ablauf mit entsprechenden Daten in SAP vollständig ausgeführt werden kann.

Die Ausprägung der Berechtigungen in den SAP-Systemen erfolgt auf Transaktionsebene üblicherweise restriktiv, während auf Berechtigungsobjektebene meist aus Gründen der Administrationsentlastung durchaus eine „Übersorgung“ anzutreffen ist. Ging man bisher davon aus, dass ein Ausnutzen der höheren Rechte nicht möglich ist, wenn Transaktionen nicht gewährt werden, ergibt sich – dies gilt sowohl in den Fachmodulen als auch auf Customizing- und Entwicklungsebene, d.h. dem Entwickeln und Ausführen von Quellcode – über die Nutzungsmöglichkeit **externer Connectoren** ein anderes Bild. Es ist häufig einer Vielzahl von Mitarbeitern möglich, über die Nutzung der RFC-Schnittstelle und externer Zugriffsprogramme, die frei verfügbar sind, uneingeschränkt auf SAP-Tabellen Zugriff zu nehmen, ohne dabei die Transaktionsberechtigungen innerhalb der Berechtigungsstämme aufzuweisen. Darüber hinaus sind häufig nicht nur uneingeschränkte Lesezugriffe möglich, es kann auch unprotokolliert über RFC ABAP-Quellcode zur Ausführung gebracht werden. Dies sind erhebliche Sicherheitslücken, die es zu schließen oder zumindest sinnvoll zu handhaben gilt.

Gegen die pauschale Unterstellung eines solchen Vorgehens durch Mitarbeiter wird sich jeder verwahren, insbesondere in den als kritisch erachteten SAP-(Neben)Buchhaltungssystemen sind solche Möglichkeiten jedoch durch die gesetzeskonforme Ausgestaltungsnötigkeit und der unzureichenden Protokollierung ausgesprochen prekär. Ich erinnere an dieser Stelle gern an die Problematik des Tabellen-Debuggings und der Nutzung der Replace-Funktion.

Grundlagen

Generell werden RFC-Anmeldungen nicht protokolliert. Über das AuditLog (SM19) besteht die Möglichkeit, erfolgreiche und gescheiterte RFC-Verbindungszugriffe und Funktionsbausteinaufrufe zu protokollieren und über die SAPLogHistorie auszuwerten (s. Tabelle USOBT => SM19 = S_ADMI_FCD mit AUDA und AUDD). Die zugrunde liegenden Berechtigungen sehen wie folgt aus:

Verwalten von RFC-Verbindungen:

<u>Objekt</u>	<u>notwendige Eingrenzung</u>
S_TCODE	TCD: SM59
S_ADMI_FCD	Funktion: NADM

Aufruf von Funktionsbausteinen:

<u>Objekt</u>	<u>notwendige Eingrenzung</u>
S_RFC	Aktivität: 16 (Ausführen)
	RFC-Typ: FUGR (Funktionsgruppe)
	RFC-Name: <Name der RFC-Funktionsgruppe>

Der relevante Systemparameter über RSPARAM / RSPFPAR ist AUTH / RFC_AUTHORITY_CHECK (≥ 1 [0=keine Prüfung im System], System-Default=1).

SAP R/3 stellt spezifische Funktionsbausteine zur Verfügung, die mittels externer Programmzugriffe aufgerufen werden können. Diese können Tabelleninhalte zurückgeben oder auch ABAP-Quellcode enthalten, der im Zielsystem ohne dezidierte Detail-Protokollierung ausgeführt wird. Es existieren ca. 200.000 Funktionsbausteine und BAPI's, von denen etwa 15.000 remotefähig, d.h. über RFC aufrufbar, sind (TFDIR / TFTIT, ENLFDIR). Funktionsbausteine sind in Funktionsgruppen zusammengefasst. Sofern einem Benutzer die Berechtigung auf S_RFC mit Aktivität = 16, RFC-Objekt = FUGR und einer Eingrenzung in der Funktionsgruppe (RFC_NAME) zugewiesen wurde, kann er über RFC auf alle Funktionsbausteine der Funktionsgruppe zugreifen. Ein Beispiel für einen problematischen Baustein ist RFC_ABAP_INSTALL_AND_RUN der Funktionsgruppe SUTL. Mit diesem ist es möglich, beliebigen externen Quellcode im Zielsystem auszuführen. So kann auch Quellcode übergeben werden, der Daten manipuliert. Diese Berechtigung kann also zum Verstoß gegen § 239 (Radierverbot) und §257 HGB (Aufbewahrung von Unterlagen - Verfahrensdokumentation) genutzt werden.

Ausführen von Quellcode im Zielsystem:

Objekt	notwendige Eingrenzung
S_RFC	Aktivität: 16 (Ausführen) RFC-Typ: FUGR (Funktionsgruppe) RFC-Name: SUTL
S_ADMI_FCD	Funktion: MEMO (Speicherverwaltung)
S_DEVELOP	Aktivität: 03 (Anzeigen) Objekttyp: PROG (ABAP-Programm)

Für den uneingeschränkten Lesezugriff sind erheblich geringere Berechtigungen als zum unprotokollierten Ausführen von Quellcode notwendig (z.B. FuBa: RFC_READ_TABLE; GET_TABLE RFC; TABLE_ENTRIES_GET_VIA RFC).

Uneingeschränkter Lesezugriff:

Objekt	notwendige Eingrenzung
S_RFC	Aktivität: 16 (Ausführen) RFC-Typ: FUGR (Funktionsgruppe) RFC-Name: RFC1/SDTX/SR1T/SRTT/BDCH
S_TABU_DIS	Aktivität: 03 (Anzeigen) Berecht.gruppe: alle bzw. als kritisch erkannte, z.B. aus FI oder HR

Die hier problematischen Funktionsgruppen sind somit BDCH, RFC1, SR1T, SRTT, SDTX und SUTL, da externe Programme üblicherweise mit den hier enthaltenen Funktionsbausteinen Zugriffe definieren, Stati abfragen und Datenaustausch betreiben (siehe SE37; Berechtigung zur Anzeige von Informationen aus dem Data Dictionary und RFC-Zugangsdefinition: z.B. SRFC, SDIF*, SG00, SUSO, SUSE und SYS*).

Funktionsgruppe	Kurztext Funktionsgruppe
Name des Funktionsbausteins	Kurztext zum Funktionsbaustein
SYST	System-Interface
ABAP4_LEAVE_TO_TRANSACTION	Führt den ABAP/4-Sprachbefehl LEAVE TO TRANSACTION aus.
RFCPING	RFC-Ping
RFC_TCP_IP_CONNECTION_OPEN	Dyn. Verbindung zu RFC-Serverprogramm
SYSTEM_ATTACH_GUI	Startet SAPGUI und verbindet es mit dem aktuellen Modus (interne Verw.
SYSTEM_FORMAT	Bestimmen der Codepage und des Zahlenformats
SYSTEM_GET_UNIQUE_ID	Erzeugt eine eindeutige ID (obsolet -> SYSTEM_UUID_C_CREATE verwenden)
SYSTEM_HOOK_OPEN_DATASET	Hook für OPEN DATASET
SYSTEM_INFO	Auslesen von System-Informationen
SYSTEM_REMOTE_LOGIN	Remote Login
SYSTEM_UUID_CREATE	Erzeugt eine UUID im X-Format
SYSTEM_UUID_C_CREATE	Erzeugt UUID im Character-Format
TABLE_COMPRESS	Interne Tabelle komprimieren
TABLE_DECOMPRESS	Interne Tabelle dekomprimieren
SRFC	RFC-Verwaltung
RFC_GET_LOCAL_DESTINATIONS	Liefert alle momentan aktiven RFC-Destinations an derselben Datenbank
RFC_GET_LOCAL_SERVERS	Liefert alle momentan aktiven RFC-Destinations an derselben Datenbank
RFC_LOGIN	explizite Login eines Users.
RFC_PING	RFC-Ping
RFC_PUT_CODEPAGE	Lädt Codepagefile <frompage><topage> CDP auf Harddisk
RFC_SYSTEM_INFO	Liefert versch. Informationen über das System.
SYSTEM_INVISIBLE_GUI	Lässt aktuellen GUI unsichtbar (interne Verwendung)
SYSTEM_RFC_VERSION_3_INIT	Initialisiert ein RFC-Verbindung auf dem Server (systeminterne Verweend)
SDTX	Desktop Access
RFC_READ_TABLE	External access to R/3 tables via RFC
SUTL	Utilities
RFC_ABAP_INSTALL_AND_RUN	Installation und Ausführung eines ABAP/4
SYSU	RFC resource administration
SYSTEM_RESET_RFC_CONNECTION	Free all resources for RFC connection
SYSTEM_RESET_RFC_SERVER	Free all resources for RFC server
BDCH	ALE-Konsistenzprüfungen
CONTROL_DATA_OBJECT_CHECK	Prüfung für Steuerdatenobjekt
MESSAGE_CHECK_TECHNICAL_DATA	Prüfung der technischen Einstellungen für Nachrichtentyp
OBJECT_GET_ENTITY_TABLES	Ermittlung der Entitätstabellen für Steuerdatenobjekt
OBJECT_MODELING_CHECK	Prüfung der Modellierung für Steuerdatenobjekt
PARTNER_LOGICAL_SYSTEM_GET	Logisches System des Partnersystems holen
TABLE_ENTRIES_GET_VIA_RFC	Tabelleneinträge aus einem anderen System über RFC holen
TABLE_GET_CONTROL_DATA_OBJECTS	Ermittlung der Steuerdatenobjekte für eine Tabelle
TABLE_GET_PRIMARY_OBJECTS	Ermittlung der primären Steuerdatenobjekte für eine Tabelle

Abb. 1: Problematische Funktionsgruppen (Auszug)

Externer Zugriff auf die SAP-Systeme

Das bisher als eher theoretisch behandelte Szenario des Zugriffs auf SAP-Systeme durch externe Programme oder Zugangskanäle erhält durch die Vielzahl frei verfügbarer Programme einen praktischen Bezug. Mit Hilfe des Programms ‚ExtractOnDemand for SAP‘ (EOD), welches ausschließlich lesende Zugriffe bereitstellt, wird dieses Bedrohungsszenario beispielhaft realistisch betrachtet. Dabei sollte der Zugriff stichprobenartig sowohl mit produktiven Berechtigungen als auch mit einem Testuser unter Laborbedingungen analysiert werden. Download-Authorisation o.ä. wird nicht benötigt, da das Tool eine eigene Preview- und Download-Funktion offeriert.

Nicht jeder Mitarbeiter im Unternehmen wird das Recht besitzen, Programminstallation durchzuführen, ein Ausschluss solcher Rechte ist jedoch kaum sicherzustellen. Hinzu kommen temporär zugelassene Konfigurationen (aus Projekten o.ä.), die ebenfalls kaum abzusichern sind.

Des Weiteren werden nicht bei jeder Programminstallation lokale Administrationsrechte benötigt. Beispielsweise wird die Schnittstelle als Java-Connector (siehe bereitgestellte Klassen aus JCo) oder Access-Addon geliefert oder die Connection wird über server-basierte Skriptsprachen wie etwa PHP (siehe auch Open Source Projekt ‚SAPRFC‘ von Eduard Koucky) oder Perl (SAPRFC-Extension) bereitgestellt. EOD ist allerdings ein komplexes Programmpaket.

Zuletzt ist hier noch zu erwähnen, dass die Nutzung dieser Lücke auch über Systemgrenzen hinweg über die Verbindung von SAP-System zu SAP-System, je nach Berechtigungsausgestaltung z.B. von Entwicklung oder Test / Integration zu Produktion, möglich ist und somit ein fehlender Praxisbezug nicht unterstellt werden kann. Die Installation externer Programme stellt den schwierigeren Weg dar, insofern ist ein solches Szenarien durchaus als gegeben einzuschätzen.

Extract On Demand for SAP

EOD ist ein frei zugängliches Programmpaket, welches über die SOLONDE-Seite bezogen werden kann. Nach der Installation wird ein Licence-Key benötigt, dieser wird für eine befristete Testlizenz nach einer Registrierung bereitgestellt. Nach Vorliegen der Schlüsseldatei im Programmverzeichnis können alle SAP-Systeme angesteuert werden. EOD nutzt die SAP-Logon-Systemeinstellungen aus der SAPLOGON.INI oder eine manuelle Einstellung, die unter ‚Advanced‘ eingerichtet werden kann - das Zugangsprocedere ist mit dem des SAPGUI-Logon vergleichbar.

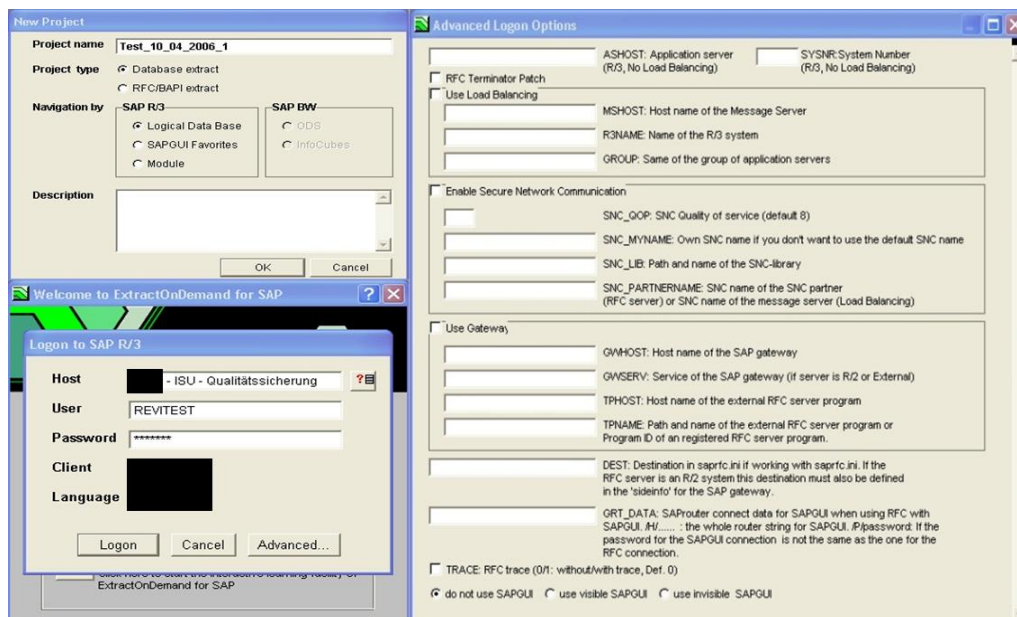


Abb. 2: Zugriff über EOD (Logon)

Nach erfolgreicher Anmeldung können aus den Tabellengruppen einzelne Tabellen- und View-Felder ausgewählt (Joins) und zu einer ‚Output-Fields‘-Liste zusammengestellt werden. Ein Search-Modus ermöglicht die explizite Suche nach einzelnen Tabellen und Views, deren Daten über die Preview-Funktion angezeigt werden können. Grundsätzlich sind - vorbehaltlich entsprechender Berechtigungen - alle Daten eines SAP-

Systems im Zugriff, die in Tabellen vorgehalten werden. Es gibt einige Bereiche, in denen die Daten in Binärform oder verschlüsselt vorliegen. Diese können nicht ohne weiteres aufgelöst werden, hierzu sind zusätzliche Bausteinaufrufe oder BAPI's zu nutzen (z.B. für Feldbeschreibungen DDIF_FIELDINFO_GET). Strukturen wie z.B. im HR die Infotypstruktur P0008 sind nicht notwendigerweise mit Tabellen verknüpft, sondern dienen meist der Aufbereitung von Daten aus verschiedenen Tabellen. Diese Strukturen werden nicht angezeigt – sehr wohl aber die zugehörigen Tabellen.

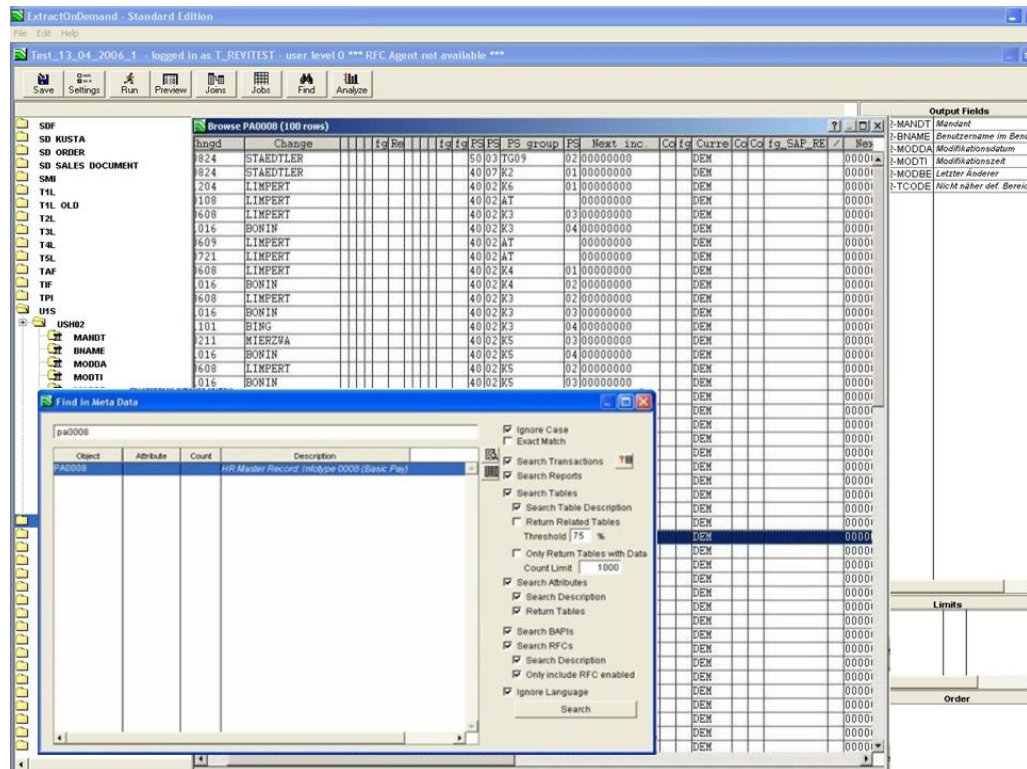


Abb. 3: Zugriff über EOD (HR PA0008)

Als besonders sensibel gelten beispielsweise die Payment-Daten. Auch diese sind über die Metadatenuche selektierbar, allerdings muss hier die BAPI-Technik (d.h. über Mitgabe eines BAPI's [HR-Cluster] – siehe u.a. BAPI_GET_PAYSLIP [Entgeltnachweis für Mitarbeiter]) einbezogen werden, um auf der Mitarbeiterebene, d.h. im detaillierten Einzelzugriff, Daten aufzubereiten.



Abb. 4: Zugriff über EOD (Payment)

So lassen sich gewünschte Ergebnislisten per Preview und Download ohne Protokollierung im SAP beliebig auf dem Arbeitsplatzrechner zusammenstellen.

Fazit

Der hier beschriebene Zugriff auf SAP-Systeme demonstriert eine einfache Handhabung beim problemlosen Umgehen dokumentierter / gewünschter Sicherheitspolicies. Es zeigt sich deutlich, dass eine Beschränkung der Berechtigungsstrukturen in SAP nicht ausreicht, die umfangreichen betriebswirtschaftlichen Informationen, die im SAP - als die im Unternehmen zumeist maßgebliche Datenhaltung - abgelegt werden, abzusichern. Zum einen ist der Zugriff im SAP selbst, aber auch auf Betriebssystem- und Datenbankebene zu begrenzen, zum anderen besonders aber auch die Kanäle, die sich über die SAP-Schnittstellen und die Nutzung externer Connectoren ergeben. Dieser letzte Punkt kann nur unterbunden werden, wenn die Schnittstellen überwacht und eingeschränkt werden.

Folgende Maßnahmen sind hierzu u.a. erforderlich:

- Restriktiver Ansatz bei der Vergabe von RFC-Zugriffsberechtigungen
- Protokollierung gescheiterter, aber auch geglückter Zugriffsversuche * über RFC und Dokumentationspflicht für die entsprechenden Benutzungen
- Auswertung der Protokollierung hinsichtlich dieser Ereignisse
- Reduzierung der Berechtigungen:
 - Ausschluss von: S_ADMI_FCD: Funktion MEMO für alle Benutzerstammsätze; Ausnahme: Notfalluser, SAP-Hotline und Nicht-Dialog-User / Systemuser
 - Ausschluss von: S_RFC: Funktionsgruppen BDCH, RFC1, SR1T, SRTT, SDTX und SUTL; Ausnahme wie zuvor
 - Einschränkung von: S_TABU_DIS: dezidierte Einschränkung auf Ebene der Tabellengruppen auch für Anzeige der Tabellen bei allen Benutzern
 - Einschränkung der Definitionsmöglichkeit von RFC-Destinationen (SM59 / NADM) => nur für SAP-Basisadministration und Notfalluser
- Analyse weiterer konkurrierender Zugangskanäle (auch RFC im Kundennamensraum u.a.) und möglicher Datencontainer und Eingrenzung dieser
- Positionierung des Unternehmens hinsichtlich des generell anzustrebenden Sicherheitsniveaus im Umfeld der SAP-Systeme und Risikoklassifizierung betriebswirtschaftlicher Informationen

Häufig entscheidet das Unternehmen aus wirtschaftlichen Erwägungen heraus, die Administration in strukturellen Fragen zu entlasten und lediglich einen geringen Teil der Einschränkungsmöglichkeiten des SAP-Systems zu nutzen. Es wird also auf der Ebene der Datenabsicherung in den SAP-Funktionen nicht in dem Maße eingegrenzt, wie dies sinnvoll ist („Überversorgung“ auf der Ebene der Berechtigungsobjekte) und überwiegend die Transaktionsebene als Schlüssel zur Funktionsbereitstellung genutzt. Tatsächlich substituiert ein wie hier dargestelltes Tool jedoch die bewusst entzogene Transaktionsberechtigung im Zielsystem (SE16, SQ01 usw.).

Es ist kaum zu verhindern, dass Schnittstellen durch externe Connectoren genutzt werden – es steht bereits eine Vielzahl von Tools zur Verfügung. Eine Reglementierung dieser von SAP bereitgestellten offenen, jedoch nicht jedem offensichtlichen Schnittstellen ist unausweichlich.

Ausgesuchte Literatur:

Beyer/Fischer/Jäck u.a. SAP Berechtigungswesen – Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, SAP Press / Galileo Press, Bonn, 2003;

Thomas Tiede SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP), 2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, S. 282 - 304, <http://www.osv-hamburg.de>;

Christoph Wildensee Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht - Teil 1 bis 3 für Basis, FI & CO; Das SAP R/3 IS-U-Berechtigungskonzept – Versorgungswirtschaft – Ein Prüfungsansatz für die Interne Revision; Regelungsbedarf über die Berechtigungsdefinition und -vergabe hinaus, ReVision III/2001ff, Ottokar-Schreiber-Verlag, Hamburg, <http://www.osv-hamburg.de>;

OPAL SAP Data Downloader <http://www.opalsoft.com.au>

SOLONDE ExtractOnDemand for SAP <http://www.solonde.com>

TISCOM RFCdirect <http://www.tiscon.com>

WINSHUTTLE TablePro <http://www.winshuttle.com>

* **Zu beachten ist:** Schnittstellen- und Systemuser (Archivierung, HR-CO-Koppelung o.ä.), aber auch Stammsätze für den Zugang zu HR-ESS benötigen die RFC-Berechtigung, dieser Zugang ist i.o.S. prinzipiell nicht beachtenswert. **Aber:** Viele Systeme knüpfen über RFC an die SAP-Systeme an (z.B. auch ACL über DirectLink), RFC bietet jedoch bisher keine Authentifizierung von Fremd-Systemen, die die eingerichtete Berechtigung nutzen. Ist ein Benutzerstammsatz berechtigt, über RFC auf das SAP-System zu schalten und Daten zu lesen oder zu manipulieren, ist er hierzu mit **allen externen** Programmen / Connectoren in der Lage.

* **Zu beachten ist außerdem:** Sowohl in diesem als auch im folgenden Artikel SAPRFC2 wird nicht explizit dargestellt, dass Funktionsgruppen wie z.B. SUSE, SUSO, SYST, SRFC, RFC1, RFCH usw., die den Zugang per RFC erst ermöglichen, vorhanden sein müssen. Die Artikel fokussieren auf die zu nutzenden kritisch-funktionalen Funktionsbausteine, wenn per RFC eine Datenselektion oder Datenmanipulation vorgenommen werden soll. Diese werden als kritisch bezeichnet. Natürlich ist die Nutzungsbedingung, dass zuerst einmal der Zugang an sich vorhanden sein muss. Dieser wird durch die obigen Gruppen ermöglicht (siehe auch Trace-Lauf). Entsprechend sind auch die obigen Funktionsgruppen zu beachten. Soll der RFC-Zugang einer Berechtigung gekappt werden, ist das Entfernen der Zugangsgruppen ein erster sinnvoller Schritt, sofern die Integrationsnotwendigkeiten nicht dagegen sprechen. Eine Schlüsselrolle nimmt dabei auch die Gruppe RFC1 ein.

Funktionsbaustein (Grundlage Tabellen lesen)	Funktionsgruppe
RFCPING	SYST
RFC SYSTEM INFO	SRFC
RFC GET FUNCTION INTERFACE	RFC1
RFC GET UNICODE STRUCTURE	RFCH
SUSR LOGIN CHECK RFC	SUSO
SUSR USER AUTH FOR OBJ GET	SUSE
(DDIF FIELD*	SDIFRUNTIME)
[... Bausteine, die dann weiter genutzt werden]	

siehe auch

http://www.wildensee.de/Artikel_SAPRFC2.pdf

Ein letzter Hinweis

Sofern zunächst grundsätzlich ein unkontrollierter Zugriff über S_RFC verhindert werden soll, kann die folgende Grunddefinition von Funktionsgruppen Verwendung finden:

- ARFC
- ATSV
- CJDT
- ERFC
- GR*
- LPRF
- SH05
- SINA
- SLST
- SMTR
- SO*
- SPOX
- SWEL
- SWOR
- SWWA
- THFB

u.a.

Zu einer solchen Basisausstattung von Funktionsgruppen, die jeder Rolle zugewiesen wird, können dann rollenindividuell weitere Funktionsgruppen hinzugefügt werden, die prozessintegrativ notwendig sind. Eine Klassifizierung der Funktionsgruppen kann dabei helfen, die wesentlichen Gruppen herauszufiltern, die grundsätzlich nicht zur Verfügung gestellt werden sollen und die ggf. auch den Administrations-, Modulbetreuer- und Entwicklerrollen nicht bereitgestellt werden.