

# Nachvollzugsansätze zum Remote Function Call in SAP durch Entwicklungen der Berechtigungssteuerung

*Dipl.-Betriebswirt Christoph Wildensee, CISM, CRISC, IV-Revisor und Datenschutzbeauftragter der Stadtwerke Hannover AG.*

## 1. Einleitung

Die Methodik des „Remote Function Call“ (RFC), im ursächlichen Sinn der systemübergreifende Aufruf von funktional abgeschlossenen Codebausteinen mit entsprechenden Übergabestrukturen, bildet eine der Grundlagen für die Prozessintegration mehrerer SAP-Systeme, aber auch die bidirektionale Anbindung von Non\_SAP- zu SAP-Systemen mit entsprechender Datenversorgung. Möglich sind entfernte Funktionsaufrufe mit Datenbereitstellungen, aber auch Durchreichungen von Benutzerzugriffen mit prozessualen Aufrufen im Zielsystem. Die Funktion ist prinzipiell veraltet, jedoch durch ihre Schlichtheit und das multiple Einsatzpotential für die Administration kaum wegzudenken. Entsprechend hat SAP auch in den letzten Jahren maßgebliche Erweiterungen hinzugefügt. So kommen also nicht nur komplexe (RFC-basierte) Schnittstellentechnologien zur Interprozesskommunikation (Connectoren und eigenständige Multiprotokollserver wie SAP XI / PI) zum Einsatz, sondern auch Verbindungen und Funktionsbereitstellungen der Administration als unkomplizierte RFC-Implementierungen.

## 2. Risiken

In vielen Unternehmen erfolgt die Ausprägung der Berechtigungen in SAP-Systemen auf Transaktionsebene üblicherweise restriktiv, während auf Berechtigungsobjektebene in den Rollen vornehmlich aus Gründen der Administrationsentlastung häufig eine „Übersorgung“ festzustellen ist (z.B. Trennung von Menü- und Modulrollen). Ging man bisher davon aus, dass ein Ausnutzen der höheren Rechte aus der Objektversorgung nicht möglich ist, wenn Transaktionen nicht gewährt werden, ergibt sich – dies gilt sowohl in den Fachmodulen als auch auf Customizing- und Entwicklungsebene – über die Nutzungsmöglichkeit externer Connectoren ein anderes Bild.

Es ist häufig einer Vielzahl von Mitarbeitern möglich, über die Nutzung der RFC-Schnittstelle und externer, frei zugänglicher Programme mindestens uneingeschränkt lesend auf SAP-Tabellen Zugriff zu nehmen, ohne dabei die notwendigen Transaktionsberechtigungen innerhalb der ihnen zugewiesenen Rollen aufzuweisen.

Aber auch die unterschiedlich weit reichende Versorgung von Berechtigungen in sinnvoll abgestuften Systemlandschaften (z.B. vermehrte Rechte in Entwicklungs-, Schulungs-, Test- / Integrationssystemen bei geringeren Rechten im Produktionssystem) eröffnet die Möglichkeit, sofern entsprechende RFC-Destinationen zur Verfügung stehen, die durch die Administration (ggf. versehentlich allen) Benutzern offeriert werden, Einsicht in Daten zu nehmen oder ohne Hinterlegung der Benutzerkennung sogar manipulierende Funktionen aufzurufen (Bereitstellung z.B. über Transportwesen). Dort stehen Datenbestände gespiegelt zur Verfügung mit lediglich temporärem Versatz, eine weit reichende Berechtigungsverorgung in als untergeordnet angesehenen Systemen ist also nicht unproblematisch. Es reicht somit kaum aus, ausschließlich Produktionsumgebungen revisorisch einzusehen – auch die parallelen SAP-Landschaftsbereiche sind von hohem Interesse.

## 3. Grundlagen

Die Einsicht in die Tabelle RFCDES (Destinations-Tabelle für RFC) ergibt einen ersten Überblick über alle im System verfügbaren RFC-Verbindungen. Das Feld „Optionen“ enthält dabei unterschiedliche Informationen, die Aufschluss über Zielsystem, Zielmandant, Schnittstellenbenutzer, Kennworthinterlegung usw. geben. Eingrenzungsparameter hierfür sind z.B.:

- H= IP-Adresse oder System- / Instanzname des Zielsystems
- S= Instanznummer
- N= Logon-Group
- G= Gateway-Server
- M= Mandant des Zielsystems
- X= Load Balancing (LB=ON)
- U= Benutzerstammsatz, der für die Connection hinterlegt ist
- V= Kennwort (in ERP lediglich der Hinweis einer Hinterlegung, vorherige Systeme enthalten Hash)
- L= Sprache (D) .

Die Eingrenzung zu Verbindungen des **Typs 3** (Connection-Typ für Verbindungen zu ABAP-Systemen [siehe Domäne RFCTYPE mit Wertebereich]; Änderungsnachvollzug über Report RSTBHIST) legt Hinweise auf relevante Verbindungen der Systeme untereinander offen. Kritische Systemkommunikationsverbindungen sind bereits hier erkennbar. Die Verwaltung und insbesondere auch der Test der Destinationen erfolgt über die Transaktion SM59 (RFC-Destinationen Anzeige und Pflege).

Weitere interessante Transaktionen in diesem Kontext sind beispielsweise:

- SE37                    Function Builder
- SM20 / SM21        Auswertung Security-Audit-Log / System-Log
- ST22                    ABAP Dumpanalyse
- SMT1 / SMT2        Trusted / Trusting Systeme (Anzeige und Pflege)
- SMGW                    Gateway Monitor

SAP stellt remotefähige Funktionsbausteine zur Verfügung, die mittels externer Programmzugriffe aufgerufen werden können. Sie werden weitestgehend thematisch gruppiert und als Gruppe zur Verfügung gestellt bzw. als solche berechtigt. Es existieren mehr als 400.000 Funktionsbausteine und BAPI's, von denen mehr als 30.000 in aktuellen Systemen remotefähig, d.h. über RFC aufrufbar, sind (Tabelle TFDIR, Feldbezeichnung Modus [FMODE] = R). Funktionsbausteine arbeiten dabei nicht selten ohne Berechtigungsprüfung oder die Prüfung ist optional. Sofern einem Benutzer die Berechtigung auf das Berechtigungsobjekt S RFC mit Aktivität (ACTVT) = 16, Typ des RFC-Objektes (RFC\_TYPE) = FUGR und einer Eingrenzung in der Gruppe (RFC\_NAME) im Zielsystem zugewiesen wurde, kann er über RFC auf alle Funktionsbausteine der Funktionsgruppe zugreifen.

Beispiele für kritische Bausteine sind zunächst RFC\_ABAP\_INSTALL\_AND\_RUN der Funktionsgruppe SUTL und EBA\_ABAP\_EXECUTE der Gruppe EWRC. Mit diesen ist es möglich, beliebigen externen Quellcode im Zielsystem auszuführen. So kann auch Quellcode übergeben werden, der unprotokolliert Daten manipuliert. Auch der remotefähige Funktionsbaustein EBA\_TABLE\_UPDATE zum Update von Tabellen ist nicht unproblematisch. Diese drei Beispiele haben gemeinsam, dass eine Berechtigung auf das Objekt S\_DEVELOP mit mindestens der Aktivität 02 und Objekttyp PROG benötigt wird (Replace-Funktion <sup>1</sup> [Debugging]; auch Objekttyp DEBUG mit Aktivität 02). Diese Objektausprägung sollte zwar grundsätzlich in keinem produktiven System (analog z.B. S\_SCD0 mit Aktivität 06 [Änderungsprotokolle löschen]) in Arbeitsplatzrollen zu finden sein (Replace-Funktion bestenfalls in der Notfalluserrolle), trotzdem können also die Bausteine unter bestimmten Bedingungen zum Verstoß gegen handelsrechtliche Vorschriften genutzt werden.

#### Ausführen von Quellcode im Zielsystem:

<u>Objekt</u>	<u>notwendige Eingrenzung</u>
S RFC	Aktivität:        16 (Ausführen) RFC-Typ:            FUGR (Funktionsgruppe) RFC-Name:        EWRC oder SUTL
[ S_ADMI_FCD Funktion:	MEMO (Speicherverwaltung; Objekt bei älterem SAP-Release) ]
S_DEVELOP <sup>1</sup>	Aktivität: <b>02 (EWRC) bzw. 01 (SUTL; bis zum Change durch SAP auf 03)</b> Objekttyp:        PROG (ABAP-Programm)

Während der Baustein der Gruppe SUTL (Bezeichnung „Utilities“) zu den systemnahen Funktionen gehört, ist die Gruppe EWRC (Benennung „Interne Tools“) im Bereich der „Industrial Solutions“ zu finden. In diesem Abschnitt Funktionsgruppeneausschlüsse zu identifizieren, ist eher ungewöhnlich.

Es muss aber nicht immer der Manipulationsgedanke im Vordergrund stehen. Für den fast uneingeschränkten Lesezugriff sind erheblich weniger Berechtigungen als zum unprotokollierten Ausführen von Quellcode notwendig (z.B. FuBa: RFC\_READ\_TABLE; GET\_TABLE RFC; TABLE\_ENTRIES\_GET\_VIA RFC).

#### Remote (un)eingeschränkter Lesezugriff:

<u>Objekt</u>	<u>notwendige Eingrenzung</u>
S RFC	Aktivität:        16 (Ausführen) RFC-Typ:            FUGR (Funktionsgruppe) RFC-Name:        SDTX / SR1T / SRTT / BDCH / RFC1 (und ggf. aus Kundennamensraum)

<sup>1</sup> Notwendig für die Nutzung der Replace-Funktion und der Quellcodeausführung ist allerdings auch eine weit reichende Ausprägung der anderen Steuerungsfelder (z.B. \*/\*\* bzw. exemplarisch konkreter ACTVT = (01/02/03/07, DEVCLASS = \*, OBJNAME = \*, OBJTYPE = (DEBUG,) PROG, FUGR, P\_GROUP = \*). Eine Reduzierung analog z.B. S\_DEVELOP mit ACTVT = 01/02/03/07, DEVCLASS = \$TMP, Z\*, OBJNAME = ZQUEUE1, OBJTYPE = PROG und P\_GROUP = ' ' führt **nicht** zur Berechtigung der Inhaltsänderung im Speicher oder von originären SAP-Tabellen.

S\_TABU\_DIS Aktivität: 03 (Anzeigen)  
Berecht.gruppe: alle (\*\*) bzw. ggf. als kritisch erkannte, z.B. aus FI oder HCM

Die problematischen Funktionsgruppen sind somit BDCH, RFC1, SR1T, SRTT, SDTX (Tabellen) und SUTL und EWRC (ABAP), da externe Programme üblicherweise (neben den Gruppen zum eigentlichen Verbindungsaufbau) mit den hier enthaltenen Funktionsbausteinen Zugriffe definieren, Stati abfragen und Datenaustausch betreiben.

Im Zuge der Tabellenzugriffe werden auch solche bereitgestellt, die keiner Berechtigungsgruppe zugeordnet sind. Eine Zuordnungsüberprüfung von Tabellen zu Berechtigungsgruppen kann über die Tabelle TDDAT (Feld CCLASS; Wenn hier kein Eintrag gefunden wird, erfolgt eine Default-Prüfung gegen die Dummy-Berechtigungsgruppe '&NC&') erfolgen, die zur Verfügung stehenden Tabellenberechtigungsgruppen finden sich in der Tabelle TBRG (Objekt [BROBJ] = 'S\_TABU\_DIS').

In Systemen mit aktuellem SAP-Netweaver-Kernel-Release ab 700 ergeben sich Eingrenzungsmöglichkeiten über ein neues Berechtigungsobjekt (SAP-Hinweis 1481950 vom 07.11.2010), das in älteren Releaseständen nicht offeriert wird. Es können Zugriffe auf einzelne – d.h. konkret angegebene – Tabellen eingegrenzt werden.

Dies hat mittelbar auch Auswirkungen auf die RFC-Nutzung (Tabellenzugriff mit externen Mitteln). Sofern keine oder eine geringe Ausprägung des Objektes S\_TABU\_DIS vorliegt, können einzelne Tabellen über das Berechtigungsobjekt S\_TABU\_NAM zusätzlich zugewiesen werden. So ist steuerbar, dass z.B. nur bestimmte Tabellenzugriffe aus Gruppen berechtigt sind, aber eben zusätzlich auch **einzelne angegebene Tabellen** nicht berechtigter Berechtigungsgruppen der S\_TABU\_DIS-Zuweisung. Die Steuerungsfelder dieses neuen Objektes sind ACTVT (Aktivität; z.B. '03' = Anzeige und '02' = Änderung) und TABNAME (Tabellenname).

In der SAP-Help-Dokumentation steht hierzu: „*To also protect tables that are not assigned to an authorization group, you can also use the authorization object S\_TABU\_NAM. It is integrated into the authorization check of the central function module VIEW\_AUTHORITY\_CHECK. In this case, the system first checks S\_TABU\_DIS. If this authorization check is not successful, the system also checks S\_TABU\_NAM. For more information about S\_TABU\_NAM, see SAP Note 1481950.*“ Zunächst sollen also Zugriffe auf Tabellen geschützt werden, die keiner Berechtigungsgruppe zugeordnet sind, es können jedoch über das Berechtigungsobjekt S\_TABU\_NAM dezidierte Tabellenzugriffe zugelassen werden. Das Objekt ist in der Berechtigungsprüfung des zentralen Funktionsbausteins VIEW\_AUTHORITY\_CHECK integriert. Die Priorität der Verarbeitung liegt zunächst in der Prüfung von S\_TABU\_DIS. Ist hier kein Zugriff möglich, erfolgt die Prüfung auf S\_TABU\_NAM. Dieser Ansatz geht davon aus, dass Tabellen, die keiner Gruppe (&NC&) zugehörig sind, über die Eingrenzung nicht zur Verfügung gestellt werden. Wird jedoch hiervon der Zugriff auf Einzelne benötigt, können sie über S\_TABU\_NAM dezidiert zugewiesen werden. Gleiches gilt grundsätzlich für alle Tabellen, die einzeln zugewiesen werden sollen, deren Berechtigungsgruppe aber nicht.

Im OSS-Hinweis steht entsprechend: “[...] Die Berechtigungsprüfung auf S\_TABU\_NAM ist [...] ausschließlich im Baustein VIEW\_AUTHORITY\_CHECK implementiert. Die im ABAP-Code direkt auf S\_TABU\_DIS codierten Berechtigungsprüfungen und die in den Startberechtigungen (Transaktion SE93 oder Tabelle TSTCA) einer Transaktion hinterlegten S\_TABU\_DIS-Berechtigungsprüfungen können durch entsprechende Berechtigungsvergabe zu S\_TABU\_NAM derzeit nicht ersetzt werden. Ein vollständiger Verzicht auf die Vergabe von S\_TABU\_DIS-Berechtigungen ist deshalb nicht möglich.“, was wiederum bedeutet, dass codierte Authority-Check-Prüfungen auf S\_TABU\_DIS nicht abgelöst / ersetzt werden. Entsprechend wird die S\_TABU\_DIS-Eingrenzung in den Berechtigungszuweisungen weiterhin ein kritischer Aspekt bleiben und die Berechtigung auf S\_TABU\_NAM nur als **sektorale Ergänzung** dienen.

In vielen Unternehmen wird allerdings auch kaum von der Möglichkeit Gebrauch gemacht, auf notwendige Tabellen (-Berechtigungsgruppen) einzuschränken, denn hierfür ist zunächst eine (Arbeitsplatz-) Beschreibung notwendig, in der ausgeführt wird, welche Funktionen und Zugriffe in welcher Rollenwahrnehmung überhaupt benötigt werden und welche entbehrlich sind. Um dabei im Tagesgeschäft aber flexibel zu bleiben, erfolgt nicht selten auf der Ebene der Berechtigungsobjekte eine Generalberechtigung oder sehr starke Ausprägung der Steuerungsfelder – auch bei den Objekten S\_RFC und S\_TABU\_DIS. Der Zugriff wird dann wie oben erwähnt zumeist über das Gewähren oder den Entzug von Aufruftransaktionen gesteuert – sowohl auf Modulbetreuer- und Administrations- als auch auf Funktionsebene.

Entsprechend ist es nicht abwegig, dass S\_TABU\_NAM in vielen Unternehmen möglicherweise kaum zu tatsächlichen Tabellenberechtigungseinschränkungen führen wird.

Wesentliche Tabellen und Reports im Bereich der RFC-Bearbeitung:

- RFCDES (Destination-Tabelle für RFC)
- RFCDOC (Beschreibung der möglichen RFC-Verbindungen (=>RFCDES))
- RFCATTRIB (Verwaltungstabelle für RFC-Destinationen)
- TFDIR (Funktionsbaustein) mit Modus (Feld FMODE) = R (remotefähig)
- ENLFDIR (Zusatzattribute zu Funktionsbausteinen)
- TFTIT (Kurztext eines Funktionsbausteins)
- RSRFCRFC (analog und Voraussetzung SM59)
- RSRDEST und RSRDEST (Systemübersicht RFC)
- RSRFCTRC (RFC-Trace-Informationen – Voraussetzung SM59)

<b>Funktionsgruppe Name des Funktionsbausteins</b>	<b>Kurztext der Funktionsgruppe Kurztext zum Funktionsbaustein</b>
<b>BDCH</b>	<b>ALE-Konsistenzprüfungen</b>
PARTNER_LOCICAL_SYSTEM_GET	Logisches System des Partnersystems holen
TABLE_ENTRIES_GET_VIA_RFC	Tabelleneinträge aus einem entfernten System per RFC holen
<b>EWRC</b>	<b>Interne Tools</b>
EBA_ABAP_EXECUTE	PRIVAT: Führt einen ABAP-Code aus
EBA_TABLE_SELECT	PRIVAT: Lesen einer Tabelle per RFC
EBA_TABLE_UPDATE	PRIVAT: Ändern einer Tabelle per RFC (Struktur)
<b>SDTX</b>	<b>Desktop Access</b>
RFC_READ_TABLE	External access to R/3 tables via RFC
<b>SRTT</b>	<b>Funktionen zum remote-Tabellentransport</b>
GET_TABLEBLOCK_COMPRESSED_RFC	Tabelle aus einem anderen System (mittels RFC) holen
GET_TABLE_BY_KEYLIST_COMPRESS	Tabelle aus einem anderen System (mittels RFC) holen
SRTT_GET_COUNT_BEFORE_KEY_RFC	Liefert nächsten Schlüssel und zählt die Einträge ...
SRTT_GET_REMOTE_DOMA_DEF	Holt die Domänendefinition aus einem RFC-System
SRTT_GET_REMOTE_DTEL_DEF	Holt die Datenelementsdefinition aus einem RFC-System
SRTT_GET_REMOTE_TABLE_DEF	Holt die Tabellendefinition aus einem RFC-System
SRTT_GET_REMOTE_TADIR_ENTRY	Holt einen TADIR-Eintrag aus einem RFC-System
SRTT_GET_REMOTE_VIEW_DEF	Holt die View-Definition aus einem RFC-System
<b>SUTL</b>	<b>Utilities</b>
RFC_ABAP_INSTALL_AND_RUN	Installation und Ausführung eines ABAP
<b>RFCl</b>	<b>RFC-Utilities</b>
RFC_GET_TABLE_ENTRIES	Tabelleneinträge lesen
[...]	

Tab. 1: Problematische RFC-Funktionsgruppen (Auszug).

#### 4. Benutzer- / Kennworthinterlegung und Sicherheit

Es besteht grundsätzlich die Möglichkeit, innerhalb von RFC-Destinationsdefinitionen jeweils eine Benutzererkennung mit Kennwort zu hinterlegen. RFC-Verbindungen mit solchen Angaben werden für die automatische Kommunikation zwischen unterschiedlichen Mandanten eines Systems oder auch zwischen verschiedenen Systemen verwendet (RFCDES mit Typ 3 und \*U=\* in Optionen). Beispiele hierfür sind die Verbindungen zwischen HCM und Classic (CO) oder zwischen IS-U und Classic (FI, CO) zur Abbildung der monetären konsolidierten Werteflüsse, sofern die Systeme voneinander getrennt betrieben werden. Dabei können hierüber alle remotefähigen Funktionsbausteine über RFC extern aufgerufen werden, sofern der eingetragene Benutzer entsprechende Berechtigungen aufweist. Falls also ein Benutzer eine solche Definition ansteuern kann, ist der Zugriff auch ohne Eingabe eines Kennwortes möglich, die Protokollierung erfolgt mit der mitgegebenen Benutzererkennung.

Sofern ein externes Programm oder System über eine RFC-Destinationsdefinition einen sicheren Zugriff auf SAP-Funktionalität erhalten soll, kann dieser Verbindungsaufbau über Secure Network Connection (SNC) abgesichert werden.

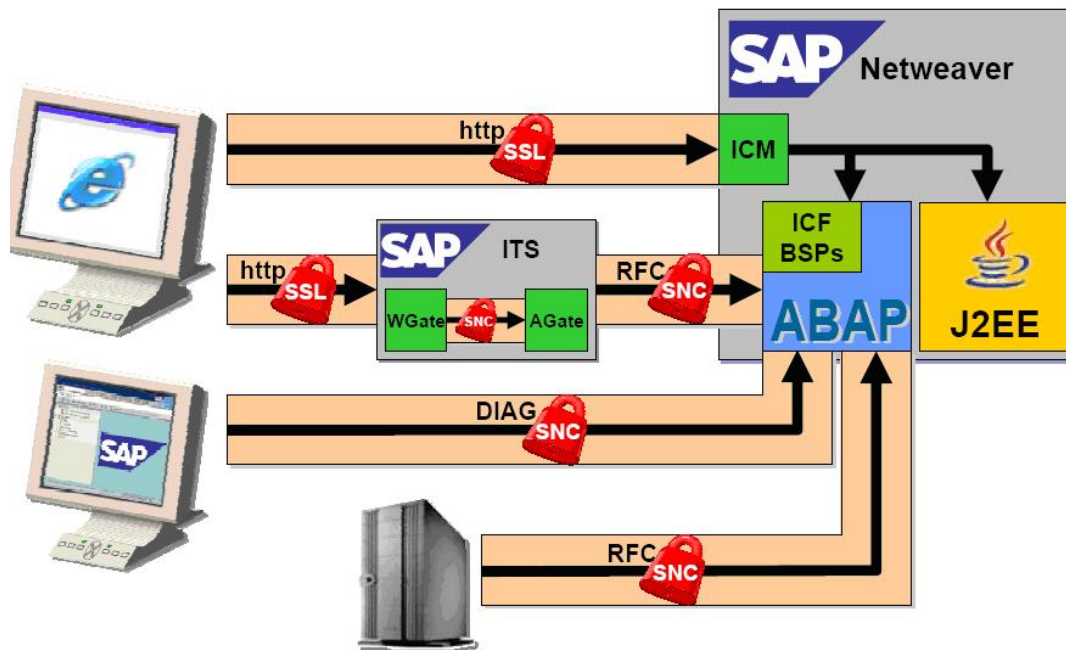


Abb. 1: SNC-Integration im Sicherheitskonzept (Quelle: SAP España, 2005 - „Conexión de acceso local vía SNC“).

Die SAP-Help-Dokumentation stellt fest: „Connections between SAP system components that communicate using RFC can be secured with SNC, which secures the data communication paths between the various SAP system components. SAP systems support external security products that implement cryptographic algorithms. With SNC, you can apply these algorithms to your data for increased protection. SNC supports three levels of security protection: authentication only, integrity protection, and confidentiality protection.“

Es besteht also die Möglichkeit, dass Verbindungen zwischen SAP-System-Komponenten über SNC abgesichert werden – sowohl hinsichtlich SAP-SAP- als auch SAP-Non\_SAP-Kommunikationsvorgängen. Unterstützt werden Sicherheitsprodukte / -bibliotheken, die in die Verbindungsdefinitionen kryptographische Algorithmen implementieren, z.B. von SAP selbst für die Absicherung von SAP-Serverkomponenten die SAP Cryptographic Library. Im Rahmen von SNC sorgen diese Produkte / Bibliotheken für einen gesteigerten Schutz, allerdings müssen sie neben der Plattformverfügbarkeit und der Gewährleistung der SAP-Zertifizierung den vollen Funktionsumfang der Standardschnittstelle GSS-API V2 (Generic Security Service API V2) unterstützen und die Funktionen müssen dynamisch geladen werden können. SNC unterstützt drei Sicherheitsstufen: Ausschließlich Schutz der Authentifizierung (Verifizieren der Identität der Kommunikationspartner), Schutz der Integrität (wird dieser verwendet, ermittelt das System alle Änderungen an Daten, die zwischen den beiden Endpunkten der Kommunikation aufgetreten sind) und Schutz der Vertraulichkeit (Verschlüsselung der übertragenen Nachrichten, was auch den Schutz der Integrität beinhaltet).

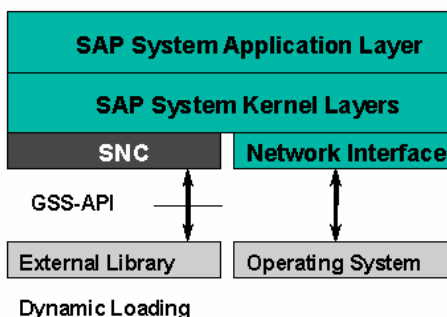
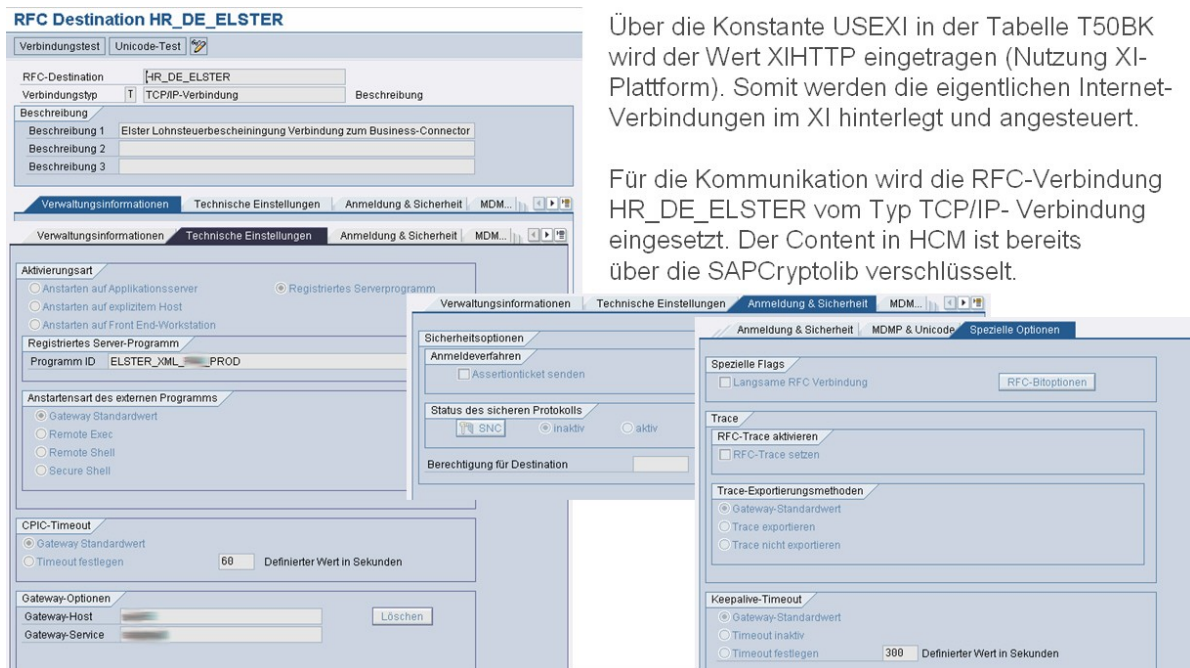


Abb. 2: SNC-GSSAPI-Zusammenspiel (Quelle: SAP).

Die SAPCryptolib findet im Übrigen auch Verwendung bei Einsätzen ohne SNC, z.B. bei der HCM-XI-Integration zur Kommunikation mit den Clearingstellen der Finanzbehörden im Rahmen des „Elster“-Verfahrens. Die Verschlüsselung der Datenpakete erfolgt bereits in HCM über die SAPCryptolib mit dem

Algorithmus PKCS#7 [Public Key Cryptography Standards; Cryptographic Message Syntax Standard]. Die interne Kommunikation zwischen HCM und XI wird folgend per RFC ohne SNC aufgebaut und XI eröffnet einen Transferkanal über http(s) nach außen.



Über die Konstante USEXI in der Tabelle T50BK wird der Wert XIHTTP eingetragen (Nutzung XI-Plattform). Somit werden die eigentlichen Internet-Verbindungen im XI hinterlegt und angesteuert.

Für die Kommunikation wird die RFC-Verbindung HR\_DE\_ELSTER vom Typ TCP/IP-Verbindung eingesetzt. Der Content in HCM ist bereits über die SAPCryptolib verschlüsselt.

Abb. 3: HCM-XI-Integration zum Verfahren „Elster“.

Eine weitere Sicherheitsfunktion ergibt sich über die Verwendung des Berechtigungsobjektes S\_ICF (Berechtigungsprüfung beim Internet Communication Framework - Zugriff). **Ausgehende** RFC-Zugriffe können über dieses Objekt begrenzt werden.

Objekt notwendige Eingrenzung

S\_ICF ICF\_FIELD (Framework-Bereich):

SERVICE, DEST oder PROXY (Services des Frameworks, RFC-Destination [siehe Transaktion SM59] oder Proxy-Einstellungen)

ICF\_VALUE (Framework-Wert):

Prüfwert für Zielobjekt.

Mit dem Wert DEST für den Framework-Bereich und der Angabe eines Absicherungsstrings im Wert-Feld kann die Nutzung auf solche RFC-Verbindungen eingeschränkt werden, die in der Definition unter Logon&Security diesen String aufweisen. Die SAP-Help-Dokumentation unterstreicht: *Man kann in „SM59 einen beliebigen Berechtigungswert (Literal) angeben, der auch im Berechtigungsobjekt [S\_ICF unter ICF\_VALUE und mit ICF\_FIELD=DEST] hinterlegt wird. Nur wenn beide Werte identisch sind, verfügt der Benutzer über die Berechtigung zum Aufruf der Destination“.* Eine '\*'-Generalberechtigung sollte restriktiv vergeben sein.

## 5. Sich vertrauende Systeme

Existiert exemplarisch systemübergreifend ein Workflow, z.B. zur Rechnungsbearbeitung, soll es der / dem Mitarbeiter/-in möglich sein, ohne nochmalige Anmeldung im Zielsystem die Rechnung weiterzureichen und so die Bearbeitung fortzuführen. Möglich wird dies durch die Definition von „Trusted Systems“, d.h. sich vertrauenden Systemen. Im Zielsystem wird das Quellsystem als vertrauenswürdig eingerichtet (Transaktion SMT1), im Quellsystem wird analog eine RFC-Verbindung zum Zielsystem aufgesetzt (SM59).

Das Berechtigungsobjekt S\_RFCACL im Benutzerstammsatz des Zielsystems wird bei der Kommunikation von Benutzern von einem zum anderen SAP-System geprüft, um bei vertrauten (oder sich vertrauenden) Systemen die Möglichkeit zu schaffen, ohne Anmeldung am Zielsystem berechtigte Funktionsaufrufe zu starten. Voraussetzung ist eine gleich lautende Benutzerkennung in den Systemen. Die Objektbeschreibung lautet „Berechtigungsprüfung für RFC-Benutzer (Trusted Systems)“.

<u>Objekt</u>	<u>notwendige Eingrenzung</u>	
S_RFCACL	Aktivität (ACTVT):	16 (Ausführen)
	aufrufender RFC-Client oder Domäne (RFC_CLIENT)	NNN (Mandant)
	RFC gleiche Benutzerkennung (RFC_EQUSER)	Y (Benutzer-Kennung in beiden Systemen)
	RFC Information (RFC_INFO)	* (inaktiv)
	System-ID (RFC_SYSID)	<rufendes Quellsystem>
	RFC-Transaktionscode (RFC_TCODE)	*
	RFC User (RFC_USER)	' ' (oder sy-uname)
	(hier ist ein Leerwert oder sy-uname einzugeben, wenn RFC_EQUSER = Y: Ein Benutzer muss in beiden Systemen identische Stammsatzkennungen haben. – Oder explizite Nennung. Grundsätzlich sollte die '*'-Ausprägung in keiner Berechtigung zu finden sein.)	

#### Die Berechtigungsprüfung im Beispiel läuft wie folgt ab:

Der Stammsatz beinhaltet den Transaktionsaufruf zur Weitergabe der Rechnung, er ruft diese auf. Das Zielsystem prüft, ob es sich um einen „Trusted System“-Verbindungsaufbau handelt (siehe auch Transaktion SMT1 für Liste / Definition von Vertrauensbeziehungen). Ist dies der Fall, wird geprüft, ob es einen Stammsatz mit der aufrufenden Benutzerkennung im Zielsystem gibt und es wird im Zielsystem weiterhin verprobt, welche Berechtigung diese hat. Hat der Benutzerstammsatz neben der entsprechenden Eingrenzung von S\_RFCACL auch die Berechtigung der weiteren Rechnungsbearbeitung, erfolgt die weitere Verarbeitung wie gewünscht. Ist dies nicht der Fall, erfolgt der Abbruch mit Hinweisgebung. Der Vorteil ist, dass die bearbeitende Person sich nicht nochmals am Zielsystem anmelden muss – es erfolgt ein „Durchschleifen“ der Anmeldung aus dem Quellsystem.

Die Funktion ist eine integrierte Weiterverarbeitungsfunktion über (SAP-) Systemgrenzen hinweg, sofern sie als gerichtete Verbindung / „Trusted System“ deklariert ist. Das Vertrauensverhältnis zwischen den Systemen ist die Voraussetzung. So kann die S\_RFCACL-Berechtigung wie vorliegend auch in der Berechtigungsobjekt-Grundversorgung enthalten sein. Allerdings birgt sie auch Gefahrenpotentiale. Wird S\_RFCACL im Zielsystem weit reichender konfiguriert, können Verbindungen mit fremden Nutzerkennungen und ohne Kennworteingabe aktiviert werden – die Weiterverarbeitung erfolgt mit ggf. hohen Rollenausprägungen der Zielsystembenutzer (besser: konkrete Angaben in den Steuerungsfeldern und restriktiv mit '\*' für RFC-Client).

## 6. Folgerungen

Die Nutzung des RFC-Mechanismus' bzw. des Remote-Aufrufs von RFC-Funktionsbausteinen ist und bleibt problematisch. Wenn dies auch in der Administrationsebene für die Sicherstellung des laufenden Betriebs nicht zu verhindern ist, sollten die Risiken den Verantwortlichen zumindest bewusst und ein gewisses Maß an Eingrenzung und Überwachung implementiert sein. Kritisch ist RFC insofern, als dass die bereitgestellten remotefähigen Funktionsbausteine – neben der gewollten vornehmlich integrativen Funktion – genutzt werden können, um an der Protokollierung und Berechtigungskonzeption vorbei Informationen / Daten einzusehen oder unbefugt ohne adäquate Dokumentation Daten zu manipulieren. In dieser Form erfüllen die Funktionsbausteine also keinen ursächlich artikulierten Zweck – im Gegensatz zu remotefähigen Bausteinen wie z.B. BAPI\_PO\_CREATE, BAPI\_ISUMOVEIN\_CREATEFROMDATA und ähnliche zur Business-Prozesssteuerung von außen.

Beispiele für kritische Gruppen bei der Nutzung remotefähiger Funktionsbausteine sind wie oben erwähnt also SDTX, SR1T, SR1T, BDCH, RFC1, SUTL und EWRC. Heikel können parallel aber auch beispielsweise Aufrufe der Funktionsbausteine

- INST\_CREATE\_R3 RFC\_DEST [RFC-Verbindungen anlegen ohne Transaktion SM59]
- SYSTEM\_REMOTE\_LOGIN [Remote-Login ohne SM59]
- RPY\_TRANSACTION\_INSERT [Transaktionsanlage im Kundennamensraum mit Referenz auf andere, ggf. gesperrte Transaktionen, jedoch nur mit RFC-Berechtigung nutzbar]
- RPY\_TABLE\* bzw. FuGr SIFD [Tabelle / Struktur bzw. andere Elemente lesen / manipulieren]
- RS\_FUNCTIONMODULE\_INSERT [Anlegen eines eigenen FuBa, nur mit RFC-Berechtigung]
- RS\_FUNCTION\_POOL\_INSERT [Anlegen neuer Funktionsgruppen]
- LAW\_CREATE\* [Kommunikationsbenutzer mit Kennwort und Rolle anlegen bzw. nur Kennwort ändern; RFC-Destination anlegen]
- TPM\_TRG\_READ\_TABLE\_RFC [Tabelle und Tabellenbeschreibung per RFC lesen; Ausgabe allerdings in hexadezimal]
- BBP\_RFC\_READ\_TABLE [External access to R/3 tables via RFC] oder
- CRM\_CODEX\_GET\_TABLE\_VIA\_RFC [Generisches Lesen von Tabelleneinträgen via RFC für CODEX-Report im CRM]

sein, da sie definierte und abgestimmte Sicherheitsmechanismen bzw. Prozess- / Aufgabenverantwortungen aushebeln können. Entsprechend kann die Liste der grundsätzlich kritischen Funktionsgruppen um die Basiseinträge SUNI, SIFD, SAIO, SEUF und SEUK und um Modulfunktionseinträge wie FV64, BBPB und IAOM\_CRMSRV\_SERVICE erweitert werden. Sicherlich lassen sich ggf. noch weitere Gruppen dieser Art identifizieren, speziell auch solche der Fachmodule und auch im Kundennamensraum.

Es ist offenkundig, dass RFC-Definitionen nicht nur in Produktions-, sondern auch in anderen SAP-Systemen wie z.B. Entwicklung, Test / Integration und Schulung kritisch sind, da insbesondere die Administrationsebene, aber auch temporär eingesetzte Berater oder sogar Fachbereichs-Key-User solche Verbindungen in Produktionssysteme ohne ernsthafte Kontrollinstanz schalten können. Funktionsgruppen beinhalten zumeist mehrere Funktionsbausteine, von denen nur wenige kritisch sind, aber viele in den Fachfunktionen benötigt werden. Gleiches gilt für die Tabellenberechtigungsgruppen. Es ist nur vereinzelt belegt, welche Effekte der Entzug einer ganzen Gruppe im Systemverhalten hervorruft, nur um die Wirkung eines oder weniger kritischer Elemente zu eliminieren. So kann kaum verhindert werden, dass auch kritische Bausteine (und trotz Fehlen der Aufruftransaktionen analog kritische Tabellen) im Zugriff verbleiben, um die Systemstabilität nicht zu gefährden bzw. die Berechtigungskonzeption nicht ausufern zu lassen. **Insofern ist eine theoretisch maximale Entzugsstrategie kritischer Elemente kaum umsetzbar. Allerdings ist für diese – unter Wahrung der Prozessautomatismen und integrativen Notwendigkeiten – eine weitgehende Ausschließlichkeit auf Administrations- und Modultreuebene (einschließlich einiger Service- und Schnittstellenuser) bzw. für zu klassifizierende Inhalte eine solche in der Notfallberechtigung anzustreben.**

## **7. Fazit**

Die Renaissance in der Wahrnehmung der Risiken von RFC – nach zwischenzeitlich sehr leisen Erwähnungen – ist nachvollziehbar. RFC stellt für die Revision auch weiterhin einen bedeutsamen Prüfungsaspekt dar, denn diese Funktion mit seinen Erweiterungen wird voraussichtlich noch sehr lange auf Administrations- / Systemzugangsebene in der Benutzung bleiben.

## 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.
- Hex-Umwandlung <http://www.string-functions.com/hex-string.aspx> .
- SAP AG Berechtigungsobjekt S\_ICF,  
[http://help.sap.com/saphelp\\_nw73/helpdata/de/48/9671360eec3987e10000000a421937/content.htm](http://help.sap.com/saphelp_nw73/helpdata/de/48/9671360eec3987e10000000a421937/content.htm) .
- SAP AG Checking Using the Assignment of Authorization Groups to Tables,  
[http://help.sap.com/saphelp\\_nw73/helpdata/en/4c/a0ac7a68243b9ee10000000a42189b/content.htm](http://help.sap.com/saphelp_nw73/helpdata/en/4c/a0ac7a68243b9ee10000000a42189b/content.htm) .
- SAP AG Conceptos de Seguridad en SAP, SAP España, 2005,  
Conexión de acceso local vía SNC,  
<http://aseguresap.com/node/22> .
- SAP AG Integration von SNC und einem externen Sicherheitsprodukt in SAP-Systeme,  
[http://help.sap.com/saphelp\\_nwmobile711/helpdata/de/3f/3dadb1c27344e29f3c7b5864825eb5/content.htm](http://help.sap.com/saphelp_nwmobile711/helpdata/de/3f/3dadb1c27344e29f3c7b5864825eb5/content.htm) .
- SAP AG OSS-Hinweis 1481950 vom 07.11.2010.
- SAP AG RFC and SNC,  
[http://help.sap.com/saphelp\\_nw04/helpdata/en/72/e52c4057cb185de10000000a1550b0/content.htm](http://help.sap.com/saphelp_nw04/helpdata/en/72/e52c4057cb185de10000000a1550b0/content.htm) .
- SAP AG SNC-Terminologie,  
[http://help.sap.com/saphelp\\_nwpi71/helpdata/de/c4/19cb798a9343a2af55a62f860fe930/content.htm](http://help.sap.com/saphelp_nwpi71/helpdata/de/c4/19cb798a9343a2af55a62f860fe930/content.htm) .
- SAP AG Trusted / Trusting zwischen SAP Systemen,  
[http://help.sap.com/saphelp\\_nw70/helpdata/de/8b/0010519daef443ab06d38d7ade26f4/content.htm](http://help.sap.com/saphelp_nw70/helpdata/de/8b/0010519daef443ab06d38d7ade26f4/content.htm) .
- SAP AG Übertragung von Daten über SAP XI;  
[http://help.sap.com/saphelp\\_sem60/helpdata/de/9b/821140d72dc442e10000000a1550b0/content.htm](http://help.sap.com/saphelp_sem60/helpdata/de/9b/821140d72dc442e10000000a1550b0/content.htm) .
- Schrott, Gerald IBS-Newsletter 05.02.2007, 07.04.2009, 05.04.2011.
- Tiede, Thomas SAP R/3 - Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP),  
2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, 2004.
- Wildensee, Christoph Externer Zugriff auf SAP R/3-Systeme über RFC,  
In: PRev Revisionspraxis II/2006, S. 15-19.

## Abstract

Die unbestritten erforderliche integrative Funktion remotefähiger Funktionsbausteine in SAP bedeutet auf der anderen Seite, dass über diese auch unberechtigte Zugriffe auf Informationen ohne Vorliegen der berechtigungsseitigen Voraussetzungen möglich sind. SAP hat zusätzliche Sicherheitsmechanismen eingezogen, die systemübergreifende Kommunikation grundsätzlich autorisieren und absichern soll. Beispiele hierfür sind die Implementierung von Secure Network Connection, die Definition von „Trusted Systems“ und die Gewährung oder Beschränkung von Zugriffen auf dieser Ebene über die Berechtigungsobjekte S\_RFCACL und S\_ICF. Auch die Absicherung von Tabelleneinsichten wurde erweitert um das Objekt S\_TABU\_NAM zur expliziten Gewährung anzugebender Tabellen trotz fehlender Zuweisung der zugehörigen Berechtigungsgruppe. Jedoch bleiben die Möglichkeiten bestehen, am abgestimmten Berechtigungskonzept vorbei Zugriffe zu definieren und ggf. manipulierend in das System einzugreifen. Dabei ist eine theoretisch maximale Entzugsstrategie kritischer Elemente kaum umsetzbar. Ein Entzug bestimmter Funktions- und Tabellenberechtigungsgruppen scheidet zumeist an den im Unternehmen benötigten Berechtigungsstrukturen. Der nachfolgende Artikel thematisiert die Entwicklungen der letzten Jahre und streift die Anpassungsoptionen im Berechtigungskonzept.

**SAP-Abkürzungen:**

- Internet Communication Manager (ICM)
- Internet Connection Framework (ICF)
- Business Server Pages (BSP)
- Internet Transaction Server (ITS)
- Web Application Server (WAS)
- Secure Socket Layer (SSL)

**Verfasser:**

Dipl.-Betriebswirt Christoph Wildensee, CISM, CRISC, ist seit 1993 als IV-Revisor und zusätzlich seit 2008 als Datenschutzbeauftragter bei der Stadtwerke Hannover AG tätig.

**Key-Words:**

SAP, RFC, SNC, Tabellenberechtigungen, Berechtigungsobjekte

**Anlage 1:**

**Vorschlag einer Objektverteilung ausgesuchter besonders kritischer Basis-Objekte \***

Objekt und Wert in besonderen Admin- rollen	Produktionssystem (für Komm.user / Schnittstellenuser, Administratoren, Modulbetreuer...)	System Test / Integration (für Komm.user / Schnittstellenuser, Administratoren, Modulbetreuer...)	Entwicklungs- system (Entwicklerrolle)	Schulungssystem, weitere Systeme (für Komm.user / Schnittstellenuser, Modulbetreuer...)	Notfalluser im Produktionssystem
S_DEVELOP mit Aktivität 01 und PROG			X		
S_DEVELOP mit Aktivität 02 und PROG / DEBUG			X		X
S_DEVELOP mit Aktivität 03 und PROG / DEBUG	X	X	X	X	X
S_RFC mit Aktivität 16 + FUGR + kritische Gruppen (Notwendigkeit je Gr. prüfen; restriktiv)	X	X	X	X	X
S_RFC mit Aktivität 16 + FUGR + SUTL / EWRC					
S_ADMI_FCD mit MEMO					
S_SCD0 mit Aktivität 06					

\* S\_RFC bei Interprozesskommunikation / Integration. Einzelne kritische Funktionsgruppen sind ggf. auch in Fachfunktionsrollen zu implementieren. In S\_DEVELOP mit Aktivität 01 oder 02 muss auch eine starke Ausprägung in den anderen Steuerungsfeldern vorliegen.