# Kapitel 5
# Remote Function Calls

*Schnittstellen sind ein Einfallstor für Angriffe auf SAP-Systeme. In diesem Kapitel erfahren Sie alles zur Absicherung und Prüfung dieser Schnittstellen.*



*Remote Function Calls*, kurz RFCs (entfernte Funktionsaufrufe), sind Aufrufe von Funktionsbausteinen in einem anderen SAP-System. Funktionsbausteine sind ausführbare ABAP-Programme. Sie können von anderen Systemen aus (SAP- und Nicht-SAP-Systemen wie z. B. Microsoft Excel) aufgerufen werden. Berechtigungen zum Ausführen von Funktionsbausteinen werden in Berechtigungskonzepten häufig vernachlässigt, wodurch eine große Gefahrenquelle entsteht. Per RFC können z. B. Verbindungen zu anderen Systemen angelegt oder Buchhaltungsbelege gebucht werden – und das ohne weitere Berechtigungsprüfungen. In diesem Kapitel erfahren Sie, welche Gefahren durch falsche RFC-Konfigurationen entstehen und welche Sicherungsmaßnahmen Sie dagegen ergreifen können.

## 5.1 Funktionsbausteine

Die RFC-Technologie bietet die Möglichkeit, *Funktionsbausteine* in entfernten Systemen aufzurufen. Funktionsbausteine sind ausführbare ABAP-Programme. Sie können *remotefähig* sein. Dies bedeutet, sie können auch von anderen Systemen (SAP- und Nicht-SAP-Systemen) aus aufgerufen werden. Es existieren über 500.000 Funktionsbausteine in SAP ERP bzw. SAP S/4HANA. Davon sind über 45.000 Funktionsbausteine remotefähig und können somit von anderen SAP-Systemen oder Fremdsystemen aus aufgerufen werden.

Mit Funktionsbausteinen können Aktionen ausgeführt werden, für die auch Transaktionen existieren. Tabelle 5.1 zeigt einige Beispiele für solche Funktionen.

| Aktion | Transaktion | Funktionsbaustein |
|---|---|---|
| Sachkontenbeleg buchen | FB50 | BAPI_ACC_GL_POSTING_POST |
| Buchhaltungsbeleg buchen | FB01 | BAPI_ACC_DOCUMENT_POST |

**Tabelle 5.1** Beispiele für Funktionsbausteine

| Aktion | Transaktion | Funktionsbaustein |
|---|---|---|
| Bestellung buchen | ME21N | BAPI_ACC_PURCHASE_ORDER_POST |
| Warenbewegung buchen | MIGO | BAPI_ACC_GOODS_MOVEMENT_POST |
| Kundenauftrag buchen | VA01 | BAPI_ACC_SALES_ORDER_POST |
| Faktura buchen | VF01 | BAPI_ACC_BILLING_POST |
| Benutzer anlegen/ändern | SU01 | BAPI_USER_CREATE1<br>BAPI_USER_CHANGE |
| RFC-Verbindungen pflegen | SM59 | RFC_MODIFY_R3_DESTINATION |
| Funktionsbausteine anlegen | SE37 | RS_FUNCTIONMODULE_INSERT |
| Tabelleninhalte anzeigen | SE16 | RFC_READ_TABLE |

**Tabelle 5.1** Beispiele für Funktionsbausteine (Forts.)

Funktionsbausteine werden mit Transaktion SE37 ausgeführt. Um die Eigenschaften eines Funktionsbausteins einzusehen, tragen Sie in der Einstiegsmaske der Transaktion den Namen eines Funktionsbausteins ein, z. B. »RFC_READ_TABLE«. Wählen Sie die Schaltfläche **Anzeigen** (siehe Abbildung 5.1).

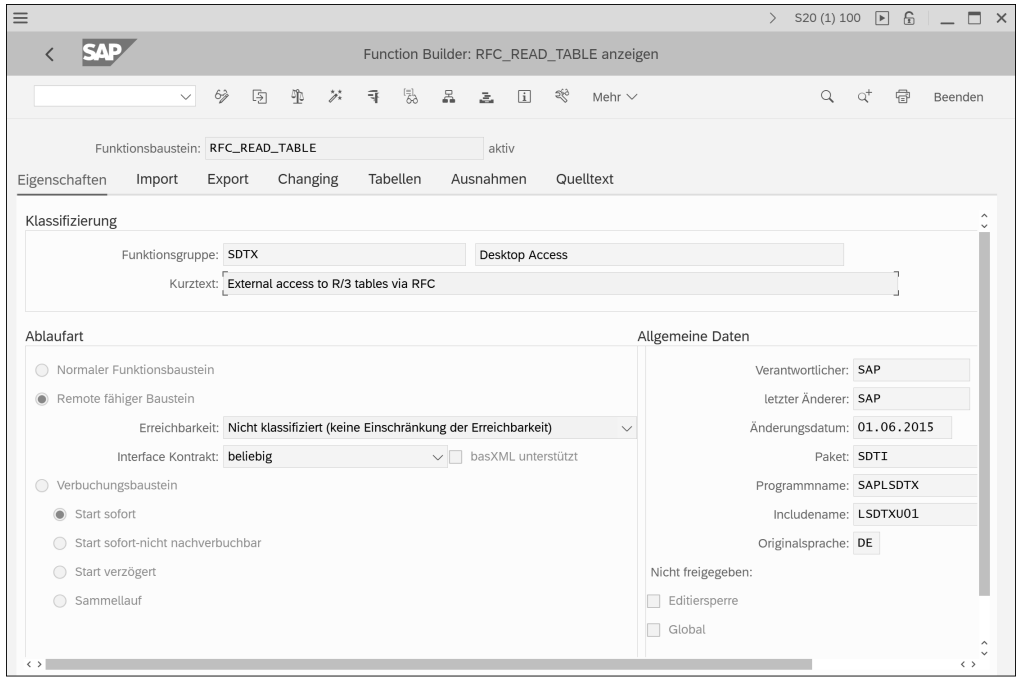


**Abbildung 5.1** Eigenschaften eines Funktionsbausteins





Tabelle 5.2 zeigt die Eigenschaften eines Funktionsbausteins, die in Transaktion SE37 auf verschiedenen Registerkarten angezeigt werden.

| Registerkarte | Eigenschaft |
|---|---|
| **Eigenschaften** | ■ **Funktionsgruppe**<br>Die Funktionsgruppe wird zur Vergabe einer Berechtigung für den Funktionsbaustein genutzt.<br>■ **Ablaufart**<br>Die Eigenschaft **Remote fähiger Baustein** zeigt an, dass der Funktionsbaustein von anderen Systemen aus aufgerufen werden kann. |
| **Import** | Die meisten Funktionsbausteine haben eine Selektionsmaske, ähnlich wie Reports. Hier sind die Felder der Selektionsmaske aufgeführt. Beim Aufruf durch ein Programm müssen sie als Übergabeparameter mitübergeben werden. |
| **Export** | Hier sind die Rückgabeparameter des Funktionsbausteins angegeben. Dies sind die Daten, die nach dem Ausführen des Funktionsbausteins ausgegeben werden. |
| **Changing** | Dies sind Übergabeparameter, die sowohl als Import- als auch als Exportparameter fungieren. Es wird ein Wert an den Funktionsbaustein übergeben, der zur Laufzeit geändert und zurückgegeben werden kann. |
| **Tabellen** | Die Ergebnisse von Funktionsbausteinen werden häufig in Tabellenstrukturen zurückgegeben. |
| **Ausnahmen** | Listet die Fehlermeldung auf, die der Funktionsbaustein beim Auftreten von Fehlern zurückgibt. |
| **Quelltext** | der Quelltext des Funktionsbausteins |

**Tabelle 5.2** Eigenschaften eines Funktionsbausteins

Zum Ausführen des Funktionsbausteins drücken Sie die Funktionstaste F8. Abbildung 5.2 zeigt das Ausführen des Funktionsbausteins. In den Importparametern müssen Sie die Selektionskriterien angeben. Hier soll mit dem Funktionsbaustein RFC_READ_TABLE Tabelle TIBAN (IBAN-Nummern) angezeigt werden. Die Rückgabewerte werden hier in Tabelle DATA ausgegeben. Klicken Sie auf den Namen der Tabelle, werden Ihnen die Datensätze von Tabelle TIBAN angezeigt.

Um die remotefähigen Funktionsbausteine zu ermitteln, können Sie Tabelle TFDIR nutzen. Im Feld FMODE (**Modus**) wird die Art des Funktionsbausteins gespeichert. Der Wert »R« steht für Remote.

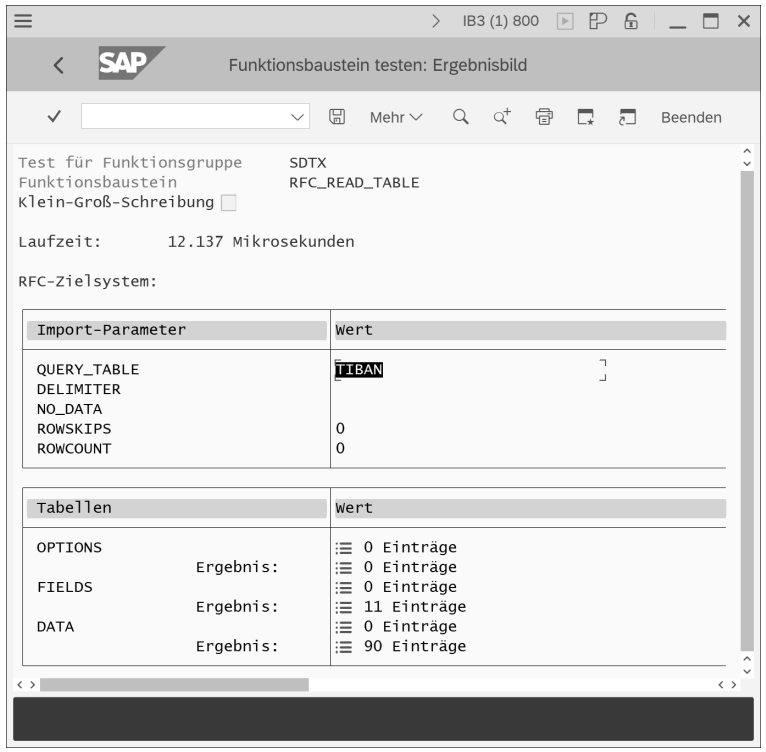


**Abbildung 5.2** Ausführen eines Funktionsbausteins

Zum Prüfen der Berechtigungen zum Ausführen von Funktionsbausteinen ist die Zuordnung zur Funktionsgruppe relevant, da Berechtigungen für diese Gruppen vergeben werden können. Die Zuordnung der Funktionsbausteine zu den Funktionsgruppen wird in Tabelle `ENLFDIR` gespeichert. Das Feld `AREA` enthält hier die Funktionsgruppen.

### 5.1.1 Funktionsbausteine ohne Berechtigungsprüfungen

Eine Vielzahl von Funktionsbausteinen ermöglicht eine Ausführung explizit ohne Berechtigungsprüfung. Viele dieser Bausteine haben einen Importparameter (siehe Tabelle 5.2), mit dem die Berechtigungsprüfung bei der Ausführung deaktiviert werden kann (z. B. `AUTHORITY_CHECK`). Somit ist es möglich, Aktionen ohne die erforderlichen Berechtigungen auszuführen. Daher sind Berechtigungen zum Ausführen von Funktionsbausteinen als sehr kritisch anzusehen. Abbildung 5.3 zeigt als Beispiel den Funktionsbaustein `RFC_MODIFY_R3_DESTINATION`, mit dem RFC-Verbindungen angelegt und gepflegt werden können. Durch das Leerlassen des Übergabeparameters `AUTHORITY_CHECK` wird die Berechtigungsprüfung deaktiviert. Somit können z. B. RFC-Verbindungen ohne die erforderliche Berechtigung angelegt werden.







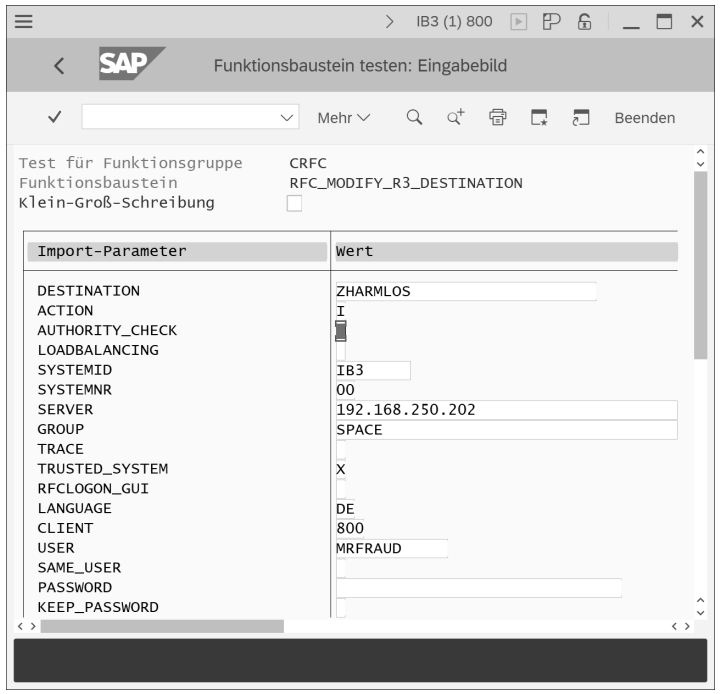


**Abbildung 5.3** Berechtigungsprüfung deaktivieren

Einen groben Überblick über die Anzahl der Funktionsbausteine, in denen Berechtigungsprüfungen deaktiviert werden können, gibt Tabelle `FUPARAREF` (Parameter von Funktionsbausteinen). In dieser Tabelle werden u. a. die Importparameter der Funktionsbausteine gespeichert. Es existieren ca. 1.100 Funktionsbausteine, in denen Berechtigungsprüfungen deaktiviert werden können. Diese Funktionsbausteine können Sie über die folgende Selektion in der Tabelle ermitteln:

- `PARAMTYPE: I` (= Importparameter)
- `PARAMETER: *AUTHORITY*`

### 5.1.2 Funktionsbausteine mit schaltbaren Berechtigungen

Mit schaltbaren Berechtigungen (siehe Abschnitt 9.5.3, »Gefahrenpunkte in der ABAP-Programmentwicklung«) können Berechtigungsprüfungen in Funktionsbausteinen aktiviert werden, die standardmäßig deaktiviert sind. Hierzu hat SAP mehr als 50 SAP-Hinweise ausgegeben. Der Sammelhinweis 2078596 listet diese Hinweise auf. Betroffen sind Funktionsbausteine aus allen SAP-Komponenten und -Systemen. Einige Beispiele für Funktionsbausteine, die standardmäßig ungeschützt sind und durch schaltbare Berechtigungen geschützt werden können, zeigt Tabelle 5.3.

| Funktionsbaustein | Bezeichnung |
|---|---|
| BAPI_ACC_BILLING_POST | Rechnungswesen: Faktura buchen |
| BAPI_ACC_EMPLOYEE_EXP_POST | Rechnungswesen: HR-Buchung, Kontierung Hauptbuch buchen |
| BAPI_ACC_EMPLOYEE_PAY_POST | Rechnungswesen: HR-Buchung, Kontierung Kreditor buchen |
| BAPI_ACC_EMPLOYEE_REC_POST | Rechnungswesen: HR-Buchung, Kontierung Debitor buchen |
| BAPI_ACC_GL_POSTING_POST | Rechnungswesen: allgemeine Sachkontenbuchung |
| BAPI_ACC_GOODS_MOVEMENT_POST | Rechnungswesen: Warenbewegung buchen |
| BAPI_ACC_INVOICE_RECEIPT_POST | Rechnungswesen: Rechnungseingang buchen |
| BAPI_ACC_DOCUMENT_POST | Rechnungswesen: Buchung |
| BAPI_ACC_DOCUMENT_REV_POST | Rechnungswesen: Storno buchen |
| BAPI_IBAN_CHANGE | IBAN ändern |
| BAPI_IBAN_CREATE | IBAN anlegen |

**Tabelle 5.3** Beispiele für Funktionsbausteine mit schaltbaren Berechtigungen

Sind im SAP-System Prozesse abgebildet, zu denen Funktionsbausteine ohne bzw. mit nicht ausreichenden Berechtigungsprüfungen existieren, sollten hierfür die schaltbaren Berechtigungsprüfungen genutzt werden. Über sogenannte *Szenarien*, die mit den SAP-Hinweisen heruntergeladen werden können, werden die schaltbaren Berechtigungsprüfungen aktiviert. Die Pflege und Aktivierung der Szenarien erfolgt mittels Transaktion SACF. Abbildung 5.4 zeigt das Szenario FI_DOC_POST, mit dem in Funktionsbausteinen für FI-Belegbuchungen die angezeigten Berechtigungsobjekte aktiviert werden können, z. B. für den Baustein BAPI_ACC_DOCUMENT_POST.

Welche Szenarien aktiviert sind, können Sie in Tabelle TOBJ_CHK_CTRL_R einsehen. Einen Überblick über alle im System vorhandenen Szenarien gibt Transaktion SACF_INFO.

**Weitere Informationen zur Absicherung von RFC-Aufrufen**

Aufgrund der Kritikalität hat SAP ein Whitepaper zur Absicherung von RFC-Aufrufen veröffentlicht. Das Whitepaper ist als Anhang zu SAP-Hinweis 2008727 (Sichere RFC-Aufrufe (Remote Function Calls)) hinterlegt. Alternativ können Sie das Dokument über die URL *https://service.sap.com/securitywp* herunterladen.





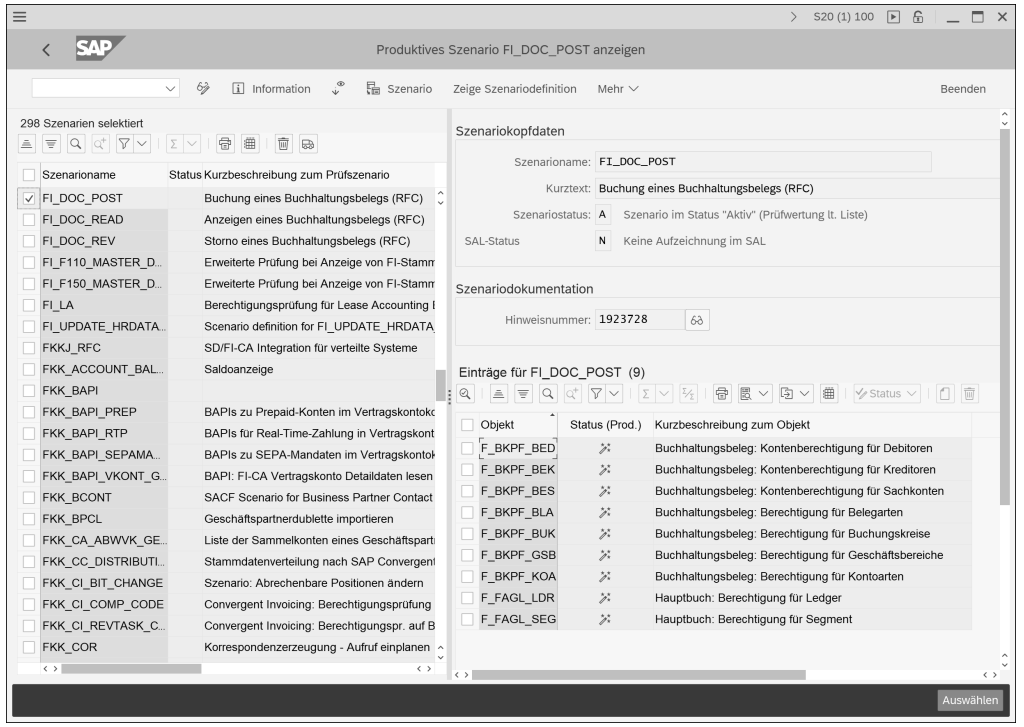


**Abbildung 5.4** Szenario FI_DOC_POST

### 5.1.3 Protokollierung von RFC-Aktionen

Standardmäßig werden Anmeldungen per RFC und das Ausführen von Funktionsbausteinen nicht protokolliert. Allerdings werden die Zugriffe über die Zugriffsstatistik protokolliert. Da dies kein ständiges Protokoll ist, müssen Auswertungen hier zeitnah erfolgen, z. B. mit Transaktion STRFCTRACE.

Informationen zu den Auswertungen der Zugriffsstatistik zu RFC-Aktionen finden Sie in Abschnitt 4.7.3, »Analyse von RFC-Zugriffen«. Des Weiteren können Sie die in den folgenden Abschnitten beschriebenen Protokollkomponenten aktivieren, die noch detailliertere Informationen zu den RFC-Aktionen liefern.

#### Protokollierung mit dem Security-Audit-Log

Mit dem Security-Audit-Log (SAL) können verschiedene RFC-Aktionen protokolliert werden (siehe Tabelle 5.4). Weitere Informationen zum SAL finden Sie in Abschnitt 4.1, »Security-Audit-Log«.

| Meldungs-ID | Meldungstext |
|---|---|
| AU5 | RFC-/CPI-C-Login erfolgreich (Typ = &A, Methode = &C) |
| AU6 | RFC-/CPI-C-Login gescheitert, Grund = &B, Typ = &A, Methode = &C. |
| AUK | Erfolgter RFC-Aufruf &C (FuGr = &A) |
| AUL | Gescheiterter RFC-Aufruf &C (FuGr = &A)) |
| CUZ | Generischer Tabellenzugriff per RFC auf &A mit Aktivität &B |
| DU1 | FTP-Server-Whitelist ist leer. |
| DU2 | FTP-Server-Whitelist ist durch Verwendung von Platzhaltern unsicher. |
| DU3 | Server &A ist nicht in der Whitelist enthalten! |
| DU4 | Verbindung zu Server &A ist fehlgeschlagen. |
| DU8 | FTP-Konnektierungsanfrage für Server &A erfolgt. |
| DUI | RFC-Callback ausgeführt (Destination &A, gerufen &B, Callback &C). |
| DUJ | RFC-Callback abgewiesen (Destination &A, gerufen &B, Callback &C). |
| DUK | RFC-Callback im Simulationsmodus (Destination &A, grufen &B, Callback &C) |
| DUR | JSON-RPC-Aufruf des Funktionsbausteins &A erfolgreich. |
| DUS | JSON-RPC-Aufruf des Funktionsbausteins &A fehlgeschlagen. |
| DUT | Kritischer JSON-RPC-Aufruf des Funktionsbausteins &A (S_RFC *-Berechtigung) |
| EUE | Erfolgreicher Aufruf des RFC-Funktionsbausteins &A |
| EUF | Aufruf des RFC-Funktionsbausteins &A fehlgeschlagen. |
| EUG | Benutzer hat keine Berechtigung, um RFC-Funktionsbaustein &A auszuführen. |
| EUI | Setup der UCON-HTTP-Whitelist wurde verändert. |
| EUJ | Phase der UCON-HTTP-Whitelist des Kontexttyps &A wurde geändert. |
| EUK | Zugriff auf die UCON-HTTP-Whitelist des Kontexttyps &A wurde abgewiesen. |
| EUL | HTTP Security Header Register wurde für Header &A geändert. |

**Tabelle 5.4** Protokollierte RFC-Aktionen im SAL





| Meldungs-ID | Meldungstext |
|---|---|
| EUM | Trusted Site List &A für HTTP Security Header wurde geändert. |
| EUN | Content Security Policy für Service &A wurde verletzt. |
| EUO | UCON-HTTP-Whitelist des Kontexttyps &A wurde geändert. |
| FU1 | In Programm &A wurde RFC-Funktion &B mit dynamischer Destination &C aufgerufen. |

**Tabelle 5.4** Protokollierte RFC-Aktionen im SAL (Forts.)



#### Protokollierung mit der Lesezugriffsprotokollierung

Mit der Lesezugriffsprotokollierung (Read Access Logging) kann der Aufruf von Funktionsbausteinen detailliert protokolliert werden. So wird nicht nur aufgezeichnet, welche Funktionsbausteine wann von wem aufgerufen wurden, sondern auch detailliert die Selektionsparameter, mit denen der Aufruf erfolgte. Weitere Informationen zur Lesezugriffsprotokollierung finden Sie in Abschnitt 4.6, »Lesezugriffsprotokollierung«.

### 5.1.4 Patterns in SAP Enterprise Threat Detection

Zur Überwachung des Ausführens von Funktionsbausteinen stellt SAP Enterprise Threat Detection die folgenden Standard-Patterns zur Verfügung:

- Blacklisted function modules
- DoS attack against different RFC destinations
- DoS attack via RFC_PING/RFCPING to one destination
- ABAP SOAP rfc brute force login
- ABAP function modules with removed RFC enablement
- Access to critical database tables via RFC
- Calls from a non-productive to a productive system
- ABAP deactivated or deleted function modules
- RFC calls from non-productive to productive systems
- ABAP critical FM calls per SOAP rfc
- Failed logon by RFC/CPIC call
- Service Calls by Dialog User
- Service Calls by Technical User
- New Service Calls by Technical Users

Die Patterns basieren teilweise auf vordefinierten Wertelisten (Value Lists), in denen kritische Funktionsbausteine bereits vorgegeben sind. Tabelle 5.5 zeigt einen Ausschnitt.

| ValueList | Funktionsbausteine (Auszug) |
|---|---|
| ABAPBlacklistedFunctionModules | ■ BAPI_USER_CREATE<br>■ BAPI_USER_CREATE1<br>■ BAPI_USER_DELETE<br>■ BAPI_USER_PROFILES_ASSIGN<br>■ PRGN_INTERFACE_USER<br>■ RFC_ABAP_INSTALL_AND_RUN<br>■ RFC_GET_TABLE_ENTRIES<br>■ RFC_READ_TABLE<br>■ RS_FUNCTIONMODULE_INSERT<br>■ SUSR_RFC_USER_INTERFACE<br>■ SXPG_CALL_SYSTEM<br>■ SXPG_COMMAND_EXECUTE<br>■ SXPG_COMMAND_EXECUTE_LONG<br>■ TABLE_ENTRIES_GET_VIA_RFC<br>■ TH_REMOTE_TRANSACTION |
| ABAPBlacklistedSOAPRFCFMs | ■ SXPG_COMMAND_EXECUTE<br>■ SXPG_CALL_SYSTEM<br>■ RFC_SYSTEM_INFO<br>■ BAPI_USER_CREATE1<br>■ RFC_READ_TABLE |
| ■ ABAPDeactivatedDeletedFMs<br>■ AndReports/ABAPFunction-ModulesRFC<br>■ EnablementRemoved | deaktivierte/gelöschte Funktionsbausteine aufgrund von Sicherheitshinweisen |

**Tabelle 5.5** Value Lists mit kritischen Funktionsbausteinen

### 5.1.5 Zugriffsrechte

Die folgenden Tabellen zeigen Ihnen die Berechtigungen zu Funktionsbausteinen. Tabelle 5.6 zeigt die Berechtigung zum Ausführen einzelner Funktionsbausteine.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_TCODE | TCD<br>(Transaktion) | SE37 oder SE80 oder Report<br>RS_TESTFRAME_CALL |

**Tabelle 5.6** Berechtigung zum Ausführen von Funktionsbausteinen





| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_DEVELOP | ACTVT<br>(Aktivität) | 16 (Ausführen) |
| | OBJTYPE<br>(Objekttyp) | FUGR (Funktionsgruppe) |
| | OBJNAME<br>(Objektname) | Name der Funktionsgruppe |
| | DEVCLASS<br>(Paket) | Paket der Funktionsgruppe |

**Tabelle 5.6** Berechtigung zum Ausführen von Funktionsbausteinen (Forts.)

Tabelle 5.7 zeigt die Berechtigung zum Ausführen aller Funktionsbausteine.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_TCODE | TCD<br>(Transaktion) | SE37 oder SE80 oder Report<br>RS_TESTFRAME_CALL |
| S_DEVELOP | ACTVT<br>(Aktivität) | 16 (Ausführen) |
| | OBJTYPE<br>(Objekttyp) | FUGR (Funktionsgruppe) |
| | OBJNAME<br>(Objektname) | * |
| | DEVCLASS<br>(Paket) | * |
| | P_GROUP<br>(Berechtigungsgruppe) | * |

**Tabelle 5.7** Berechtigung zum Ausführen aller Funktionsbausteine

### 5.1.6 Checkliste

In Tabelle 5.8 finden Sie die Checkliste mit den prüfungsrelevanten Fragestellungen zur Absicherung von Funktionsbausteinen.

| Risiko | Fragestellung<br>Vorgabe oder Erläuterung |
|---|---|
| 2 | Werden Anmeldungen und Funktionsbausteinaufrufe über RFC protokolliert? |
| | RFC-Falschanmeldungen und fehlgeschlagene Funktionsbausteinaufrufe sind zu protokollieren.<br>Hier besteht das Risiko, dass Funktionsbausteine ohne Nachvollziehbarkeit von externen Programmen ausgeführt werden können und dass Eindringversuche über RFC unbemerkt bleiben. |
| 1 | Wer besitzt das Recht zum Ausführen aller Funktionsbausteine? |
| | Dieses Zugriffsrecht ist für keinen Benutzer erforderlich.<br>Hier besteht das Risiko, dass Benutzer über die Funktionsbausteine kritische Aktionen im SAP-System durchführen können. |
| 1 | Wer besitzt das Recht, mit Transaktion SE37 Funktionsbausteine auszuführen? |
| | Dieses Zugriffsrecht sollte nur wenigen administrativen Benutzern zugeordnet werden.<br>Hier besteht das Risiko, dass Benutzer über RFC-Verbindungen mit hinterlegtem Benutzer und Kennwort unberechtigten Zugriff auf andere SAP-Systeme erlangen. |

**Tabelle 5.8** Checkliste zu Funktionsbausteinen

Wie Sie die einzelnen Punkte praktisch am SAP-System prüfen können, erfahren Sie in Abschnitt 5.1 des Dokuments **Tiede_Checklisten_Sicherheit_und_Pruefung.pdf**, das Sie im Downloadbereich zu diesem Buch unter *www.sap-press.de/5145* finden.

## 5.2 RFC-Verbindungen

*RFC-Verbindungen* sind im SAP-System hinterlegte Verbindungsdaten zu SAP-Systemen oder Fremdsystemen. Standardmäßig sind bereits einige RFC-Verbindungen im System vorhanden, u. a. die erforderlichen Verbindungen für das Transport Management System (TMS) sowie zu allen Applikationsservern des SAP-Systems. Allerdings ist es erforderlich, weitere RFC-Verbindungen anzulegen, z. B. zum Datenaustausch mit anderen Systemen oder für Mandantenkopien aus einem anderen System.

Verwaltet werden die RFC-Verbindungen mit Transaktion SM59, deren Oberfläche Sie in Abbildung 5.5 sehen. Hier werden die Eigenschaften der RFC-Verbindungen festgelegt. Für Verbindungen zu SAP-Systemen wird der Mandant des Zielsystems angegeben sowie (wahlweise) ein Benutzer aus dem Mandanten und sein Kennwort.







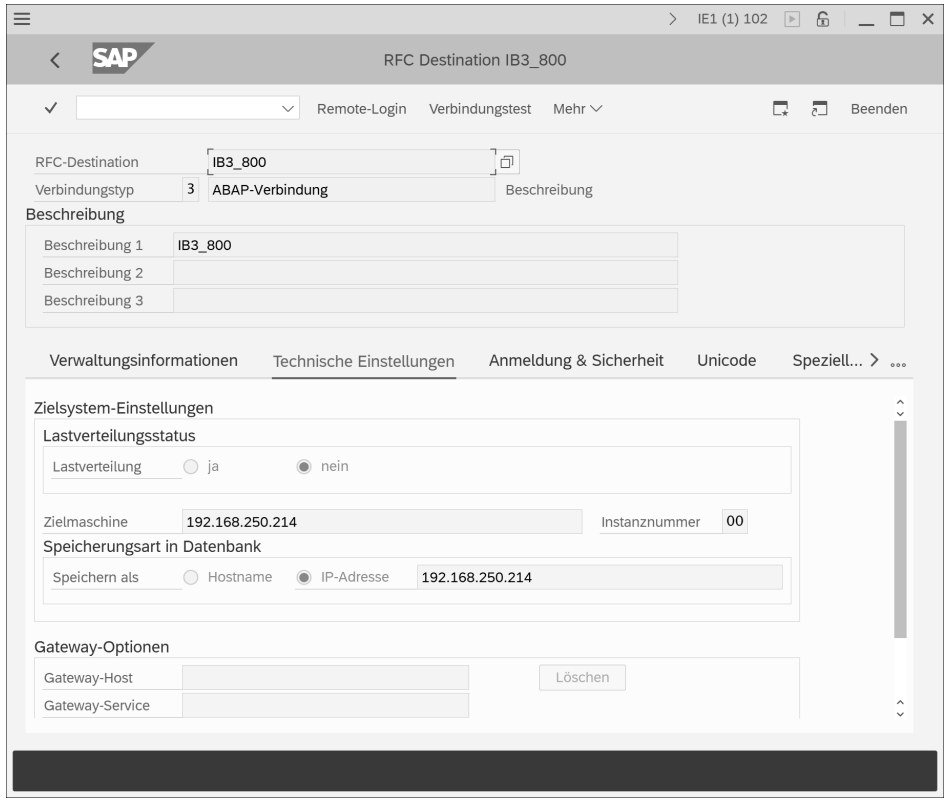


**Abbildung 5.5** Transaktion SM59 – RFC-Verbindungen pflegen

Gespeichert werden die RFC-Verbindungen in Tabelle `RFCDES`. Eine Übersicht über alle RFC-Verbindungen bieten auch die Transaktionen/Reports `RSRSDEST` (Anzeige aller RFC-Verbindungen) und `RSRFCCHK` (Anzeige aller RFC-Verbindungen mit Anmeldedaten). Im Zuge einer Systemprüfung sollten Sie überprüfen, welche RFC-Verbindungen existieren und wozu sie genutzt werden.

Über Berechtigungen kann gesteuert werden, welche Benutzer welche RFC-Verbindungen nutzen dürfen. Hierzu kann in den Eigenschaften der RFC-Verbindungen im Feld **Berechtigung für Destination** ein beliebiger Wert angegeben werden (siehe Abbildung 5.6). Benutzer, die diese RFC-Verbindung nutzen wollen, benötigen dann eine Berechtigung für das Berechtigungsobjekt `S_ICF`. Das Objekt besteht aus den folgenden beiden Feldern:

- Bereich: Hier muss der Wert »DEST« (für RFC-Destinationen) eingetragen sein.
- Wert: Hier muss der Wert aus dem Feld **Berechtigung** der RFC-Verbindung eingetragen sein, für die der Benutzer eine Berechtigung erhalten soll.

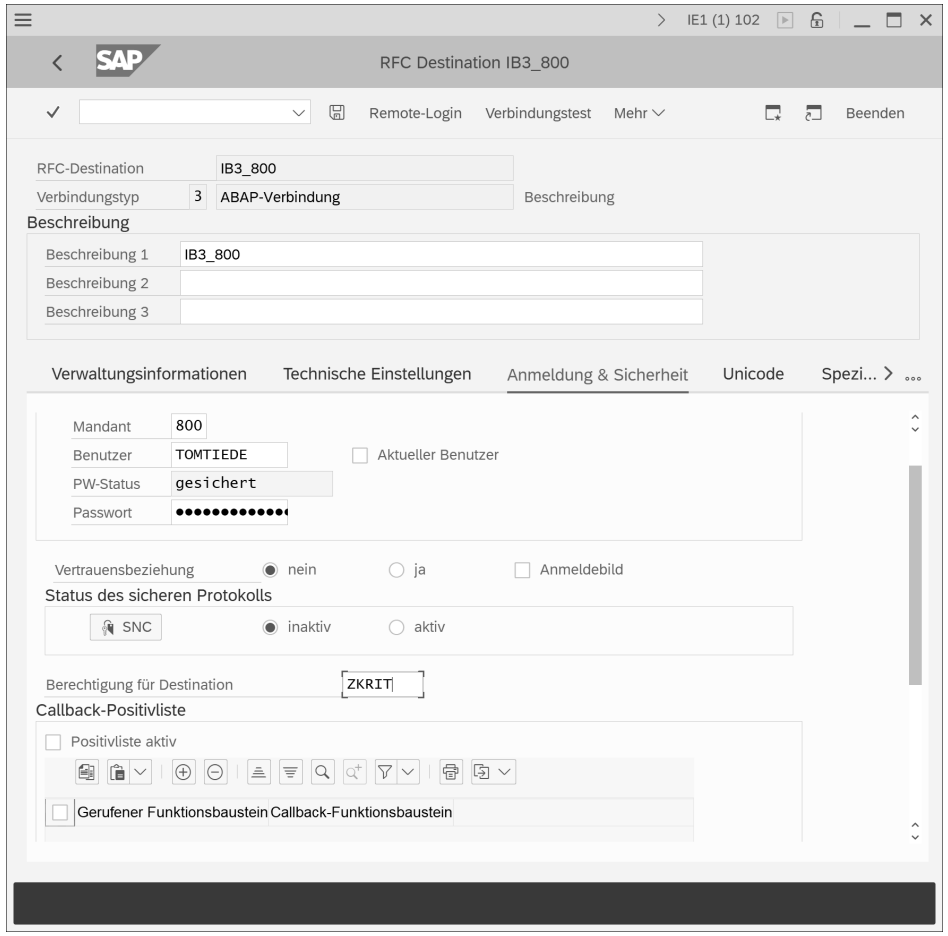


**Abbildung 5.6** RFC-Verbindung durch einen Berechtigungswert schützen

Um die in Abbildung 5.6 dargestellte RFC-Verbindung auszuführen, benötigt ein Benutzer beispielsweise die in Tabelle 5.9 beschriebene Berechtigung.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_ICF | ICF_FIELD (ICF-Typ) | DEST |
| | ICF_VALUE (ICF-Wert) | ZKRIT |

**Tabelle 5.9** Beispielberechtigung zum Ausführen einer RFC-Verbindung







### 5.2.1 Hinterlegte Kennwörter

Besonders kritisch ist es, wenn zu RFC-Verbindungen Dialog- oder Servicebenutzer und Kennwörter hinterlegt werden. Solch eine Verbindung kann dann dazu genutzt werden, eine Verbindung ohne Anmeldung aufzubauen. RFC-Verbindungen mit hinterlegten Kennwörtern für Dialog- oder Servicebenutzer sollten nicht existieren. Es dürfen ausschließlich Kommunikations- oder Systembenutzer benutzt werden. Des Weiteren müssen die Berechtigungen der hinterlegten Benutzer auf das erforderliche Minimum reduziert werden. Eine Zuordnung des Profils SAP_ALL oder ähnlicher Rechte darf nicht erfolgen.

Die verschlüsselten Kennwörter der RFC-Verbindungen werden in den Tabellen RSECACTB und RSECTAB (*sicherer Speicher*) gespeichert. Den Inhalt dieser Tabellen können Sie mit den Standard-Tabellenanzeigetransaktionen nicht anzeigen. Zur Anzeige kann z. B. der SQL-Editor des DBA Cockpits genutzt werden (siehe Abschnitt 1.12.1, »Zugriff auf SAP HANA über das DBA Cockpit«). Das Kennwort wird hier verschlüsselt in einem Clusterfeld abgelegt. Dass ein Kennwort hinterlegt ist, können Sie über Tabelle RFCDES prüfen. Der Eintrag »v=%_PWD« im Feld RFCOPTIONS (**Optionen**) zeigt an, dass ein Kennwort hinterlegt ist (siehe Abbildung 5.7).

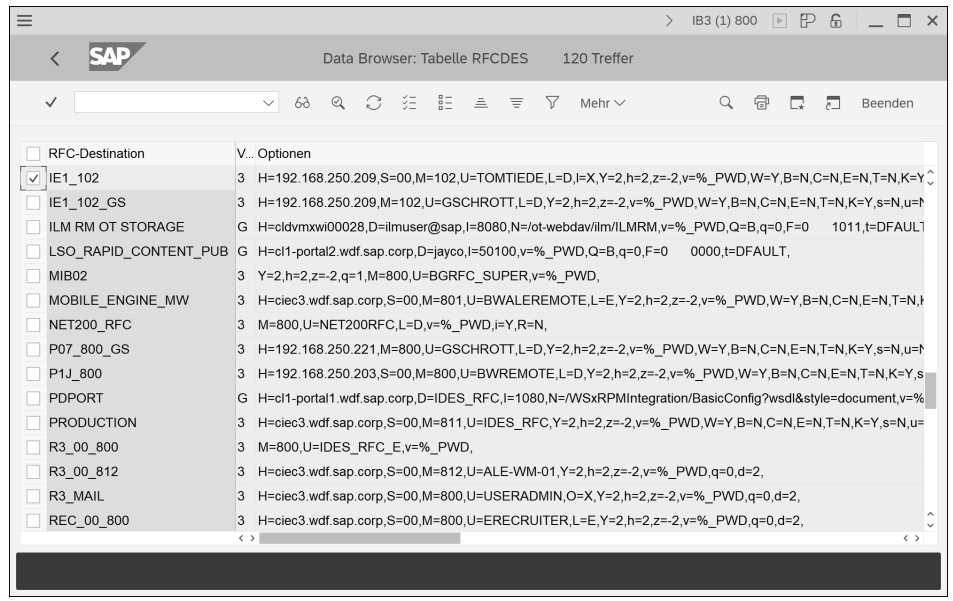


**Abbildung 5.7** RFC-Verbindungen mit hinterlegten Kennwörtern

Die weiteren Einträge im Feld RFCOPTIONS im markierten Datensatz in der Abbildung bedeuten:

- Server (H): 192.168.250.209
- Instanznummer (S): 00

- Mandant (M): 102
- Benutzer (U): TOMTIEDE

Bei einer Prüfung müssen Sie im jeweiligen Mandanten des Zielsystems kontrollieren, um welchen Benutzertyp es sich bei dem hinterlegten Benutzer handelt. In unserem Beispiel muss eine Anmeldung am Mandanten 102 in dem System erfolgen, das über die IP-Adresse 192.168.250.209, Instanz 00, erreichbar ist. Ist Ihnen nicht bekannt, um welches System es sich dabei handelt, können Sie dies bei der Administration erfragen.

In dem Mandanten prüfen Sie über Transaktion SU01 oder SU01D (Registerkarte **Logon-Daten**), welchen Benutzertyp der hinterlegte Benutzer hat. Zulässig sind Kommunikations- und Systembenutzer. Dialog- oder Servicebenutzer dürfen nicht hinterlegt sein.

Alternativ können Sie auch Transaktion/Report RSRFCCHK nutzen, der alle RFC-Verbindungen mit den hinterlegten Anmeldedaten anzeigt. Bei hinterlegtem Kennwort wird im Feld **Passwort** der Wert »Password saved« angezeigt. Um diesen Report auszuführen, benötigen Sie die Berechtigung zur Netzwerkadministration (Berechtigungsobjekt S_ADMI_FCD, Wert NADM). Lesende Berechtigungen sind nicht ausreichend.

### 5.2.2 Systemübergreifender Zugriff über Funktionsbausteine

Eine kritische und häufig unterschätzte Berechtigung ist das Ausführen von Transaktion SE37 (Ausführen von Funktionsbausteinen). Problematisch ist hier, dass zu allen remotefähigen Funktionsbausteinen eine RFC-Verbindung angegeben werden kann, über die dann der entsprechende Funktionsbaustein in einem anderen System ausgeführt wird. Sind Systeme miteinander über RFC verbunden, sind in den meisten Fällen in den Systemen RFC-Verbindungen fest eingerichtet, in denen Kommunikationsbenutzer mit Kennwort und meist sehr umfangreichen Rechten (häufig noch die des Profils SAP_ALL) hinterlegt sind. Bei der Nutzung solch einer RFC-Verbindung können im anderen System beliebige Funktionsbausteine ausgeführt werden, da Benutzer und Kennwort bereits in der RFC-Verbindung hinterlegt sind (zum Remoteausführen von Funktionsbausteinen reicht ein Kommunikationsbenutzer).

Abbildung 5.8 zeigt das Ausführen eines Funktionsbausteins im System IE1, Mandant 102, mit der RFC-Verbindung IB3_800. Diese Verbindung enthält die Verbindungsdaten zum SAP-System IB3, Mandant 800. Ausgelesen wird Tabelle PA0009 (Bankverbindungen der Mitarbeiter in SAP ERP HCM). Hinterlegt ist in der RFC-Verbindung der Benutzer TOMTIEDE, inklusive Kennwort. Da dieser im System IB3, Mandant 800, die entsprechenden Berechtigungen zum Anzeigen aller Tabellen besitzt, wird Tabelle PA0009 angezeigt. Hierüber können somit vom System IE1 aus alle HCM-Daten (sowie auch alle anderen Daten) aus dem System IB3 ausgelesen werden.







Zur Absicherung dieses Vorgangs sollten die Kommunikationsbenutzer, die in RFC-Verbindungen genutzt werden, nicht über das Berechtigungsprofil SAP_ALL oder ähnliche Berechtigungen verfügen. Ihnen dürfen nur die tatsächlich erforderlichen Berechtigungen zugeordnet werden. Da Berechtigungen für Schnittstellenbenutzer aufwendig einzurichten sind, bietet u. a. SAP Consulting hierzu Beratungsleistungen an. Diese sind in SAP-Hinweis 1682316 (SAP Consulting: Optimierung von RFC-Benutzerberechtigungen) beschrieben. SAP Consulting nutzt hierzu den *Xiting Role Builder* aus der Xiting Authorization Management Suite (XAMS).

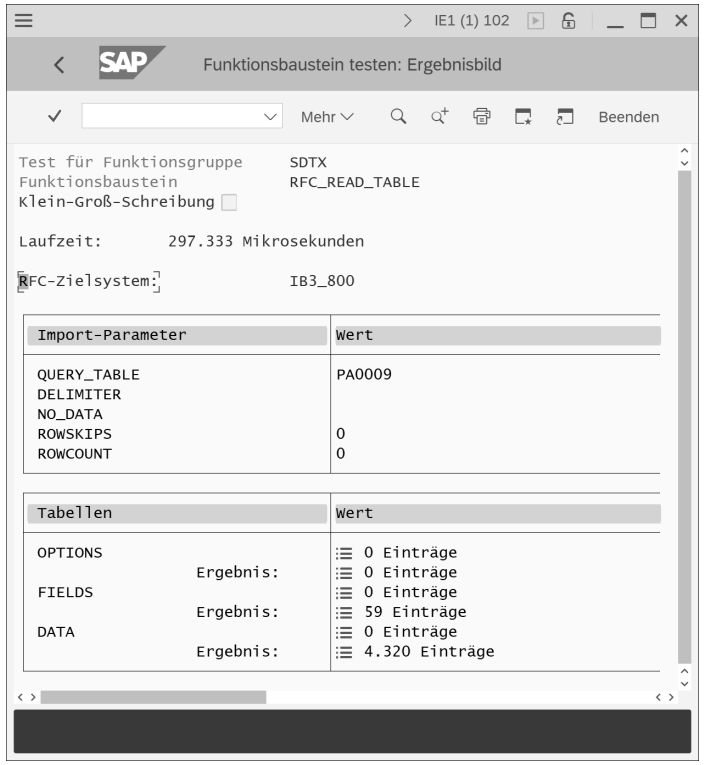


**Abbildung 5.8** Funktionsbaustein in einem anderen System ausführen

Eine weitere Möglichkeit des Schutzes bietet der Langzeit-Trace für Berechtigungen (Transaktion STUSERTRACE bzw. Report RSUSR_SUAUTHVALTRC_DISPLAY). Hierüber ist es möglich, die Berechtigungen von mehreren Benutzern (Anzahl ist konfigurierbar) protokollieren zu lassen. Da die Trace-Daten redundanzfrei in einer Tabelle gespeichert werden, kann der Trace auch für einen längeren Zeitraum aktiviert werden. Aus den Trace-Informationen können dann Rollen erzeugt werden. Weitere Informationen zum Langzeit-Trace finden Sie in Abschnitt 10.6.3, »Der Benutzer-Langzeit-Trace«.

### 5.2.3 Zugriffsrechte

Die folgenden Tabellen zeigen Ihnen die Berechtigungen zu RFC-Verbindungen. Tabelle 5.10 zeigt die Berechtigung zum Verwalten von RFC-Verbindungen.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_TCODE | TCD (Transaktion) | SM59 |
| S_RFC_ADM | ACTVT (Aktivität) | ■ 01 (Anlegen)<br>■ 02 (Ändern)<br>■ 06 (Löschen) |
| | RFCTYPE (Verbindungstyp) | 3 (Verbindung zu einem ABAP-System) |
| | RFCDEST (Name einer RFC-Verbindung) | <Name einer RFC-Verbindung> |
| | ICF_VALUE (ICF-Wert) | <Berechtigungswert> |

**Tabelle 5.10** Berechtigung zum Verwalten von RFC-Verbindungen

Tabelle 5.11 zeigt die Berechtigung zum Aufrufen von RFC-Verbindungen.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_ICF | ICF_FIELD (ICF-Typ) | DEST |
| | ICF_VALUE (ICF-Wert) | * |

**Tabelle 5.11** Berechtigung zum Nutzen aller RFC-Verbindungen bei vergebenen Berechtigungsgruppen

### 5.2.4 Checkliste

In Tabelle 5.12 finden Sie die Checkliste mit den prüfungsrelevanten Fragestellungen zur Absicherung von RFC-Verbindungen.

| Risiko | Fragestellung |
|---|---|
| | Vorgabe oder Erläuterung |
| 1 | Welche RFC-Verbindungen existieren in den verschiedenen Systemen der SAP-Systemlandschaft? |

**Tabelle 5.12** Checkliste zu RFC-Verbindungen





| Risiko | Fragestellung |
|---|---|
| | Vorgabe oder Erläuterung |
| 1 | In allen Systemen der Systemlandschaft dürfen nur RFC-Verbindungen existieren, die notwendig sind und genutzt werden.<br>Hier besteht das Risiko, dass durch RFC-Verbindungen Schnittstellen zu Systemen aufgebaut werden können, die nicht mit dem SAP-System verbunden sein sollten. |
| 2 | Sind die eingerichteten RFC-Verbindungen dokumentiert (außerhalb des SAP-Systems)? |
| | Jede RFC-Verbindung muss so dokumentiert sein, dass ihr Verwendungszweck eindeutig nachvollziehbar ist.<br>Hier besteht das Risiko, dass RFC-Verbindungen aufgrund einer fehlenden Dokumentation falsch genutzt werden. |
| 1 | Existieren RFC-Verbindungen, in denen für Dialog- oder Servicebenutzer Kennwörter hinterlegt sind? |
| | RFC-Verbindungen mit hinterlegten Kennwörtern für Dialogbenutzer dürfen nicht existieren.<br>Hier besteht das Risiko, dass durch diese RFC-Verbindungen eine Anmeldung ohne Benutzerkennung und Kennwort möglich ist. |
| 2 | Wer ist berechtigt, RFC-Verbindungen zu pflegen? |
| | Dieses Zugriffsrecht dürfen nur Basisadministratoren besitzen.<br>Hier besteht das Risiko, dass unberechtigte Benutzer RFC-Verbindungen ändern, neue anlegen oder vorhandene löschen. |
| 2 | Wer besitzt das Recht, alle RFC-Verbindungen zu nutzen? |
| | Dieses Zugriffsrecht sollten nur Administratoren besitzen.<br>Hier besteht das Risiko, dass Benutzer zu viele RFC-Verbindungen nutzen können und dadurch Zugriff auf andere SAP-Systeme erhalten. |

**Tabelle 5.12** Checkliste zu RFC-Verbindungen (Forts.)

Wie Sie die einzelnen Punkte praktisch am SAP-System prüfen können, erfahren Sie in Abschnitt 5.2 des Dokuments **Tiede_Checklisten_Sicherheit_und_Pruefung.pdf**.

## 5.3 Trusted Systems

*Trusted Systems* sind SAP-Systeme, die sich gegenseitig vertrauen. Dies bedeutet, dass Zugriffe von einem System auf das andere ohne explizite Authentifizierung

möglich sind. Im Folgenden unterscheide ich zwischen *Trusting System* und *Trusted System*. Diese sind per Definition:

- **Trusting System**
  Das System, das einem anderen System vertraut.
- **Trusted System**
  Das System, dem vertraut wird.

In Abbildung 5.9 bedeutet dies: Vom Trusted System (IB3) können Aktionen im Trusting System (IE1) ohne explizite Anmeldung ausgeführt werden (notwendige Berechtigungen vorausgesetzt).

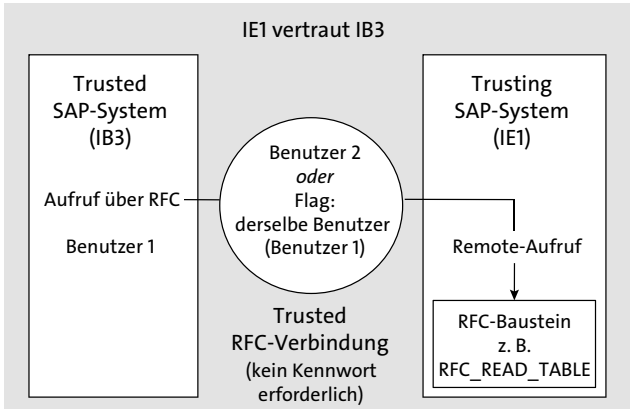


**Abbildung 5.9** Vertrauensbeziehung zwischen zwei Systemen

Im Trusting System wird das Trusted System definiert (in Abbildung 5.10 das System IB3). Die Pflege erfolgt über Transaktion SMT1. Über diese Transaktion können Sie somit auch bestehende Vertrauensbeziehungen überprüfen.

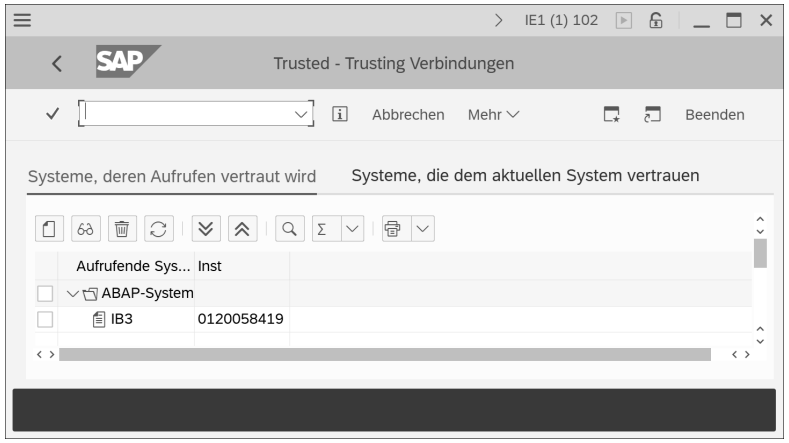


**Abbildung 5.10** Transaktion SMT1







Im zweiten Schritt muss im Trusted System (im Beispiel System IB1) eine RFC-Verbindung zum System IE1 eingerichtet werden. Dies geschieht über Transaktion SM59. Als Beispiel wird hier die RFC-Verbindung `IE1_102_NO` verwendet (siehe Abbildung 5.11).

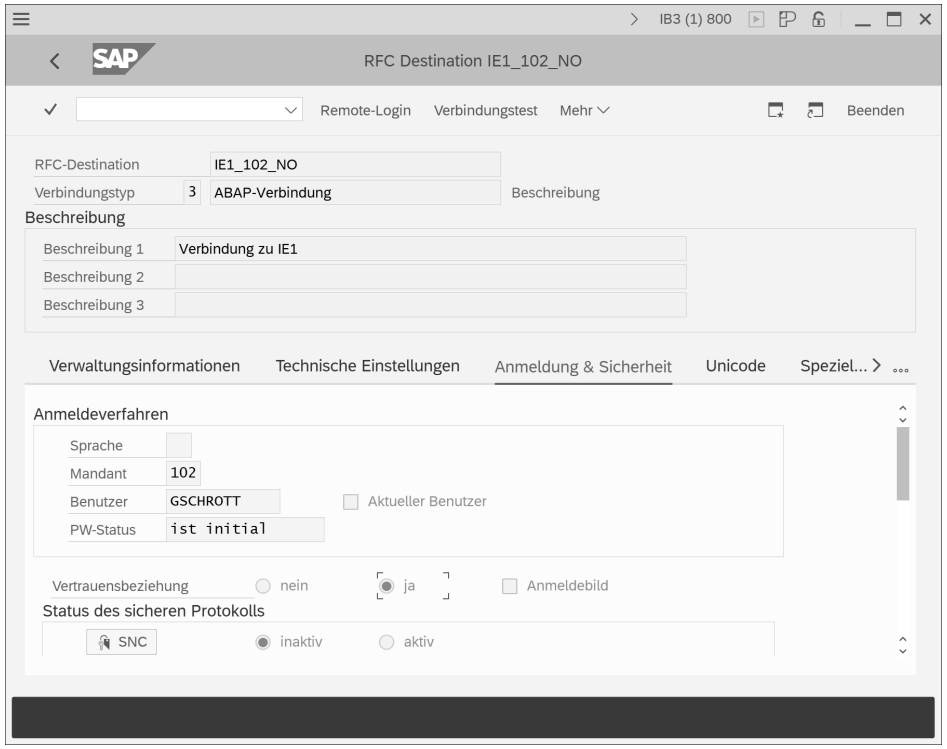


**Abbildung 5.11** Unsichere RFC-Verbindung zu einem Trusting System

Auf der zweiten Registerkarte (**Anmeldung & Sicherheit**) werden die Verbindungseinstellungen gespeichert. Dazu gehört u. a. die Eigenschaft, dass es sich um eine Trusted-Verbindung handelt (Option **Vertrauensbeziehung** = ja), mit der im Zielsystem keine weitere Anmeldung erfolgt. Ferner wird hier definiert, unter welcher Benutzerkennung der angemeldete Benutzer auf das Zielsystem IE1 springen würde. In dem vorliegenden Fall könnte also ein in IB3 angemeldeter Benutzer unter der Kennung `GSCHROTT` auf das System IE1 springen, falls für diesen Benutzer dort zusätzlich noch entsprechende Berechtigungen vorliegen.

Da bei einer Trusted-Verbindung im Zielsystem keine weitere Anmeldung erfolgt, muss an dieser Stelle kein Kennwort hinterlegt werden. Weil damit die Möglichkeit besteht, unter einer anderen Benutzerkennung zu arbeiten, ist diese Art der Konfiguration grundsätzlich als kritisch einzustufen. Eine Voraussetzung für die Nutzung dieser Verbindung ist, dass der Benutzer mit entsprechenden Berechtigungen im Zielsystem IE1 existiert.

Eine unkritische Definition einer Trusted-Verbindung ist in Abbildung 5.12 abgebildet. Durch den Haken in der Checkbox **Aktueller Benutzer** wird das Feld für die Eingabe eines Benutzernamens ausgegraut. Damit wird vorgegeben, dass im Zielsystem IE1 grundsätzlich nur unter derselben Benutzerkennung gearbeitet werden kann, mit der die Anmeldung im aktuellen System (hier IB3) erfolgt ist.

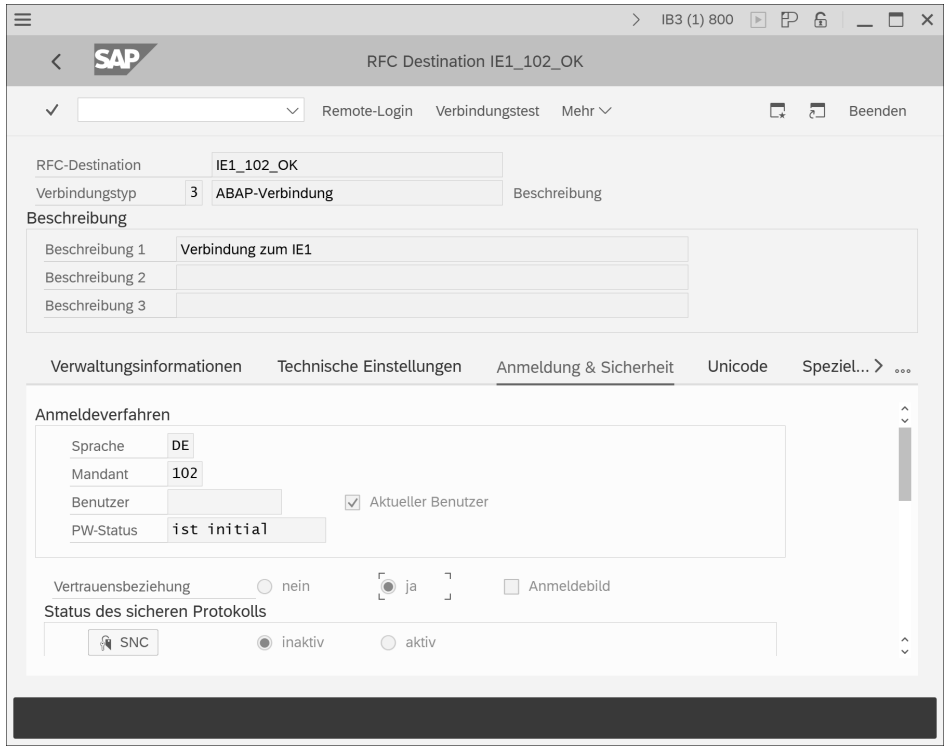


**Abbildung 5.12** Sichere RFC-Verbindung zu einem Trusting System

Auch bei dieser Definition der RFC-Verbindung ist Voraussetzung für die Nutzung, dass im Zielsystem IE1 ein Benutzer mit derselben Kennung und den notwendigen Berechtigungen existiert. Die Nutzung der Trusted-Verbindung stellt somit lediglich eine Arbeitserleichterung dar, da ansonsten die Alternative bestünde, sich in IE1 direkt unter dieser Kennung anzumelden.

Ob Trusted-RFC-Verbindungen existieren, können Sie über Tabelle RFCDES prüfen. Der Wert »Q=Y« im Feld RFCOPTIONS (**Optionen**) zeigt an, dass es sich um eine Trusted-RFC-Verbindung handelt. Der Eintrag »U=Y« gibt an, dass die Anmeldung im Zielsystem unter derselben Benutzerkennung stattfindet. Abbildung 5.13 zeigt die Selektionsmaske zu Tabelle RFCDES zur Anzeige aller Trusted-Verbindungen.





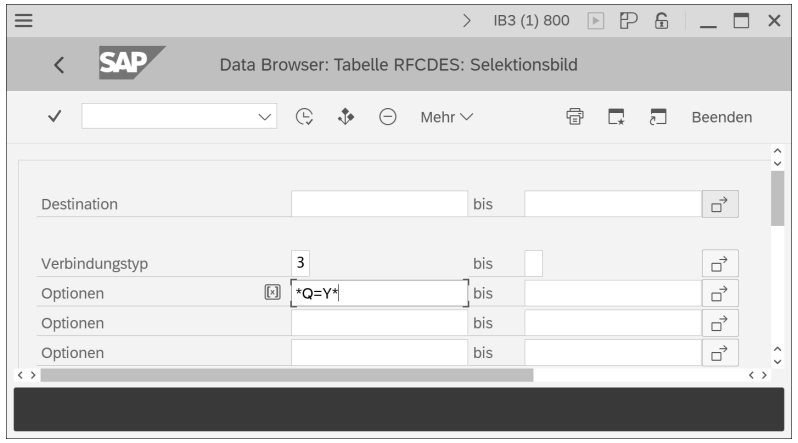


**Abbildung 5.13** Selektion aller Trusted-Verbindungen

Die Trusting Systems und die Trusted Systems werden in den folgenden Tabellen gespeichert:

- **Tabelle RFCTRUST**

  Trusted Systems
- **Tabelle RFCSYSACL**

  Trusting Systems

Die Tabellen RFCDES, RFCTRUST und RFCSYSACL sind standardmäßig zur Protokollierung vorgesehen. Bei aktivierter Tabellenprotokollierung (Systemparameter rec/client; siehe Abschnitt 4.3, »Protokollierung von Tabellenänderungen«) können Sie über Transaktion SCU3 (alternativ über den Report RSVTPROT) nachvollziehen, welche Änderungen an den Einstellungen der Vertrauensbeziehungen erfolgt sind.

### 5.3.1 Berechtigungen zur Nutzung von Trusted-Verbindungen

Damit über die Trusted-Funktionalität ein Benutzer aus einem anderen System heraus genutzt werden kann, muss er über eine Berechtigung für das Objekt S_RFCACL verfügen. Diese Berechtigung ist standardmäßig nicht im sonst sehr umfassenden Sammelprofil SAP_ALL enthalten. Ob dieses Objekt in SAP_ALL automatisch generiert wird, wird über den Schalter ADD_S_RFCACL in Tabelle PRGN_CUST definiert. Der Schalter kann zwei Werte enthalten:

- NO: Das Berechtigungsobjekt S_RFCACL wird nicht automatisch in dem Profil SAP_ALL generiert (Default-Wert).
- YES: Das Berechtigungsobjekt S_RFCACL wird automatisch in dem Profil SAP_ALL generiert.

Aus Sicherheitsgründen sollte dieser Schalter auf dem Wert »NO« stehen bzw. nicht in Tabelle PRGN_CUST enthalten sein (in dem Fall ist der Default-Wert »NO« gesetzt).

Die in Abbildung 5.14 abgebildete Berechtigung zeigt Folgendes an:

- Nur Aufrufe aus dem System IB1 sind gültig (Feld **System-Id** = IB1).
- Eine Nutzung ist nur jeweils mit derselben Benutzerkennung möglich (Feld **RFC gleiche Benutzerkennung** = Y).

Verfügt ein Benutzer im System IB2 über diese Berechtigung, kann die Trusted-Verbindung aus dem anderen System IB1 nur von einem Benutzer mit derselben Kennung aufgerufen werden.

| | | |
|---|---|---|
| Berechtigungsobjekt S_RFCACL | Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System) | |
| Berechtigung T-S026048400 | Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System) | |
| RFC_SYSID | System-Id (für SAP- und externe Systeme) | IE1 |
| RFC_CLIENT | RFC Client oder Domäne | 102 |
| RFC_USER | RFC User (SAP oder extern) | '' |
| RFC_EQUSER | RFC gleiche Benutzerkennung | Y |
| RFC_TCODE | RFC Transaktionscode | * |
| RFC_INFO | RFC Information | * |
| ACTVT | Aktivität | 16 |

**Abbildung 5.14** Berechtigung für das Objekt S_RFCACL (unkritisch)

Bei der Berechtigung in Abbildung 5.15 kann der Benutzer, dem diese Berechtigung im Trusting System (IB3) zugeordnet ist, grundsätzlich durch jeden Benutzer aus dem Trusted System (IE1) genutzt werden, wodurch diese Berechtigung als äußerst kritisch einzustufen ist. Wenn eine kritische Berechtigung dieser Art vorliegt, könnte im Trusted System IB3 eine RFC-Verbindung definiert werden, in der z. B. der Benutzername GSCHROTT fest hinterlegt wird. Somit könnte jeder Benutzer im System IB3, der diese RFC-Verbindung nutzen kann, unter der Benutzerkennung GSCHROTT im System IE1 arbeiten, also anonym.

| | | |
|---|---|---|
| Berechtigungsobjekt S_RFCACL | Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System) | |
| Berechtigung T-S026048400 | Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System) | |
| RFC_SYSID | System-Id (für SAP- und externe Systeme) | IE1 |
| RFC_CLIENT | RFC Client oder Domäne | 102 |
| RFC_USER | RFC User (SAP oder extern) | * |
| RFC_EQUSER | RFC gleiche Benutzerkennung | * |
| RFC_TCODE | RFC Transaktionscode | * |
| RFC_INFO | RFC Information | * |
| ACTVT | Aktivität | 16 |

**Abbildung 5.15** Berechtigung für das Objekt S_RFCACL (kritisch)





### 5.3.2 Zugriffsrechte

Die folgenden Tabellen zeigen Ihnen die Berechtigungen für Trusted Systems. Tabelle 5.13 enthält die Berechtigung zum Anlegen neuer Trusted Systems.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_TCODE | TCD (Transaktion) | SMT1 oder SMT2 |
| S_RFC_TT | ACTVT (Aktivität) | ■ 01 (Anlegen)<br>■ 02 (Ändern) |
| | RFC_TT_TYP (Typ in der Trusted-Beziehung) | ■ 1: aufzurufendes System<br>■ 2: aufrufendes System |
| | RFC_SYSID (System-IS) | <SID des SAP-Systems> |
| | RFC_INSTNR (Installationsnummer) | <Installationsnummer> |

**Tabelle 5.13** Berechtigung zum Anlegen neuer vertrauenswürdiger Systeme

Tabelle 5.14 zeigt die Berechtigung, um einen Benutzer mit der gleichen Kennung systemübergreifend zu verwenden.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_RFCACL | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_EQUSER (gleiche Benutzerkennung) | Y |
| | RFC_SYSID (System-ID) | <SID des SAP-Systems> |
| | RFC_USER (RFC-Benutzer) | sy-uname oder <leer> |

**Tabelle 5.14** Berechtigung zum Verwenden eines Benutzers vom anderen System aus mit derselben Benutzerkennung

Tabelle 5.15 zeigt die Berechtigung, um einen Benutzer mit einer beliebigen Benutzerkennung systemübergreifend zu verwenden.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_RFCACL | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_EQUSER (gleiche Benutzerkennung) | Y |
| | RFC_SYSID (System-ID) | <SID des SAP-Systems> |
| | RFC_USER (RFC-Benutzer) | * |

**Tabelle 5.15** Berechtigung zum Verwenden eines Benutzers vom anderen System aus mit einer beliebigen Benutzerkennung

### 5.3.3 Checkliste

In Tabelle 5.16 finden Sie die Checkliste mit den prüfungsrelevanten Fragestellungen zur Absicherung von Trusted Systems.

| Risiko | Fragestellung |
|---|---|
| | Vorgabe oder Erläuterung |
| 1 | Existieren in Systemen mit sensiblen Daten Vertrauensbeziehungen zu anderen Systemen? |
| | In allen Systemen dürfen nur Vertrauensbeziehungen existieren, die notwendig sind und genutzt werden.<br>Hier besteht das Risiko, dass durch Vertrauensbeziehungen ein anonymer Zugriff auf sensible Daten ermöglicht wird. |
| 1 | Wurden Berechtigungen vergeben, mit denen Benutzer aus anderen Systemen heraus für Zugriffe über eine Trusted-Verbindung genutzt werden können? |
| | Berechtigungen für Trusted-Zugriffe dürfen nur sehr restriktiv vergeben werden.<br>Hier besteht das Risiko, dass durch falsch vergebene Berechtigungen ein anonymer Zugriff auf Daten ermöglicht wird. |
| 2 | Existieren Benutzer, die dazu berechtigt sind, neue Vertrauensbeziehungen zu Systemen anzulegen? |
| | Es dürfen nur Basisadministratoren dazu berechtigt sein, Vertrauensbeziehungen zu definieren.<br>Hier besteht das Risiko, dass durch neue Vertrauensbeziehungen ein anonymer Zugriff auf die Daten des Systems ermöglicht wird. |
| 1 | Existieren RFC-Verbindungen zu Systemen mit sensiblen Daten, die als Trusted-Verbindung ausgewiesen sind? |
| | In allen Systemen dürfen nur Trusted-RFC-Verbindungen existieren, die notwendig sind, genutzt werden und dokumentiert worden sind.<br>Hier besteht das Risiko, dass durch die Trusted-RFC-Verbindungen ein anonymer Zugriff auf sensible Daten ermöglicht wird. |
| 1 | Existieren RFC-Verbindungen zu Systemen mit sensiblen Daten, die als Trusted-Verbindung ausgewiesen sind, bei denen eine feste Benutzerkennung hinterlegt ist und für die im Zielsystem die Berechtigung zum Aufruf über verschiedene Benutzer vergeben ist? |
| | In allen Systemen sollten nur Trusted-RFC-Verbindungen existieren, die eine Anmeldung über denselben Benutzer im Zielsystem ermöglichen.<br>Hier besteht die konkrete Möglichkeit, über die Trusted-RFC-Verbindung anonym auf das Zielsystem zuzugreifen. |

**Tabelle 5.16** Checkliste zu Trusted Systems







**Tabelle 5.16** Checkliste zu Trusted Systems (Forts.)

Wie Sie die einzelnen Punkte praktisch am SAP-System prüfen können, erfahren Sie in Abschnitt 5.3 des Dokuments **Tiede_Checklisten_Sicherheit_und_Pruefung.pdf**.

## 5.4 Zugriff von externen Programmen

Über externe Programme können alle Funktionsbausteine ausgeführt werden, die remotefähig sind. In einem SAP-NetWeaver-7.5x-System existieren ca. 18.000 remotefähige Funktionsbausteine, in einem SAP-ERP-System insgesamt ca. 50.000.

Das Ausführen von Funktionsbausteinen über RFC wird über das Berechtigungsobjekt S_RFC geschützt. Die Funktionsbausteine sind in Funktionsgruppen zusammengefasst. Mit dem Berechtigungsobjekt kann der Zugriff über die Funktionsgruppen oder über die Namen der Funktionsbausteine gesteuert werden. Die Funktionalität

dieses Objekts wird über den Systemparameter auth/rfc_authority_check gesteuert. Der Parameter kann die folgenden Werte enthalten:

- 0: Bei diesem Wert wird zum Ausführen von Funktionsbausteinen keine Berechtigung für das Objekt S_RFC benötigt. Dies stellt eine Gefährdung für das System dar; dieser Wert darf nicht eingestellt werden.
- 1: Das Berechtigungsobjekt S_RFC wird überprüft, allerdings nicht für Funktionsbausteine der Funktionsgruppe SRFC (siehe Tabelle 5.17). Es findet ebenfalls keine Berechtigungsprüfung für denselben Benutzer und denselben Benutzerkontext (Mandant und Benutzername) statt. Dies ist der Auslieferungszustand eines SAP-Systems.
- 2: Das Berechtigungsobjekt S_RFC wird überprüft, außer für Funktionsbausteine der Funktionsgruppe SRFC.
- 3: Es ist ein Login zur Ausführung der Funktionsbausteine RFC_PING und RFC_SYSTEM_INFO erforderlich, es findet aber keine Berechtigungsprüfung statt.
- 4: Es findet eine Berechtigungsprüfung für alle Funktionsbausteine statt, außer für RFC_PING und RFC_SYSTEM_INFO.
- 5: Es ist ein Login zur Ausführung des Funktionsbausteins RFC_PING erforderlich, es findet aber keine Berechtigungsprüfung statt.
- 6: Es findet eine Berechtigungsprüfung für alle Funktionsbausteine statt, außer für RFC_PING.
- 8: Es ist ein Login für alle Funktionsbausteine erforderlich, es findet aber keine Berechtigungsprüfung statt.
- 9: Das Berechtigungsobjekt S_RFC wird immer geprüft, auch für die Funktionsgruppe SRFC.

Die Funktionsbausteine der Funktionsgruppe SRFC sind in Tabelle 5.17 aufgeführt. Insbesondere Funktionsbausteine wie RFC_PING und RFC_SYSTEM_INFO werden häufig über Schnittstellen genutzt. Daher ist es in den meisten Systemen sinnvoll, den Parameter auth/rfc_authority_check auf den Wert »1« oder »2« zu setzen.

| Funktionsbaustein der Gruppe SRFC | Beschreibung |
|---|---|
| RFC_GET_LOCAL_DESTINATIONS | Liefert alle momentan aktiven RFC-Destinationen an dieselbe Datenbank. |
| RFC_GET_LOCAL_SERVERS | Liefert alle momentan aktiven RFC-Destinationen an dieselbe Datenbank. |

**Tabelle 5.17** Funktionsbausteine der Gruppe SRFC







| Funktionsbaustein der Gruppe SRFC | Beschreibung |
|---|---|
| RFC_PING | Liefert Informationen zum System zurück, wenn dieses über Ping angesprochen wird. Das Programm *Ping* können Sie zum Testen der Erreichbarkeit von Systemen nutzen. |
| RFC_SYSTEM_INFO | Liefert verschiedene Informationen über das System. |
| SYSTEM_FINISH_ATTACH_GUI | Verknüpft eine SAP-GUI-Session dieser RFC-Session. |
| SYSTEM_INVISIBLE_GUI | Lässt aktuellen SAP GUI unsichtbar (interne Verwendung). |
| SYSTEM_PREPARE_ATTACH_GUI | Baut das Kommando zum Starten des SAP GUI auf. |
| SYSTEM_RFC_VERSION_3_INIT | Initialisiert eine RFC-Verbindung auf dem Server (systeminterne Verwendung). |

**Tabelle 5.17** Funktionsbausteine der Gruppe SRFC (Forts.)

Die Felder des Berechtigungsobjekts S_RFC zeigt Tabelle 5.18.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | ■ FUGR (Funktionsgruppe)<br>■ FUNC (Funktionsbaustein) |
| | RFC_NAME (Name des RFC-Objekts) | <Namen von Funktionsgruppen oder Funktionsbausteinen> |

**Tabelle 5.18** Berechtigungsobjekt S_RFC

Berechtigungen für das Objekt S_RFC müssen auf die tatsächlich erforderlichen Funktionsbausteine eingegrenzt sein. Zu umfassende Berechtigungen können eine Gefahrenquelle darstellen. Eine Vollberechtigung (RFC_NAME = *) darf an keinen Benutzer vergeben werden. Unter anderem könnten damit alle Funktionsbausteine ausgeführt werden, die keine Berechtigungsprüfung enthalten oder bei denen die Berechtigungsprüfung deaktiviert werden kann (siehe Abschnitt 5.1.1, »Funktionsbausteine ohne Berechtigungsprüfungen«, und Abschnitt 5.1.2, »Funktionsbausteine mit schaltbaren Berechtigungen«).

Um zu ermitteln, wer bestimmte Funktionsbausteine ausführen darf, müssen Sie zuerst die Funktionsgruppe des Funktionsbausteins ermitteln. Hierzu haben Sie zwei Möglichkeiten:

1. Rufen Sie Transaktion SE37 auf. Geben Sie den Namen des Funktionsbausteins an, und lassen Sie ihn sich anzeigen. Auf der Registerkarte **Eigenschaften** ist die Funktionsgruppe hinterlegt.
2. Rufen Sie mit Transaktion SE16 die Tabelle ENLFDIR auf. Geben Sie in der Selektionsmaske im Feld FUNCNAME (**Funktionsbaustein**) den Namen ein, und lassen Sie sich die Tabelle anzeigen. Im Feld AREA (**Funktionsgruppe**) wird die Funktionsgruppe angezeigt.

Tabelle 5.19 zeigt exemplarisch die Berechtigungsprüfung für den Funktionsbaustein RFC_READ_TABLE.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | FUGR (Funktionsgruppe) |
| | RFC_NAME (Name des RFC-Objekts) | SDTX |
| oder | | |
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | FUNC (Funktionsbaustein) |
| | RFC_NAME (Name des RFC-Objekts) | RFC_READ_TABLE |

**Tabelle 5.19** Exemplarische Berechtigung für den Funktionsbaustein RFC_READ_TABLE

### 5.4.1 Ermittlung der erforderlichen RFC-Berechtigungen

Da für das Objekt S_RFC keine volle Berechtigung vergeben werden soll, müssen Sie die tatsächlich erforderlichen Berechtigungswerte ermitteln. Dies gilt insbesondere auch für Schnittstellenbenutzer. Hierzu können Sie den Langzeit-Trace in Transaktion STUSERTRACE nutzen. Hiermit können Sie die genutzten Werte des Berechtigungsobjekts S_RFC ermitteln. Abbildung 5.16 zeigt eine mögliche Konfiguration. Dort ist der Filter für Berechtigungsobjekte auf das Objekt S_RFC beschränkt.

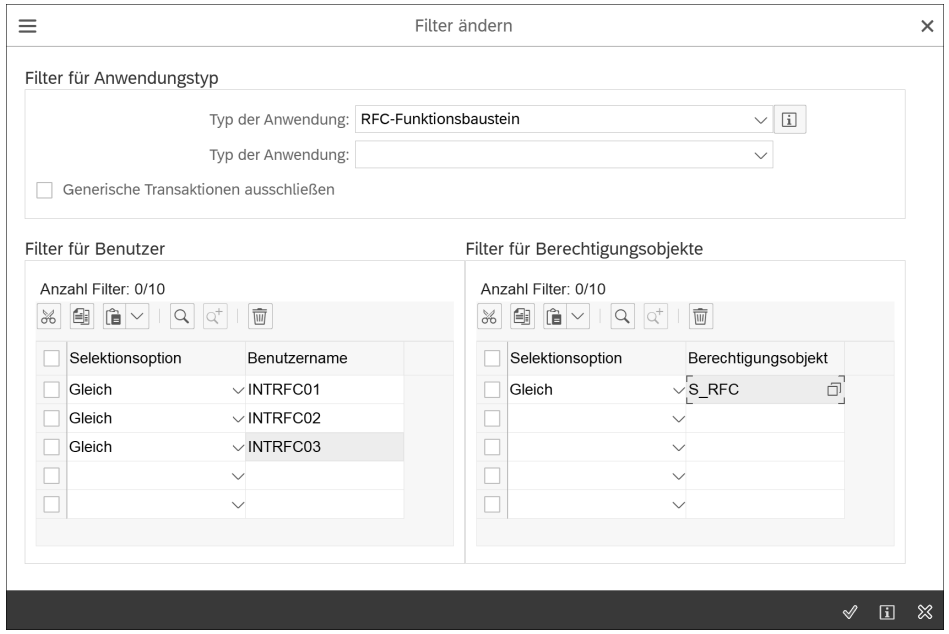


**Abbildung 5.16** Trace des Berechtigungsobjekts S_RFC

Da die Trace-Daten redundanzfrei in einer Tabelle gespeichert werden, kann der Trace auch für einen längeren Zeitraum aktiviert werden. Mithilfe der Trace-Informationen können dann Rollen erzeugt werden. Weitere Informationen zum Langzeit-Trace finden Sie in Abschnitt 10.6.3, »Der Benutzer-Langzeit-Trace«.

### 5.4.2 Zugriff auf das SAP-System über Microsoft Excel

Wie Funktionsbausteine von externen Programmen aufgerufen werden können, zeige ich in diesem Abschnitt am Beispiel von Microsoft Excel. Die Schnittstelle zu Microsoft Excel (*Dynamic Link Libraries*) wird mit dem SAP GUI auf einer Workstation installiert. Über *Visual Basic for Applications* (VBA) kann die Verbindung aufgebaut werden. Listing 5.1 zeigt den Quelltext zur Anmeldung an ein SAP-System:

```
' Objekt erstellen und Verbindung herstellen
Dim fns As Object
Set fns = CreateObject("SAP.Functions")

' Verbindungsobjekt erstellen
Dim conn As Object
```

```
Set conn = fns.Connection

' Verbindung zum Server herstellen
conn.ApplicationServer = "ibsp01"       ' Servername
conn.SYSTEM = "E01"                     ' System-ID
conn.USER = "tomtiede"                  ' Benutzername
conn.password = "cat9dog"               ' Kennwort
conn.CLIENT = "800"                     ' Mandant
conn.LANGUAGE = "D"                     ' Anmeldesprache
conn.tracelevel = 0

' Anmeldung am SAP-System ohne Anmeldebildschirm
If conn.logon(0, True) <> True Then
    MsgBox "Cannot logon!."
    Exit Sub
End If
```

**Listing 5.1** Anmeldung an ein SAP-System über Microsoft Excel

Eine Anmeldung mit korrektem Benutzernamen und Kennwort ist hier natürlich erforderlich. Nach erfolgreicher Anmeldung können nun alle Funktionsbausteine aufgerufen werden, für die der Benutzer eine Berechtigung besitzt. Mit dem Beispielcode aus Listing 5.2 können Tabelleninhalte aus dem SAP-System ausgelesen werden, indem zwei Funktionsbausteine aufgerufen werden:

```
' auszulesende Tabelle ermitteln
tabname = UCase(InputBox("Geben Sie den Namen der auszulesenden Tabelle ein",
"Tabelle auswählen", "T000"))

' Tabellenaufbau lesen: Funktionsbaustein RFC_GET_STRUCTURE_DEFINITION
result = fns.RFC_GET_STRUCTURE_DEFINITION(Exception, tabname:=tabname,
  TABLENGTH:=tablng, FIELDS:=tabfields)
the_exception = Exception

' Tabelleninhalt auslesen: Funktionsbaustein RFC_GET_TABLE_ENTRIES
result = fns.RFC_GET_TABLE_ENTRIES(Exception, BYPASS_BUFFER:=" ",
  FROM_KEY:=" ", GEN_KEY:=" ", MAX_ENTRIES:=0, TABLE_NAME:=tabname,
  TO_KEY:=" ", NUMBER_OF_ENTRIES:=num_entries, entries:=entries)
the_exception = Exception
```

**Listing 5.2** Auslesen von Tabelleninhalten aus dem SAP-System







Die Funktionsbausteine enthalten Berechtigungsprüfungen. Somit wird beim Auslesen einer Tabelle hier auch das Zugriffsrecht zum Lesen dieser Tabelle benötigt, allerdings keine Transaktionsberechtigung.

Abbildung 5.17 zeigt das Ergebnis des Auslesens in Microsoft Excel. Ausgelesen wurde die Mandantentabelle T000. Der erste Teil zeigt den Aufbau der Tabelle, der mit dem Funktionsbaustein RFC_GET_STRUCTURE_DEFINITION ausgelesen wurde. Im unteren Teil wird der Inhalt der Tabelle angezeigt. Dieser wurde mit dem Funktionsbaustein RFC_GET_TABLE_ENTRIES ausgelesen. Auf diese Weise können von jeder Programmiersprache aus Funktionsbausteine in SAP-Systemen aufgerufen werden. Berechtigungen für das Berechtigungsobjekt S_RFC dürfen nur äußerst restriktiv vergeben werden, da hiermit große Risiken verbunden sind.

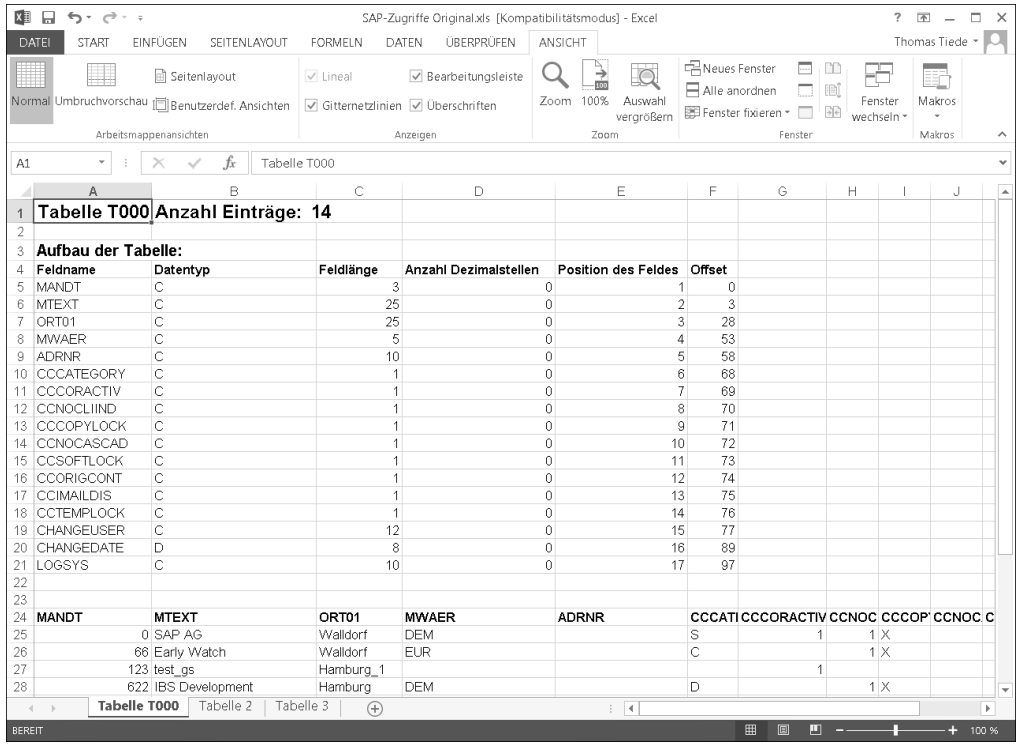


**Abbildung 5.17** Über RFC ausgelesene Tabelle in Microsoft Excel

### 5.4.3 ABAP-Quelltexte über RFC ausführen

Über Funktionsbausteine kann es möglich sein, beliebige ABAP-Quelltexte an das SAP-System zu schicken und diese ausführen zu lassen. Es kann ein Quelltext übergeben werden, der dann ohne weitere Überprüfungen ausgeführt wird. Dies ist z. B. mit dem Funktionsbaustein RFC_ABAP_INSTALL_AND_RUN möglich. Dieser existiert aktuell

noch in allen SAP-Systemen außer in SAP-S/4HANA-Systemen mit einem Releasestand >= 1909 (siehe SAP-Hinweis 2578542). In SAP S/4HANA 1809 existiert er noch, ist aber deaktiviert. In allen anderen Systemen (z. B. reinen SAP-NetWeaver-Systemen oder SAP ERP) ist er vorhanden und kann weiterhin genutzt werden.

Der Quelltext in Listing 5.3 löscht z. B. Tabellenänderungsprotokolle aus dem System, indem sie direkt aus der Protokolltabelle DBTABLOG gelöscht werden.

```
REPORT tab_del.
TABLES:  dbtablog,
         strmpar,
         tddat.
TYPES:   BEGIN OF     dbtablog_key_type,
         logdate LIKE dbtablog-logdate,
         logtime LIKE dbtablog-logtime,
         logid   LIKE dbtablog-logid,
         END OF       dbtablog_key_type.
DATA:    antwort,
         i                   TYPE i,
         cnt_loops           TYPE i,
         tabelle             LIKE tddat-tabname,
         i_dbtablog_key      TYPE TABLE OF dbtablog_key_type
           INITIAL SIZE 2000,
         edatum              LIKE strmpar-tbscdlda.

edatum  = '20140531'. " Bis zu diesem Datum wird gelöscht.
tabelle = 'T001'.     " Die Protokolle dieser Tabelle werden
                      " gelöscht.

SELECT COUNT(*) FROM dbtablog
  WHERE tabname = tabelle AND logdate <= edatum.
cnt_loops = sy-dbcnt DIV 2000.
IF cnt_loops = 0 AND sy-dbcnt > 0. cnt_loops = 1. ENDIF.

i = 0.
DO cnt_loops TIMES.
   SELECT logdate logtime logid FROM dbtablog
     INTO TABLE i_dbtablog_key
     UP TO 2000 ROWS WHERE tabname = tabelle AND logdate
                                           <= edatum.
   IF SY-SUBRC = 0.
      DELETE dbtablog FROM TABLE i_dbtablog_key.
```





```
      COMMIT WORK.
      i = i + SY-DBCNT.
   ENDIF.
ENDDO.

WRITE: 'Tabellenänderungsprotokolle für Tabelle ',
       tabelle,
       ' wurden bis zum ', EDATUM, ' gelöscht!'.
```

**Listing 5.3** Löschen von Tabelleneinträgen über einen Funktionsbaustein

Wird dieser Quelltext dem Funktionsbaustein RFC_ABAP_INSTALL_AND_RUN übergeben, werden die Tabellenänderungsprotokolle der angegebenen Tabelle bis zum angegebenen Datum unwiderruflich und ohne Protokoll gelöscht. Dies verstößt u. a. gegen § 257 HGB, da diese Protokolle als Verfahrensanweisung gelten und somit aufbewahrungspflichtig sind.

So kann jeder beliebige Vorgang über diese Funktionsbausteine ausgeführt werden. Das Zugriffsrecht zum Ausführen dieser Funktionsbausteine sollte daher keinem Dialogbenutzer zugeordnet werden.

### 5.4.4 Zugriffsrechte

Die folgenden Tabellen zeigen Ihnen die Berechtigungen zum Zugriff auf SAP-Systeme durch externe Programme. Tabelle 5.20 zeigt die Berechtigung zum externen Aufruf von Funktionsbausteinen.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | FUGR oder FUNC |
| | RFC_NAME (Name des RFC-Objekts) | * |

**Tabelle 5.20** Berechtigung zum Aufruf aller Funktionsbausteine per Remote Function Call

Tabelle 5.21 zeigt die speziellen Berechtigungen zum externen Aufruf des Funktionsbausteins RFC_ABAP_INSTALL_AND_RUN.

| Berechtigungsobjekt | Feld | Wert |
|---|---|---|
| S_TCODE | TCD (Transaktion) | SE38 |
| S_RFCRAIAR | ACTVT (Aktivität) | 16 (Ausführen) |
| S_DEVELOP | ACTVT (Aktivität) | ■ 01 (Anlegen)<br>■ 02 (Ändern) |
| | OBJTYPE (Objekttyp) | PROG |
| | OBJNAME (Objektname) | Z$$$XRFC |
| | DEVCLASS (Paket) | $TMP |
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | FUGR |
| | RFC_NAME (Name des RFC-Objekts) | SUTL |
| **oder** | | |
| S_RFC | ACTVT (Aktivität) | 16 (Ausführen) |
| | RFC_TYPE (Typ des RFC-Objekts) | FUNC |
| | RFC_NAME (Name des RFC-Objekts) | RFC_ABAP_INSTALL_AND_RUN |

**Tabelle 5.21** Berechtigung zum Aufrufen des Funktionsbausteins RFC_ABAP_INSTALL_AND_RUN

### 5.4.5 Checkliste

In Tabelle 5.22 finden Sie die Checkliste mit den prüfungsrelevanten Fragestellungen zum Zugriff auf ein SAP-System durch externe Programme.







| Risiko | Fragestellung<br>Vorgabe oder Erläuterung |
|---|---|
| 1 | Besitzen Benutzer das Recht, alle Funktionsbausteine auszuführen?<br>Dieses Zugriffsrecht sollte keinem Benutzer zugeordnet werden.<br>Hier besteht das Risiko, dass Benutzer über die Funktionsbausteine von externen Programmen aus kritische Aktionen im SAP-System durchführen können. |
| 1 | Werden im System Zugriffsrechte für das Objekt S_RFC überprüft?<br>Es müssen Zugriffsrechte für das Objekt S_RFC überprüft werden.<br>Hier besteht das Risiko, dass Funktionsbausteine ohne Berechtigung ausgeführt werden können. |
| 1 | Besitzen Benutzer das Recht, den Funktionsbaustein RFC_ABAP_INSTALL_AND_RUN auszuführen?<br>Das Zugriffsrecht zum Ausführen dieses Funktionsbausteins soll keinem Benutzer zugeordnet werden.<br>Hier besteht das Risiko, dass Benutzer ABAP-Quellcode ins System übertragen und ungeprüft ausführen können, was u. a. einen Verstoß gegen § 239 HGB, Führung der Handelsbücher (»Radierverbot«), darstellt. |

**Tabelle 5.22** Checkliste zu RFC-Berechtigungen

Wie Sie die einzelnen Punkte praktisch am SAP-System überprüfen können, erfahren Sie in Abschnitt 5.4 des Dokuments **Tiede_Checklisten_Sicherheit_und_Pruefung.pdf**.