



Aktuell zu  
SAP S/4HANA

# Sicherheit und Prüfung von SAP®-Systemen

- › Das umfassende Handbuch zu SAP-Werkzeugen und Prüfschritten
- › Systemsicherheit, Protokollierung und Berechtigungsverwaltung
- › 5., aktualisierte und erweiterte Auflage inkl. SAP HANA



Mit praktischen Checklisten und Anleitungen zum Download

Thomas Tiede

## 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 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).

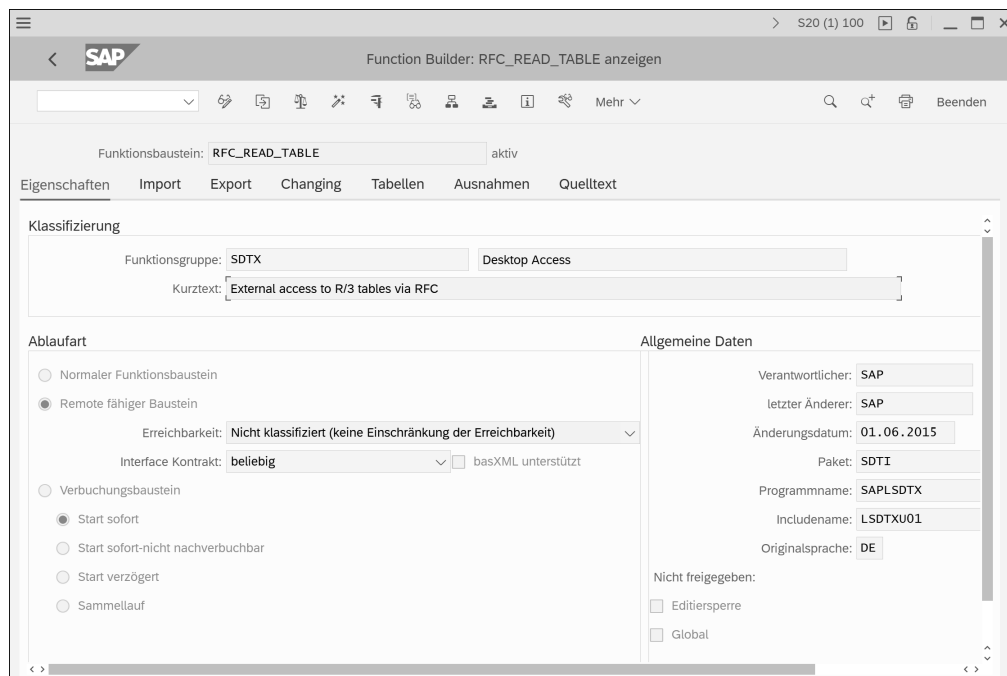


Abbildung 5.1 Eigenschaften eines Funktionsbausteins

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

Registerkarte	Eigenschaft
Eigenschaften	<ul style="list-style-type: none"> <li>■ <b>Funktionsgruppe</b> Die Funktionsgruppe wird zur Vergabe einer Berechtigung für den Funktionsbaustein genutzt.</li> <li>■ <b>Ablaufart</b> Die Eigenschaft <b>Remote fähiger Baustein</b> zeigt an, dass der Funktionsbaustein von anderen Systemen aus aufgerufen werden kann.</li> </ul>
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.

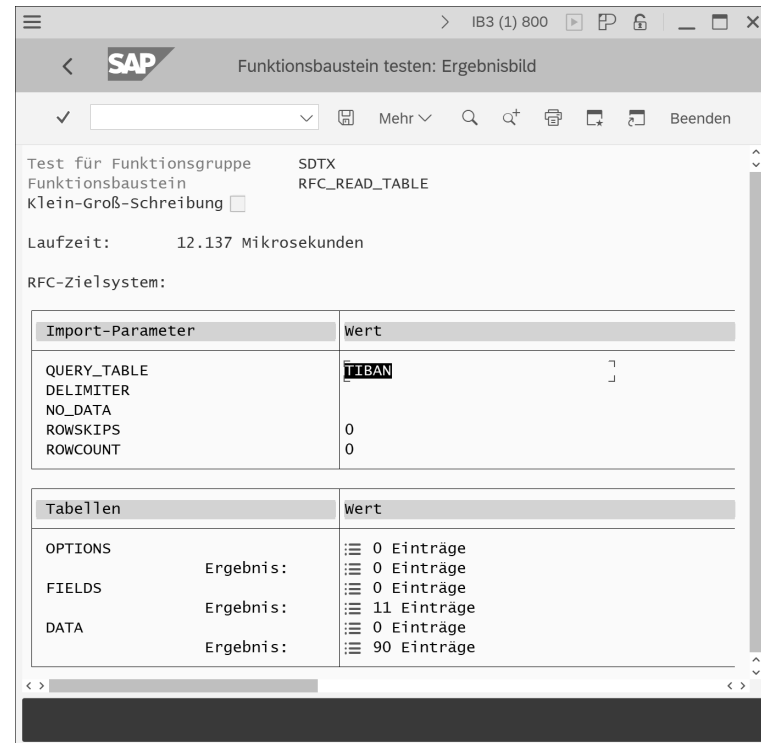


Abbildung 5.2 Ausführen eines Funktionsbausteins

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.

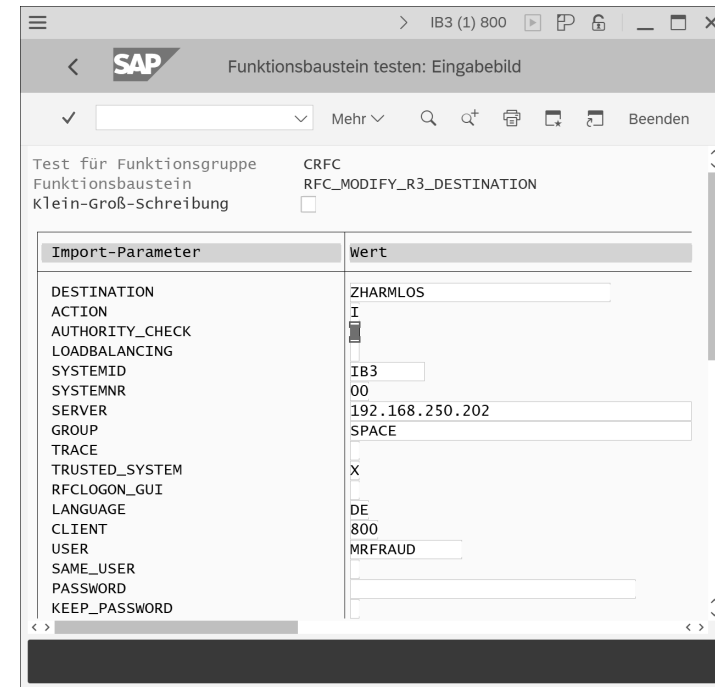


Abbildung 5.3 Berechtigungsprüfung deaktivieren

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.

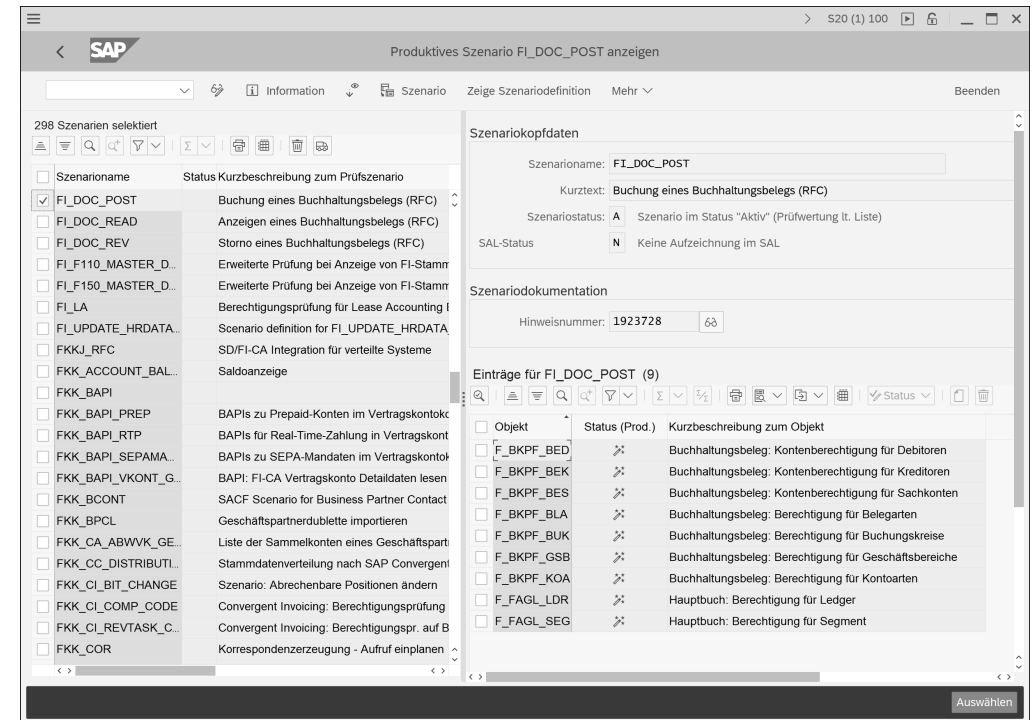


Abbildung 5.4 Szenario FI\_DOC\_POST

### 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 Protokolierte 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 Protokolierte 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	<ul style="list-style-type: none"> <li>■ BAPI_USER_CREATE</li> <li>■ BAPI_USER_CREATE1</li> <li>■ BAPI_USER_DELETE</li> <li>■ BAPI_USER_PROFILES_ASSIGN</li> <li>■ PRGN_INTERFACE_USER</li> <li>■ RFC_ABAP_INSTALL_AND_RUN</li> <li>■ RFC_GET_TABLE_ENTRIES</li> <li>■ RFC_READ_TABLE</li> <li>■ RS_FUNCTIONMODULE_INSERT</li> <li>■ SUSR_RFC_USER_INTERFACE</li> <li>■ SXPB_CALL_SYSTEM</li> <li>■ SXPB_COMMAND_EXECUTE</li> <li>■ SXPB_COMMAND_EXECUTE_LONG</li> <li>■ TABLE_ENTRIES_GET_VIA_RFC</li> <li>■ TH_REMOTE_TRANSACTION</li> </ul>
ABAPBlacklistedSOAPRFCMs	<ul style="list-style-type: none"> <li>■ SXPB_COMMAND_EXECUTE</li> <li>■ SXPB_CALL_SYSTEM</li> <li>■ RFC_SYSTEM_INFO</li> <li>■ BAPI_USER_CREATE1</li> <li>■ RFC_READ_TABLE</li> </ul>
<ul style="list-style-type: none"> <li>■ ABAPDeactivatedDeletedFMs</li> <li>■ AndReports/ABAPFunction-ModulesRFC</li> <li>■ EnablementRemoved</li> </ul>	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 (Transaktion)	SE37 oder SE80 oder Report RS_TESTFRAME_CALL

Tabelle 5.6 Berechtigung zum Ausführen von Funktionsbausteinen

Berechtigungsobjekt	Feld	Wert
S_DEVELOP	ACTVT (Aktivität)	16 (Ausführen)
	OBJTYPE (Objektyp)	FUGR (Funktionsgruppe)
	OBJNAME (Objektname)	Name der Funktionsgruppe
	DEVCLASS (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 (Transaktion)	SE37 oder SE80 oder Report RS_TESTFRAME_CALL
S_DEVELOP	ACTVT (Aktivität)	16 (Ausführen)
	OBJTYPE (Objektyp)	FUGR (Funktionsgruppe)
	OBJNAME (Objektname)	*
	DEVCLASS (Paket)	*
	P_GROUP (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
	Vorgabe oder Erläuterung
2	Werden Anmeldungen und Funktionsbausteinaufrufe über RFC protokolliert?
	RFC-Falschanmeldungen und fehlgeschlagene Funktionsbausteinaufrufe sind zu protokollieren. 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. 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. 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](http://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.

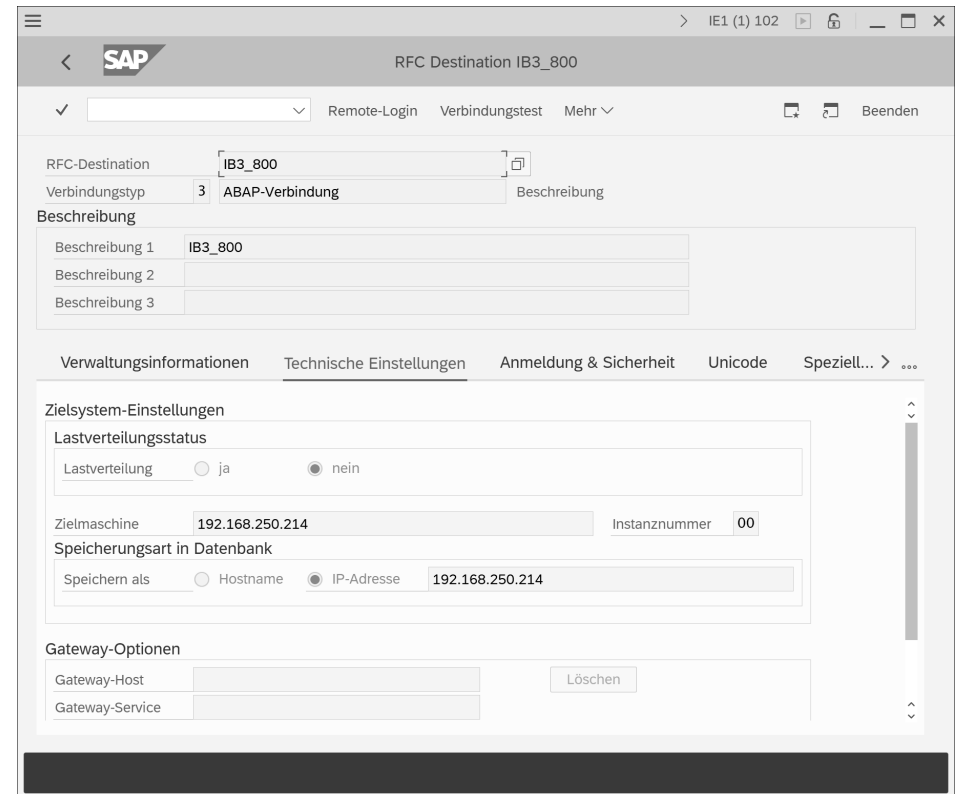


Abbildung 5.5 Transaktion SM59 – RFC-Verbindungen pflegen

Gespeichert werden die RFC-Verbindungen in Tabelle RFCDES. Eine Übersicht über alle RFC-Verbindungen bieten auch die Transaktionen/Reports RSRSDDEST (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.



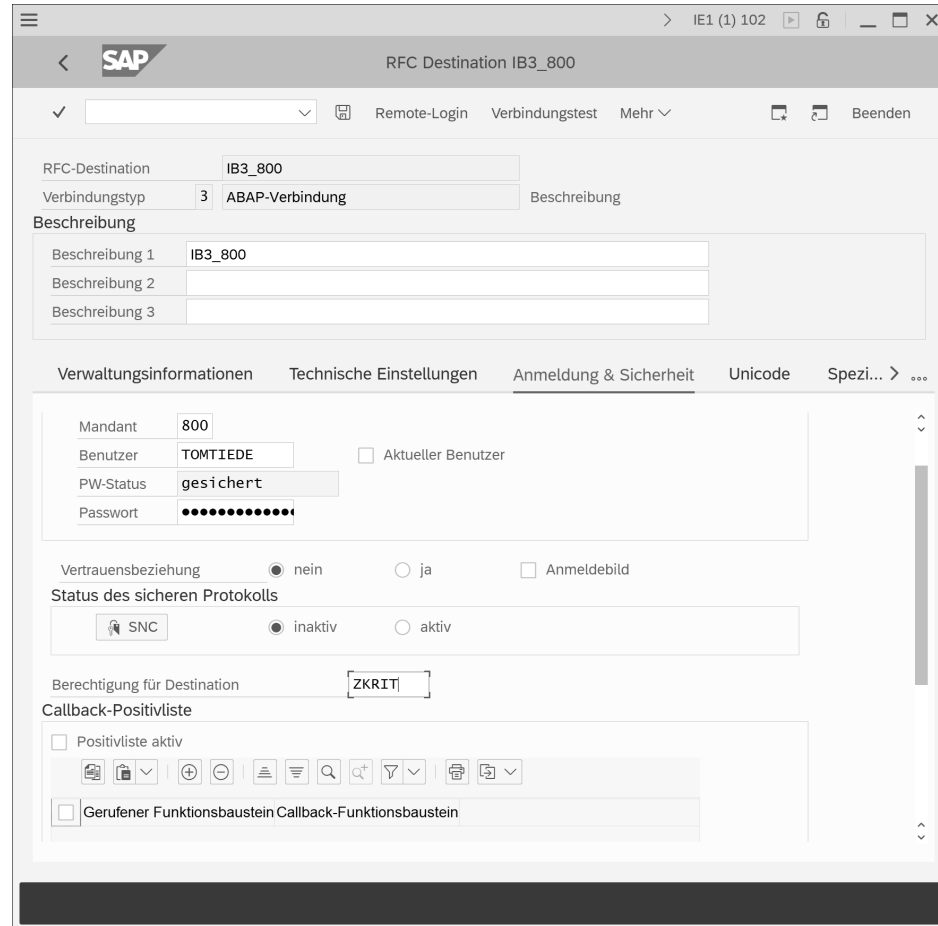


Abbildung 5.6 RFC-Verbindung durch einen Berechtigungswert schützen

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 RSEACTB und RSECTAB (*sicherer Speicher*) gespeichert. Den Inhalt dieser Tabellen können Sie mit den Standard-Tabellenanzeigttransaktionen 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).

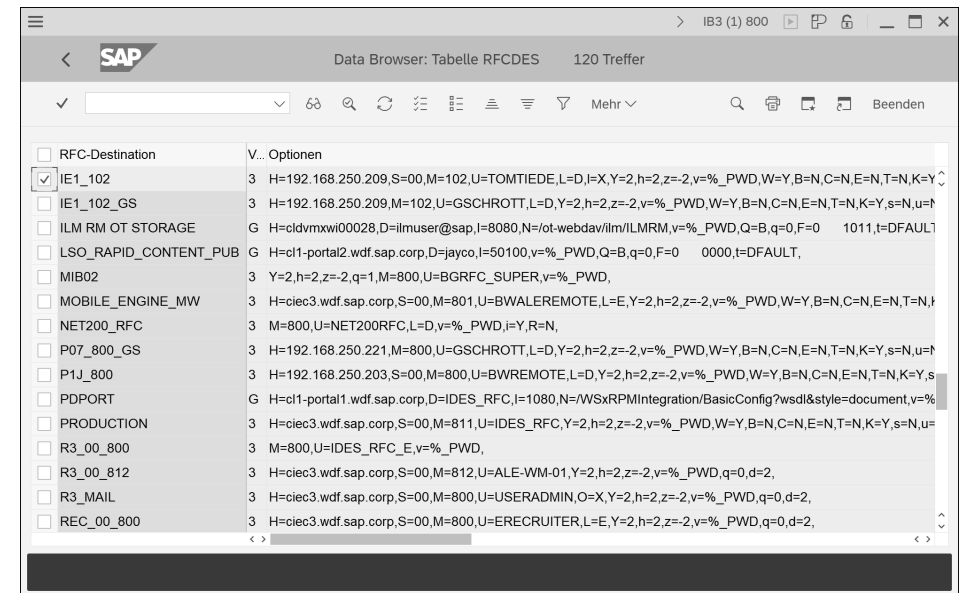


Abbildung 5.7 RFC-Verbindungen mit hinterlegten Kennwörtern

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 OO, 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 **Password** 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 solcher RFC-Verbindungen 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).

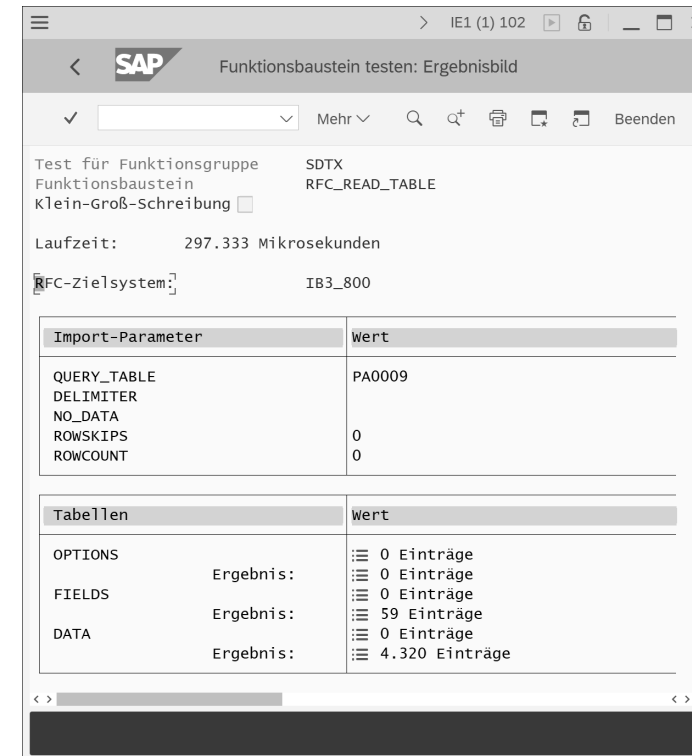


Abbildung 5.8 Funktionsbaustein in einem anderen System ausführen

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)	<ul style="list-style-type: none"> <li>■ 01 (Anlegen)</li> <li>■ 02 (Ändern)</li> <li>■ 06 (Löschen)</li> </ul>
	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	<p>In allen Systemen der Systemlandschaft dürfen nur RFC-Verbindungen existieren, die notwendig sind und genutzt werden.</p> <p>Hier besteht das Risiko, dass durch RFC-Verbindungen Schnittstellen zu Systemen aufgebaut werden können, die nicht mit dem SAP-System verbunden sein sollten.</p>
2	<p>Sind die eingerichteten RFC-Verbindungen dokumentiert (außerhalb des SAP-Systems)?</p> <p>Jede RFC-Verbindung muss so dokumentiert sein, dass ihr Verwendungszweck eindeutig nachvollziehbar ist.</p> <p>Hier besteht das Risiko, dass RFC-Verbindungen aufgrund einer fehlenden Dokumentation falsch genutzt werden.</p>
1	<p>Existieren RFC-Verbindungen, in denen für Dialog- oder Servicebenutzer Kennwörter hinterlegt sind?</p> <p>RFC-Verbindungen mit hinterlegten Kennwörtern für Dialogbenutzer dürfen nicht existieren.</p> <p>Hier besteht das Risiko, dass durch diese RFC-Verbindungen eine Anmeldung ohne Benutzerkennung und Kennwort möglich ist.</p>
2	<p>Wer ist berechtigt, RFC-Verbindungen zu pflegen?</p> <p>Dieses Zugriffsrecht dürfen nur Basisadministratoren besitzen.</p> <p>Hier besteht das Risiko, dass unberechtigte Benutzer RFC-Verbindungen ändern, neue anlegen oder vorhandene löschen.</p>
2	<p>Wer besitzt das Recht, alle RFC-Verbindungen zu nutzen?</p> <p>Dieses Zugriffsrecht sollten nur Administratoren besitzen.</p> <p>Hier besteht das Risiko, dass Benutzer zu viele RFC-Verbindungen nutzen können und dadurch Zugriff auf andere SAP-Systeme erhalten.</p>

**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).

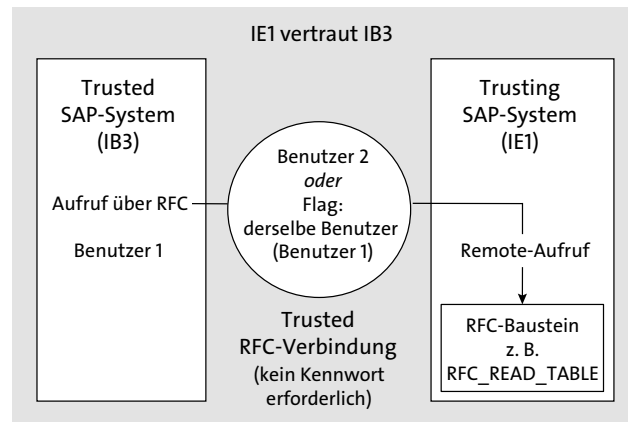


Abbildung 5.9 Vertrauensbeziehung zwischen zwei Systemen

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.

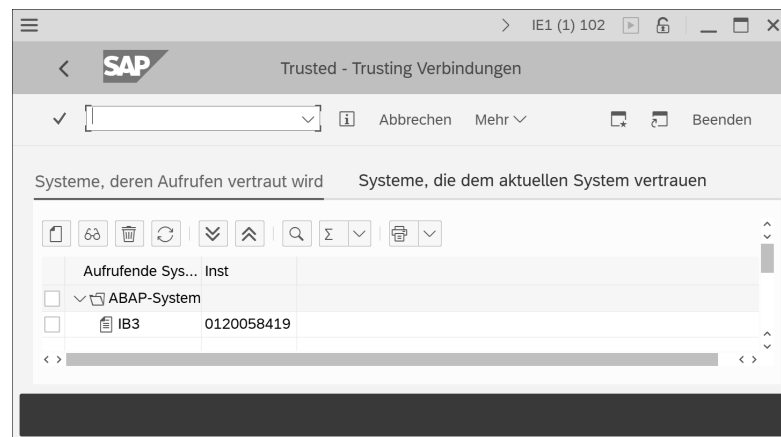


Abbildung 5.10 Transaktion SMT1

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).

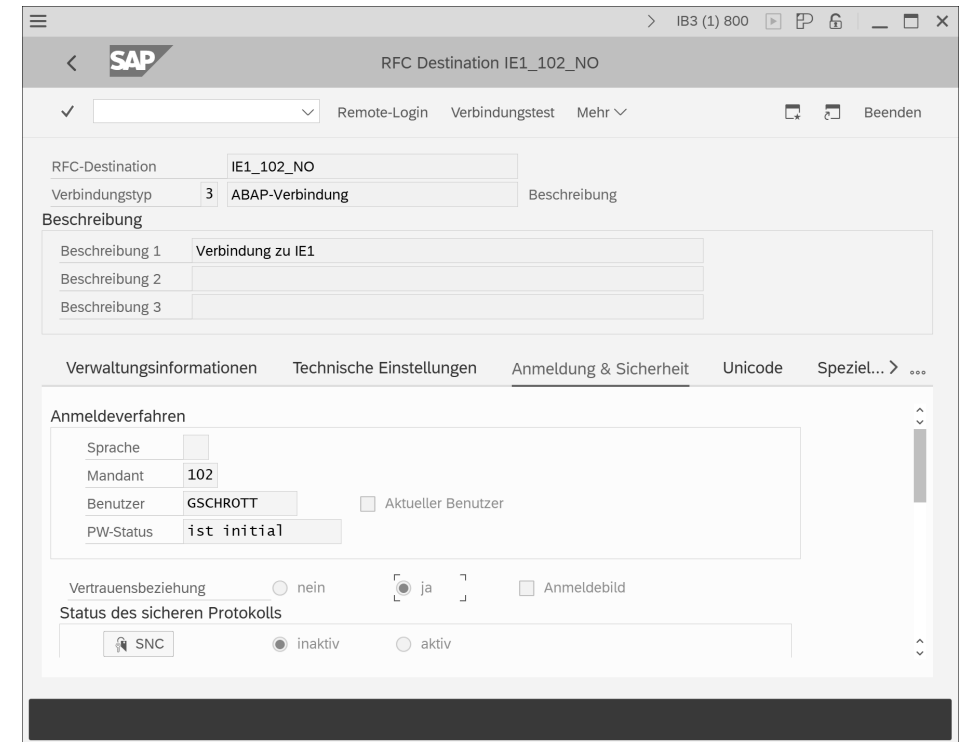


Abbildung 5.11 Unsichere RFC-Verbindung zu einem Trusting System

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 Benutzererkennung 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 Benutzererkennung 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.

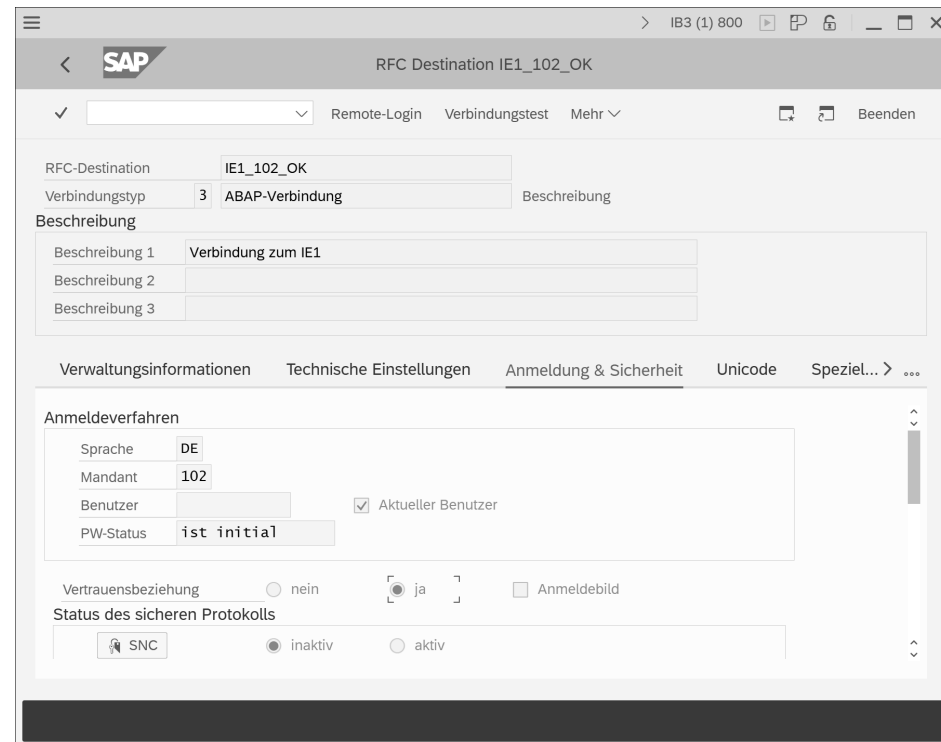


Abbildung 5.12 Sichere RFC-Verbindung zu einem Trusting System

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.

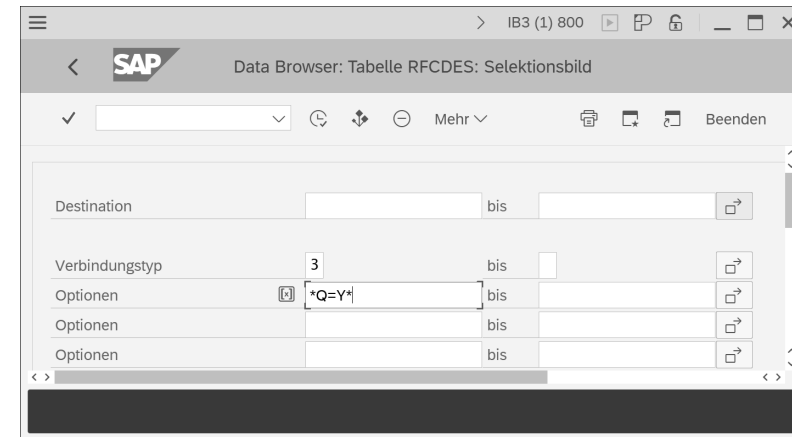


Abbildung 5.13 Selektion aller Trusted-Verbindungen

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

- **Tabelle RFCTRUST**  
Trusting Systems
- **Tabelle RFCSYSACL**  
Trusted 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.

▼ <input type="checkbox"/> <input type="checkbox"/> Berechtigungsobjekt S_RFCACL	Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System)	
▼ <input type="checkbox"/> <input type="checkbox"/> Berechtigung T-S026048400	Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System)	
<input type="checkbox"/> RFC_SYSID	System-Id (für SAP- und externe Systeme)	IE1
<input type="checkbox"/> RFC_CLIENT	RFC Client oder Domäne	102
<input type="checkbox"/> RFC_USER	RFC User (SAP oder extern)	"
<input type="checkbox"/> RFC_EUSER	RFC gleiche Benutzerkennung	Y
<input type="checkbox"/> RFC_TCODE	RFC Transaktionscode	*
<input type="checkbox"/> RFC_INFO	RFC Information	*
<input type="checkbox"/> 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.

▼ <input type="checkbox"/> <input type="checkbox"/> Berechtigungsobjekt S_RFCACL	Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System)	
▼ <input type="checkbox"/> <input type="checkbox"/> Berechtigung T-S026048400	Berechtigungsprüfung für RFC-Benutzer (z.B. Trusted System)	
<input type="checkbox"/> RFC_SYSID	System-Id (für SAP- und externe Systeme)	IE1
<input type="checkbox"/> RFC_CLIENT	RFC Client oder Domäne	102
<input type="checkbox"/> RFC_USER	RFC User (SAP oder extern)	*
<input type="checkbox"/> RFC_EUSER	RFC gleiche Benutzerkennung	*
<input type="checkbox"/> RFC_TCODE	RFC Transaktionscode	*
<input type="checkbox"/> RFC_INFO	RFC Information	*
<input type="checkbox"/> 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)	<ul style="list-style-type: none"> <li>■ 01 (Anlegen)</li> <li>■ 02 (Ändern)</li> </ul>
	RFC_TT_TYP (Typ in der Trusted-Beziehung)	<ul style="list-style-type: none"> <li>■ 1: aufzurufendes System</li> <li>■ 2: aufrufendes System</li> </ul>
	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_EUSER (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.

Berechtigungs-objekt	Feld	Wert
S_RFCACL	ACTVT (Aktivität)	16 (Ausführen)
	RFC_EQUUSER (gleiche Benutzererkennung)	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 Benutzererkennung

### 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. 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. Hier besteht das Risiko, dass durch falsch vergebene Berechtigungen ein anonymer Zugriff auf Daten ermöglicht wird.

**Tabelle 5.16** Checkliste zu Trusted Systems

Risiko	Fragestellung
	Vorgabe oder Erläuterung
2	Existieren Benutzer, die dazu berechtigt sind, neue Vertrauensbeziehungen zu Systemen anzulegen?  Es dürfen nur Basisadministratoren dazu berechtigt sein, Vertrauensbeziehungen zu definieren. 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. 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 Benutzererkennung 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. Hier besteht die konkrete Möglichkeit, über die Trusted-RFC-Verbindung anonym auf das Zielsystem zuzugreifen.

**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
<code>RFC_GET_LOCAL_DESTINATIONS</code>	Liefert alle momentan aktiven RFC-Destinationen an dieselbe Datenbank.
<code>RFC_GET_LOCAL_SERVERS</code>	Liefert alle momentan aktiven RFC-Destinationen an dieselbe Datenbank.

Tabelle 5.17 Funktionsbausteine der Gruppe SRFC

Funktionsbaustein der Gruppe SRFC	Beschreibung
<code>RFC_PING</code>	Liefert Informationen zum System zurück, wenn dieses über Ping angesprochen wird. Das Programm <i>Ping</i> können Sie zum Testen der Erreichbarkeit von Systemen nutzen.
<code>RFC_SYSTEM_INFO</code>	Liefert verschiedene Informationen über das System.
<code>SYSTEM_FINISH_ATTACH_GUI</code>	Verknüpft eine SAP-GUI-Session dieser RFC-Session.
<code>SYSTEM_INVISIBLE_GUI</code>	Lässt aktuellen SAP GUI unsichtbar (interne Verwendung).
<code>SYSTEM_PREPARE_ATTACH_GUI</code>	Baut das Kommando zum Starten des SAP GUI auf.
<code>SYSTEM_RFC_VERSION_3_INIT</code>	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
<code>S RFC</code>	<code>ACTVT</code> (Aktivität)	16 (Ausführen)
	<code>RFC_TYPE</code> (Typ des RFC-Objekts)	<ul style="list-style-type: none"> <li>■ FUGR (Funktionsgruppe)</li> <li>■ FUNC (Funktionsbaustein)</li> </ul>
	<code>RFC_NAME</code> (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
<b>oder</b>		
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.

gungsobjekts S\_RFC ermitteln. Abbildung 5.16 zeigt eine mögliche Konfiguration. Dort ist der Filter für Berechtigungsobjekte auf das Objekt S\_RFC beschränkt.

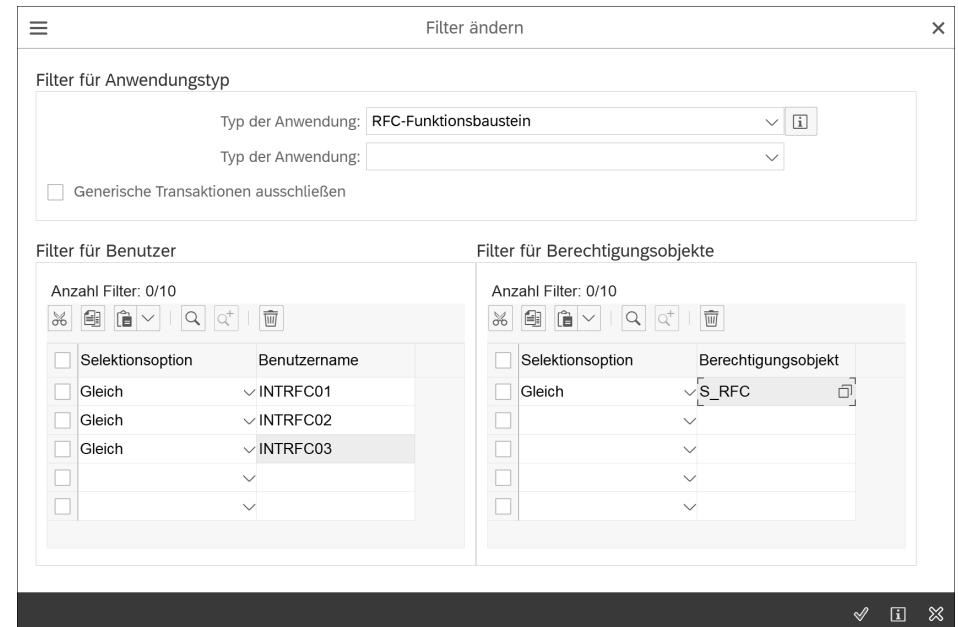


Abbildung 5.16 Trace des Berechtigungsobjekts S\_RFC

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(TextBox("Geben Sie den Namen der auszulesenden Tabelle ein",
"Table auswählen", "T000"))
```

```
' Tabellenaufbau lesen: Funktionsbaustein RFC_GET_STRUCTURE_DEFINITION
result = fns.RFC_GET_STRUCTURE_DEFINITION(Exception, tabname:=tabname,
TABLELENGTH:=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.

Tabelle T000 Anzahl Einträge: 14										
Aufbau der Tabelle:										
Feldname	Datentyp	Feldlänge	Anzahl Dezimalstellen	Position des Feldes	Offset					
MANDT	C	3	0	1	0					
MTEXT	C	25	0	2	3					
ORT01	C	25	0	3	28					
MWAER	C	5	0	4	53					
ADRNR	C	10	0	5	58					
CCCATEGORY	C	1	0	6	68					
CCCORACTIV	C	1	0	7	69					
CCNOCLIIND	C	1	0	8	70					
CCCOPYLOCK	C	1	0	9	71					
CCNOCASCAD	C	1	0	10	72					
CCSOFTLOCK	C	1	0	11	73					
CCORIGCONT	C	1	0	12	74					
CCMAILDIS	C	1	0	13	75					
CCTEMPLOCK	C	1	0	14	76					
CHANGEUSER	C	12	0	15	77					
CHANGEDATE	D	8	0	16	89					
LOGSYS	C	10	0	17	97					
MANDT	MTEXT	ORT01	MWAER	ADRNR	CCCATI	CCCORACTIV	CCNOC	CCCOP	CCNOC	C
0	SAP AG	Walldorf	DEM		S		1			1 X
66	Early Watch	Walldorf	EUR		C					1 X
123	test_gs	Hamburg_1					1			
622	IBS Development	Hamburg	DEM		D					1 X

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 Release-stand  $\geq$  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-abcnt DIV 2000.
IF cnt_loops = 0 AND sy-abcnt > 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-ABCNT.
      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)	<ul style="list-style-type: none"> <li>■ 01 (Anlegen)</li> <li>■ 02 (Ändern)</li> </ul>
	OBJTYPE (Objektyp)	PROG
	OBJNAME (Objektnamen)	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
<b>oder</b>		
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
	Vorgabe oder Erläuterung
1	Besitzen Benutzer das Recht, alle Funktionsbausteine auszuführen?
	Dieses Zugriffsrecht sollte keinem Benutzer zugeordnet werden. 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?
	Es müssen Zugriffsrechte für das Objekt S_RFC überprüft werden. Hier besteht das Risiko, dass Funktionsbausteine ohne Berechtigung ausgeführt werden können.
1	Besitzen Benutzer das Recht, den Funktionsbaustein RFC_ABAP_INSTALL_AND_RUN auszuführen?
	Das Zugriffsrecht zum Ausführen dieses Funktionsbausteins soll keinem Benutzer zugeordnet werden. 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](#).

## Einleitung

Die letzte Auflage dieses Buches ist 2018 im Rheinwerk Verlag erschienen, und nach drei Jahren ist es nun Zeit für eine Neuauflage. Als ich an dem Manuskript der Voraufgabe arbeitete, war SAP S/4HANA bereits zwei Jahre auf dem Markt, aber es liefen nur wenig Migrationsprojekte. SAP-Kundenunternehmen informierten sich über die neue Business Suite und führten Vorstudien für die Migration durch. Diese Situation sieht inzwischen grundlegend anders aus. Bereits Ende 2019 gaben laut der Lünen-donk-Studie 52 % der befragten Unternehmen an, sich in einer Vorstudie zur SAP-S/4HANA-Migration zu befinden (siehe unter: <http://s-prs.de/v612212>). 98 % wollten diese Vorarbeiten bis 2021 abschließen. In dieser Auflage des Buches habe ich daher sicherheitsrelevante Themen ergänzt, die bei der Einführung und dem Betrieb von SAP S/4HANA zu beachten sind.

Verglichen mit den Entwicklungen in den letzten 24 Jahren, in denen ich mich mit der Sicherheit von SAP-Systemen befasste, ist die Umstellung von der klassischen SAP Business Suite auf SAP S/4HANA (zusammen mit der Umstellung der Datenbank auf SAP HANA) der größte Technologiewechsel in der SAP-Welt. Und auch das Bewusstsein für das Thema Sicherheit hat sich in den letzten Jahren gewandelt. War es früher »ein lästiges Übel«, werden Sicherheit und Berechtigungen heute größtenteils fest in die Vorstudien zur Migration und die Durchführung der Projekte eingeplant. Das Risiko, einem Cyberangriff zum Opfer zu fallen, ist heute so hoch wie nie. Die Gefahr eines finanziellen Schadens oder eines Reputationsschadens ist permanent vorhanden.

Zur Härtung der Systeme ist insbesondere die Sicherheit der technischen Grundkomponenten – SAP NetWeaver und der Datenbank – entscheidend. Ist hier eine entsprechende Absicherung erfolgt und sind die Berechtigungen nach dem Minimalprinzip vergeben, reduziert dies die Gefahr für Angriffe erheblich. Dieses Buch ist der Versuch, alle wesentlichen Aspekte zur Absicherung von SAP NetWeaver und der SAP-HANA-Datenbank so darzustellen, dass sie für Prüferinnen und Prüfer analysierbar und für die Sicherheitsverantwortlichen umsetzbar sind.

Daher richtet sich dieses Buch sowohl an alle, die für die Sicherheit der SAP-Systeme verantwortlich sind, als auch an diejenigen, die diese Sicherheit durch Prüfungen analysieren und bewerten.

### Aufbau des Buches

Jedes Kapitel ist in sich abgeschlossen und bietet einen umfassenden Überblick zum Thema. Die jeweiligen Abschnitte sind so aufgebaut, dass sie auch als Nachschlage-

werk für einzelne Fragestellungen genutzt werden können. Um jeden Abschnitt für sich umfassend und schlüssig darzustellen, wurden Redundanzen bewusst in Kauf genommen.

Zu fast jedem Thema gibt es einen Abschnitt zu den Zugriffsrechten. Hier sind die zu prüfenden Berechtigungen aufgeführt. Zur Prüfung dieser Berechtigungen können Sie das Benutzerinformationssystem nutzen (Transaktion SUIM). Die Auswertung von Berechtigungen ist in Abschnitt 10.5, »Prüfung von Zugriffsrechten«, beschrieben.

Außerdem gibt es zu fast jedem Abschnitt eine Checkliste. In der Checkliste sind alle Prüfungsfragen zum jeweiligen Thema zusammengefasst, inklusive einer Risikobewertung:

1. hohes Risiko
2. mittleres Risiko
3. geringes Risiko

Auf der Seite [www.sap-press.de/5145](http://www.sap-press.de/5145) erhalten Sie im Bereich **Materialien zum Buch** das Dokument **Tiede\_Checklisten\_Sicherheit\_und\_Pruefung.pdf**. Darin erläutere ich zu jedem Punkt der Checklisten die praktische Vorgehensweise am System. Dies erlaubt es Ihnen als Prüfer\*in, die jeweiligen Prüfungsschritte sofort auszuführen, auch wenn Sie nicht täglich mit dem SAP-System arbeiten.

Des Weiteren erhalten Sie im Downloadbereich das folgende Handwerkszeug:

- Die Berechtigungsrolle `IBS_SICHERHEIT_PRUEFUNG_NW755`. Sie enthält ein Menü in der Struktur dieses Buches und die erforderlichen Berechtigungen, um alle Prüfungen gemäß diesem Buch durchzuführen.
- Ein Regelwerk für SAP Access Control mit den Berechtigungsabfragen aus diesem Buch. Dies kann direkt in SAP Access Control importiert werden. Näheres dazu finden Sie in Abschnitt 1.10.4, »SAP-Access-Control-Regelwerk für dieses Buch«.
- Das Dokument **Tiede\_Anhänge\_Sicherheit\_und\_Pruefung.pdf**. Hierin sind alle sicherheitsrelevanten Parameter, Transaktionen, Reports und Tabellen sowie die sicherheitsrelevanten SAP-HANA-Tabellen aufgelistet.

In hervorgehobenen Informationskästen finden Sie in diesem Buch Inhalte, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterung stehen. Damit Sie diese Informationen sofort einordnen können, haben wir die Kästen mit den entsprechenden Symbolen gekennzeichnet:



In Kästen, die mit diesem Symbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder Hintergrundwissen, das Sie sich merken sollten.



*Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Funktionen.

## Inhalt des Buches

In **Kapitel 1**, »Umgang mit dem SAP-System und Werkzeuge zur Prüfung«, stelle ich Ihnen die Funktionen vor, die zur Prüfung von SAP-Systemen erforderlich sind. Auch wenn sich für Prüfer\*innen nicht allzu viel ändert, da sie Prüfungen auch in SAP S/4HANA weiterhin im ABAP-Stack durchführen, kommen doch regelmäßig neue Tools hinzu. Die gute Nachricht ist hier, dass die seit Jahren bekannten Transaktionen weiterhin verfügbar sind, teils mit aktualisierten Oberflächen, teils unverändert. Schwerpunkt einer jeden Prüfung sind Tabellen und Reports. Für die Nutzung von Tabellen ist der *Generic Table Browser* eingeführt worden, der auch für Prüfer\*innen teilweise neue Möglichkeiten eröffnet. Aber auch die Zugriffsstatistik, der Quick-Viewer und der SQL-Trace können hilfreich für Analysen sein.

Wesentliche Komponenten für die SAP-Sicherheit sind Tools zur Überwachung und Prüfung von Berechtigungen und zur Überwachung von Betrugsdelikten. Daher stelle ich in diesem Kapitel die Werkzeuge SAP Access Control und SAP Enterprise Threat Detection vor. Beide Komponenten werden nicht im Rahmen von Prüfungen eingesetzt, sondern zur regelhaften Absicherung. Für SAP Access Control können Sie das Regelwerk aus dem Downloadbereich zu diesem Buch nutzen, um die kritischen Berechtigungen zur SAP-Basisicherheit zu überwachen. Der letzte Abschnitt dieses Kapitels zeigt Ihnen, wie Prüfungen in SAP HANA durchgeführt werden können.

**Kapitel 2**, »Aufbau von SAP-Systemen und Systemlandschaften«, stellt den Aufbau von SAP-Systemen dar. Dieses Wissen ist elementar für die Absicherung von SAP-Systemen und -Systemlandschaften. Mit SAP S/4HANA ändert sich hier einiges, da mit dem SAP Fiori Launchpad eine neue Ebene hinzukommt. Ein weiterer Schwerpunkt dieses Kapitels liegt auf der Mandantensicherheit, von der maßgeblich auch die Produktivmandanten sowie der Mandant 000, der Systemmandant, betroffen sind. Insbesondere der Mandant 000 wird im Rahmen von Sicherheitskonzepten häufig vernachlässigt, obwohl von ihm aus auch die Systemeinstellungen vorgenommen werden können und Zugriffe auf die produktiven Daten möglich sind.

In **Kapitel 3**, »Allgemeine Systemsicherheit«, behandle ich die grundsätzlichen Aspekte der Systemsicherheit. Die Anmeldesicherheit stellt ein wesentliches Element zur Absicherung dar. Richtig konfiguriert können damit bereits viele Eindringversuche geblockt werden. Themen wie das Notfallkonzept und die Zugriffe auf das Betriebssystem der SAP-Server sind grundlegende Sicherheitsthemen in jedem SAP-System. Weniger beachtet werden häufig die Funktionen von SAP Business Warehouse (SAP BW), die in jedem SAP-NetWeaver-System verfügbar sind. Dies ist abzusichern, um unberechtigte Zugriffe auf sensible Daten zu verhindern.

Die Protokollkomponenten werden in **Kapitel 4**, »Protokollierungskomponenten«, behandelt. Diese stellen eine wesentliche Komponente für Prüfungen dar. Dabei unterscheide ich nach Protokollen, die automatisch vom System erzeugt werden, und

solchen, die explizit aktiviert werden müssen. Zu Letzteren gehören die Tabellenprotokollierung, das Security-Audit-Log und die Lesezugriffsprotokollierung. Die Abschnitte zu diesen Protokollen helfen Ihnen dabei, die Komponenten gesetzes- und unternehmenskonform zu konfigurieren und deren Einsatz zu prüfen. Auch viele kleinere Protokollkomponenten sind sehr hilfreich für Prüfungen, wie die Job- oder SAP-Gateway-Protokolle. Der Abschnitt über SAP Enterprise Threat Detection zeigt Ihnen, wie SAP-Systeme effizient überwacht werden können, um Eindringversuche und Betrugsdelikte zu erkennen.

Die RFC-Sicherheit wird in **Kapitel 5**, »Remote Function Calls«, behandelt. RFC ist ein wesentliches Thema der Systemsicherheit, da eine Vielzahl von Angriffen über diese Schnittstelle erfolgt. Bedingt ist dies u. a. häufig durch eine fehlende Absicherung der RFC-Berechtigungen und der Verbindungen der SAP-Systeme untereinander.

**Kapitel 6**, »Der Verbuchungsvorgang«, behandelt das Thema der Verbuchung. Verbuchung bedeutet, dass Daten konsistent in die Datenbank geschrieben werden. Die Verbuchung kann von vielen Faktoren beeinflusst werden, u. a. durch die Pufferung von Belegnummern, die SAP mit der parallelen Pufferung grundlegend modernisiert hat. Die Absicherung der Verbuchung wird in diesem Kapitel dargestellt.

Ein zentrales Thema der SAP-Sicherheit ist die Benutzerverwaltung, die in **Kapitel 7**, »Benutzerauswertungen«, behandelt wird. Die Absicherung des Benutzerstammsatzes und insbesondere der Initial- und Produktivkennwörter stellt den größten Schutz vor Kennwort-Hacking dar. Die Hacking-Methoden werden ausführlich im Internet dargestellt, weshalb die Absicherung davor elementar für die Sicherheit der Systeme ist. Eine recht neue Funktion ist das datenschutzkonforme Löschen und Sperren von Benutzerstammsätzen. Einen weiteren Schwerpunkt dieses Kapitels bildet die Absicherung der SAP-Standardbenutzer.

Mit dem Customizing, behandelt in **Kapitel 8**, »Customizing des SAP-Systems«, wird das SAP-System an die unternehmenseigenen Geschäftsprozesse angepasst. Customizing bedeutet maßgeblich »Pflege von Tabelleneinträgen«. Zur Prüfung und Absicherung ist es daher hilfreich, mit dem Aufbau des ABAP Dictionary vertraut zu sein. Zentral zu betrachten sind hier die Berechtigungen für den direkten Zugriff auf Tabellen und Views. Mit dem Generic Table Browser gibt es inzwischen die Möglichkeit, den Zugriff auf Tabellen spalten- und zeilenweise einzugrenzen.

**Kapitel 9**, »Entwicklung in SAP-Systemen«, zeigt die Absicherung der Entwicklungsumgebung. Es existiert kein SAP-System, das nicht individuell angepasst wurde, sei es durch eigene Auswertungsreports oder durch die Implementierung komplexer Eigenentwicklungen. Dabei sind Entwicklerrichtlinien ebenso zu beachten wie die speziellen Gefahrenpunkte im Rahmen der ABAP-Programmierung. Da Entwicklung in Entwicklungssystemen stattfindet, bildet auch die Sicherheit des Transportwesens einen Schwerpunkt dieses Kapitels.

Das SAP-Berechtigungskonzept, das ich in **Kapitel 10**, »Berechtigungskonzept in ABAP-Systemen«, behandle, wirkt sich direkt auf alle anderen Sicherheitsthemen aus. Alle sicherheitsrelevanten Vorgänge werden durch Berechtigungen abgesichert. Die Serviceberechtigungen, die in SAP S/4HANA beim Einsatz von SAP-Fiori-Apps genutzt werden, stellen eine neue Ebene für Prüfer\*innen dar. Der konzeptionelle Teil dieser Absicherung ist genauso relevant wie deren technische Umsetzung. Auch können die Berechtigungen durch Customizing-Einstellungen beeinflusst werden. Dieses Kapitel erklärt den Aufbau des Berechtigungskonzepts und den konzeptionellen Teil.

In **Kapitel 11**, »Praktische Prüfung von Berechtigungen«, zeige ich dann konkrete praktische Prüfungen. Neben weiteren Berechtigungen zur Systemsicherheit werden hier auch Customizing-Berechtigungen zu den Komponenten FI, MM und SAP ERP HCM sowie Berechtigungen für SAP Business Warehouse betrachtet.

Die Sicherheit von SAP HANA wird in **Kapitel 12**, »SAP HANA«, behandelt. SAP HANA ist keine reine Datenbank. Hier werden Datenbank- und Applikationsschicht zusammengeführt. Daher sind als Benutzer dort nicht nur Datenbankadministrator\*innen tätig, sondern auch Entwickler\*innen und zukünftig vermehrt Endanwender\*innen. Bei Einsatz von SAP HANA muss daher ein entsprechendes Sicherheitskonzept erstellt werden. Neben Daten- und Kommunikationsverschlüsselungen muss die Authentifizierung abgesichert werden, um direkte Zugriffe auf die Datenbank zu unterbinden. Das Berechtigungskonzept ist hier ebenso wesentlich wie im ABAP-Stack.

### Danksagung

Ich bedanke mich bei allen, die mir bei der Fertigstellung dieses Buches geholfen haben:

- beim Rheinwerk Verlag, der mir auch diese Neuauflage ermöglicht hat,
- bei Maike Lübbers, die das Lektorat übernommen hat,
- bei der IBS Schreiber GmbH für die Nutzung der SAP-Systeme für Recherchen und Screenshots,
- bei meiner Frau Kristin, die das Buch Korrektur gelesen hat

Und zu guter Letzt möchte ich wieder an alle Leserinnen und Leser appellieren, mir jegliche positive und negative Kritik sowie Anregungen für weitere Themen zukommen zu lassen. Schreiben Sie mir gern an [thomas.tiede@ibs-schreiber.de](mailto:thomas.tiede@ibs-schreiber.de).

**Thomas Tiede**

Hamburg im Februar 2021

## Auf einen Blick

1	Umgang mit dem SAP-System und Werkzeuge zur Prüfung .....	31
2	Aufbau von SAP-Systemen und Systemlandschaften .....	125
3	Allgemeine Systemsicherheit .....	175
4	Protokollierungskomponenten .....	249
5	Remote Function Calls .....	365
6	Der Verbuchungsvorgang .....	403
7	Benutzerauswertungen .....	429
8	Customizing des SAP-Systems .....	515
9	Entwicklung in SAP-Systemen .....	587
10	Berechtigungskonzept in ABAP-Systemen .....	687
11	Praktische Prüfung von Berechtigungen .....	797
12	SAP HANA .....	867



# Inhalt

Einleitung .....	25
<b>1 Umgang mit dem SAP-System und Werkzeuge zur Prüfung</b> .....	<b>31</b>
<b>1.1 Transaktionen und SAP-Fiori-Apps</b> .....	<b>31</b>
1.1.1 Transaktionen .....	32
1.1.2 SAP-Fiori-Apps .....	33
<b>1.2 Reports</b> .....	<b>35</b>
1.2.1 Das Konzept der Reports .....	35
1.2.2 Aufrufen von Reports .....	37
1.2.3 Exportieren der Reportergebnisse .....	39
1.2.4 Festlegung des Standardpfads zum Speichern .....	41
1.2.5 Speichern der Selektionsangaben (Varianten) .....	41
<b>1.3 Anzeigen von Tabellen</b> .....	<b>43</b>
1.3.1 Anzeigetransaktionen für Tabellen .....	43
1.3.2 Transaktion SE16 .....	45
1.3.3 Transaktionen SE16N, S416N, S4H16N .....	48
1.3.4 Transaktionen SE16H, S416H, S4H16H .....	48
1.3.5 Transaktionen SE16S, S416S und S4H16S .....	51
1.3.6 Suchen von Tabellen .....	53
1.3.7 Exportieren von Tabellen .....	57
1.3.8 Speichern der Selektionsangaben (Varianten) .....	58
<b>1.4 Das Benutzerinformationssystem</b> .....	<b>59</b>
<b>1.5 Listen als PDF-Datei speichern</b> .....	<b>62</b>
<b>1.6 Nutzung der Zugriffsstatistik für Prüfungen</b> .....	<b>63</b>
1.6.1 Funktionsweise .....	63
1.6.2 Analyse von aufgerufenen Transaktionen und Reports .....	66
1.6.3 Analyse von RFC-Aufrufen .....	69
<b>1.7 Tabelleninhalte mit dem QuickViewer auswerten</b> .....	<b>71</b>
1.7.1 Erstellen eines QuickViews auf eine einzelne Tabelle .....	72
1.7.2 Erstellen eines QuickViews mit einem Tabellen-Join .....	76
1.7.3 Erstellen eines QuickViews mit einer logischen Datenbank .....	79

<b>1.8 SQL-Trace</b> .....	80
1.8.1 Aktivierung des SQL-Trace .....	81
1.8.2 Auswertung des Trace .....	82
<b>1.9 Audit Information System</b> .....	84
1.9.1 Die Auditstruktur .....	85
1.9.2 Durchführen eines Audits .....	87
1.9.3 Berechtigungen zur Nutzung des Audit Information Systems .....	89
<b>1.10 SAP Access Control</b> .....	90
1.10.1 Komponenten von SAP Access Control .....	90
1.10.2 Regelwerke .....	91
1.10.3 Auswertung der Regelwerke .....	96
1.10.4 SAP-Access-Control-Regelwerk für dieses Buch .....	102
<b>1.11 SAP Enterprise Threat Detection</b> .....	103
1.11.1 Angriffe auf SAP-Systeme – nur etwas für versierte Hacker? .....	104
1.11.2 Standardüberwachung von SAP-Systemen .....	105
1.11.3 Zentrale Sammlung von Protokollen in SAP Enterprise Threat Detection .....	107
1.11.4 Automatisierte Analyse von Protokollen in SAP Enterprise Threat Detection .....	108
1.11.5 Pseudonymisierung von Benutzernamen .....	111
1.11.6 Auswertung eingespielter Security Notes .....	113
<b>1.12 Zugriff auf SAP HANA für Prüfer</b> .....	115
1.12.1 Zugriff auf SAP HANA über das DBA Cockpit .....	115
1.12.2 Zugriff auf SAP HANA über das SAP HANA Cockpit .....	118
1.12.3 Skriptgesteuerter Export von Daten aus der SAP-HANA-Datenbank .....	123

## **2 Aufbau von SAP-Systemen und Systemlandschaften** 125

---

<b>2.1 SAP NetWeaver und SAP-Komponenten</b> .....	125
2.1.1 Komponenten von SAP NetWeaver .....	126
2.1.2 Komponenten der SAP Business Suite .....	127
2.1.3 Komponenten von SAP S/4HANA .....	128
2.1.4 Nicht mehr unterstützte Komponenten in SAP S/4HANA .....	129
2.1.5 Checkliste .....	131

<b>2.2 Technischer Aufbau von SAP-Systemen</b> .....	131
2.2.1 Applikations- und Datenbankserver .....	131
2.2.2 SAP-Fiori-Frontend-Server und SAP-Backend-System .....	133
2.2.3 Instanzen .....	134
2.2.4 SAP-Prozesse und -Dienste .....	135
2.2.5 Checkliste .....	138
<b>2.3 Systemlandschaften</b> .....	139
2.3.1 Drei-System-Landschaften .....	139
2.3.2 SAP-Fiori-Systemlandschaften .....	141
2.3.3 Systemarten .....	143
2.3.4 Checkliste .....	144
<b>2.4 Das Mandantenkonzept</b> .....	145
2.4.1 Standardmandanten eines SAP-Systems .....	146
2.4.2 Eigenschaften von Mandanten .....	147
2.4.3 Protokollierung der Änderungen von Mandanteneigenschaften .....	150
2.4.4 Risiko beim Anlegen neuer Mandanten .....	151
2.4.5 Mandantenkopien .....	153
2.4.6 Zugriffsrechte .....	156
2.4.7 Checkliste .....	162
<b>2.5 Sicherheit im Mandanten 000</b> .....	163
2.5.1 Zugriff auf Daten des Produktivmandanten .....	164
2.5.2 Systemeinstellungen pflegen .....	170
2.5.3 Anwendungsentwicklung .....	172
2.5.4 Gesetzeskritische Berechtigungen .....	173
2.5.5 Patterns in SAP Enterprise Threat Detection .....	173
2.5.6 Checkliste .....	173

## **3 Allgemeine Systemsicherheit** 175

---

<b>3.1 Grundlagen für die Prüfung der Systemsicherheit</b> .....	175
3.1.1 Der Releasestand des SAP-Systems .....	176
3.1.2 Systemparameter .....	177
3.1.3 Zugriffsrechte .....	181
3.1.4 Checkliste .....	182
<b>3.2 Anmeldesicherheit</b> .....	183
3.2.1 Unzulässige Kennwörter – Tabelle USR40 .....	184
3.2.2 Protokolle von Mehrfachanmeldungen .....	185
3.2.3 Systemparameter zur Anmeldesicherheit .....	186

3.2.4	Sicherheitsrichtlinien .....	195
3.2.5	Schutz vor Kennwort-Hacking .....	199
3.2.6	Unternehmenseigene Erweiterungen zur Anmeldesicherheit .....	200
3.2.7	Patterns in SAP Enterprise Threat Detection .....	201
3.2.8	Zugriffsrechte .....	201
3.2.9	Checkliste .....	204
<b>3.3</b>	<b>Das Notfallbenutzerkonzept .....</b>	<b>206</b>
3.3.1	Konzept für Notfallbenutzer .....	206
3.3.2	Transaktion SE16N_EMERGENCY .....	207
3.3.3	Checkliste .....	209
<b>3.4</b>	<b>Sperren von Transaktionscodes .....</b>	<b>210</b>
3.4.1	Zugriffsrechte .....	212
3.4.2	Checkliste .....	213
<b>3.5</b>	<b>Logische Betriebssystemkommandos .....</b>	<b>214</b>
3.5.1	Funktionsweise .....	214
3.5.2	Der Report RSBDCOS0 .....	218
3.5.3	Logische Betriebssystemkommandos zur Prüfung nutzen .....	219
3.5.4	Patterns in SAP Enterprise Threat Detection .....	220
3.5.5	Zugriffsrechte .....	220
3.5.6	Checkliste .....	222
<b>3.6</b>	<b>Drucken und Speichern .....</b>	<b>223</b>
3.6.1	Der Druckvorgang .....	223
3.6.2	Schutz von Druckaufträgen .....	228
3.6.3	Speichern von Daten in Dateien .....	228
3.6.4	Patterns in SAP Enterprise Threat Detection .....	229
3.6.5	Zugriffsrechte .....	229
3.6.6	Checkliste .....	230
<b>3.7</b>	<b>Batch-Input .....</b>	<b>232</b>
3.7.1	Analyse des Batch-Input-Verfahrens .....	233
3.7.2	Berechtigungen für Batch-Input-Mappen .....	236
3.7.3	Zugriffsrechte .....	238
3.7.4	Checkliste .....	240
<b>3.8</b>	<b>Funktionen von SAP Business Warehouse .....</b>	<b>241</b>
3.8.1	Datenextraktion .....	242
3.8.2	Der Extraktorchecker .....	242
3.8.3	Berechtigungen für die Extraktion einschränken .....	245
3.8.4	Zugriffsrechte .....	246
3.8.5	Checkliste .....	247

<b>4</b>	<b>Protokollierungskomponenten .....</b>	<b>249</b>
<b>4.1</b>	<b>Security-Audit-Log .....</b>	<b>249</b>
4.1.1	Konfiguration des Security-Audit-Logs .....	251
4.1.2	Auswertung des Security-Audit-Logs .....	258
4.1.3	Pseudonymisierte Auswertung des Security-Audit-Logs .....	259
4.1.4	Löschen von Security-Audit-Log-Protokollen .....	261
4.1.5	Konzept zum Einsatz des Security-Audit-Logs .....	262
4.1.6	Zugriffsrechte .....	266
4.1.7	Checkliste .....	270
<b>4.2</b>	<b>Systemprotokollierung .....</b>	<b>271</b>
4.2.1	Auswertung des SysLogs .....	272
4.2.2	Meldungen des SysLogs .....	274
4.2.3	Zugriffsrechte .....	277
4.2.4	Checkliste .....	277
<b>4.3</b>	<b>Protokollierung von Tabellenänderungen .....</b>	<b>278</b>
4.3.1	Aktivierung der Tabellenprotokollierung .....	279
4.3.2	Protokollierung bei Transporten .....	281
4.3.3	Protokollierung der einzelnen Tabellen .....	283
4.3.4	Versionierung der Protokolleigenschaft von Tabellen .....	288
4.3.5	Protokollierung unternehmenseigener Tabellen .....	291
4.3.6	Auswertung von Tabellenänderungen .....	295
4.3.7	Löschen von Tabellenänderungsprotokollen .....	299
4.3.8	Zugriffsrechte .....	300
4.3.9	Checkliste .....	302
<b>4.4</b>	<b>Protokollierung über Änderungsbelege .....</b>	<b>304</b>
4.4.1	Suchen von über Änderungsbelege protokollierten Tabellen .....	307
4.4.2	Residenzzeiten für Änderungsbelege .....	308
4.4.3	Auswertung der Änderungsbelege .....	309
4.4.4	Löschen von Änderungsbelegen .....	310
4.4.5	Ändern von Änderungsbelegobjekten .....	311
4.4.6	Zugriffsrechte .....	311
4.4.7	Checkliste .....	313
<b>4.5</b>	<b>Versionsverwaltung .....</b>	<b>313</b>
4.5.1	Anzeige der Versionen zu einzelnen Programmen .....	314
4.5.2	Anzeige der Versionen aller versionierbaren Objekte .....	316
4.5.3	Versionserzeugung bei Importen .....	317

4.5.4	Löschen der Versionshistorien .....	318
4.5.5	Checkliste .....	319
<b>4.6</b>	<b>Lesezugriffsprotokollierung .....</b>	<b>320</b>
4.6.1	Protokollierung des Zugriffs auf sensible Felder .....	321
4.6.2	Protokollierung des Aufrufs von Funktionsbausteinen .....	324
4.6.3	Konfigurationseinstellungen .....	326
4.6.4	Verwaltungsprotokoll .....	326
4.6.5	Zugriffsrechte .....	327
4.6.6	Checkliste .....	330
<b>4.7</b>	<b>Zugriffsstatistik .....</b>	<b>331</b>
4.7.1	Analyse einzelner Benutzer oder Funktionen .....	333
4.7.2	Analyse von Transaktionsaufrufen in Listenform .....	335
4.7.3	Analyse von RFC-Zugriffen .....	335
4.7.4	Langzeitauswertung der Statistik .....	336
4.7.5	Anonymisierte Auswertung von Statistiksätzen .....	340
4.7.6	Zugriffsrechte .....	340
4.7.7	Checkliste .....	341
<b>4.8</b>	<b>Weitere Protokollkomponenten .....</b>	<b>342</b>
4.8.1	Protokolle für die Systemänderbarkeit .....	342
4.8.2	Protokolle von Mandantenkopien .....	344
4.8.3	Protokolle von Änderungen an Systemparametern .....	344
4.8.4	Protokolle von Mehrfachanmeldungen .....	345
4.8.5	Protokolle von Änderungen an Betriebssystemkommandos .....	345
4.8.6	Jobprotokolle .....	345
4.8.7	Protokolle von Änderungen über Transaktion SE16N .....	346
4.8.8	Protokolle von Änderungen über den Generic Table Browser (GTB) .....	347
4.8.9	Protokolle von Änderungen an Sicherheitsrichtlinien .....	348
4.8.10	SAP Gateway – Fehlerprotokolle .....	348
4.8.11	Generische Auditauswertungen (Transaktion SAIS_MONI) .....	349
<b>4.9</b>	<b>Systemüberwachung mit SAP Enterprise Threat Detection .....</b>	<b>351</b>
4.9.1	Übertragung der Protokolle an SAP Enterprise Threat Detection .....	351
4.9.2	Auswahl der Patterns in SAP Enterprise Threat Detection .....	354
4.9.3	Definition eigener Patterns .....	355
4.9.4	Analyse mit SAP Enterprise Threat Detection .....	356
4.9.5	Zugriffsrechte .....	360
4.9.6	Checkliste .....	363

<b>5</b>	<b>Remote Function Calls .....</b>	<b>365</b>
<b>5.1</b>	<b>Funktionsbausteine .....</b>	<b>365</b>
5.1.1	Funktionsbausteine ohne Berechtigungsprüfungen .....	368
5.1.2	Funktionsbausteine mit schaltbaren Berechtigungen .....	369
5.1.3	Protokollierung von RFC-Aktionen .....	371
5.1.4	Patterns in SAP Enterprise Threat Detection .....	373
5.1.5	Zugriffsrechte .....	374
5.1.6	Checkliste .....	375
<b>5.2</b>	<b>RFC-Verbindungen .....</b>	<b>376</b>
5.2.1	Hinterlegte Kennwörter .....	379
5.2.2	Systemübergreifender Zugriff über Funktionsbausteine .....	380
5.2.3	Zugriffsrechte .....	382
5.2.4	Checkliste .....	382
<b>5.3</b>	<b>Trusted Systems .....</b>	<b>383</b>
5.3.1	Berechtigungen zur Nutzung von Trusted-Verbindungen .....	387
5.3.2	Zugriffsrechte .....	389
5.3.3	Checkliste .....	390
<b>5.4</b>	<b>Zugriff von externen Programmen .....</b>	<b>391</b>
5.4.1	Ermittlung der erforderlichen RFC-Berechtigungen .....	394
5.4.2	Zugriff auf das SAP-System über Microsoft Excel .....	395
5.4.3	ABAP-Quelltexte über RFC ausführen .....	397
5.4.4	Zugriffsrechte .....	399
5.4.5	Checkliste .....	400
<b>6</b>	<b>Der Verbuchungsvorgang .....</b>	<b>403</b>
<b>6.1</b>	<b>Das Prinzip der Verbuchung .....</b>	<b>403</b>
6.1.1	Die Verbuchungskomponenten .....	405
6.1.2	Auswertung der Verbuchung .....	407
6.1.3	Zugriffsrechte .....	412
6.1.4	Checkliste .....	413
<b>6.2</b>	<b>Abgebrochene Buchungen .....</b>	<b>414</b>
6.2.1	Kontrolle auf abgebrochene Buchungen .....	414
6.2.2	Die Abstimmanalyse der Finanzbuchhaltung (SAP ERP) .....	415
6.2.3	Zugriffsrechte .....	418
6.2.4	Checkliste .....	418

<b>6.3 Die Belegnummernvergabe</b>	419
6.3.1 Nummernkreisobjekte	420
6.3.2 Pufferung von Belegnummern	421
6.3.3 Suche nach Lücken in Belegnummern	425
6.3.4 Zugriffsrechte	426
6.3.5 Checkliste	426
<b>7 Benutzerauswertungen</b>	429
<b>7.1 Organisatorische Regelungen</b>	429
<b>7.2 Die SAP-Standardbenutzer</b>	433
7.2.1 Der Benutzer SAP*	434
7.2.2 Der Benutzer DDIC	435
7.2.3 Der Benutzer SAPCPIC	435
7.2.4 Der Benutzer TMSADM	435
7.2.5 Der Benutzer EARLYWATCH	436
7.2.6 Prüfen der Standardbenutzer	436
7.2.7 Weitere Standardbenutzer	438
7.2.8 Patterns in SAP Enterprise Threat Detection	439
7.2.9 Zugriffsrechte	439
7.2.10 Checkliste	441
<b>7.3 Der Benutzerstammsatz</b>	442
7.3.1 Benutzertypen	442
7.3.2 Eigenschaften der Benutzer	446
7.3.3 Auswertungen zu Benutzern	455
7.3.4 Patterns in SAP Enterprise Threat Detection	457
7.3.5 Zugriffsrechte	458
7.3.6 Checkliste	458
<b>7.4 Referenzbenutzer</b>	459
7.4.1 Zuordnung von Referenzbenutzern	459
7.4.2 Auswertung von Referenzbenutzerzuordnungen	460
7.4.3 Historie der Referenzbenutzerzuordnungen	461
7.4.4 Patterns in SAP Enterprise Threat Detection	462
7.4.5 Zugriffsrechte	462
7.4.6 Checkliste	464
<b>7.5 Benutzergruppen</b>	465
7.5.1 Patterns in SAP Enterprise Threat Detection	468

7.5.2 Zugriffsrechte	469
7.5.3 Checkliste	470
<b>7.6 Sammelbenutzer</b>	471
<b>7.7 Benutzervermessungsdaten</b>	474
7.7.1 Konfiguration der Vermessung	474
7.7.2 Prüfen der Systemvermessung	477
7.7.3 Zugriffsrechte	479
7.7.4 Checkliste	480
<b>7.8 Initialkennwörter und Benutzersperrungen</b>	480
7.8.1 Initialkennwörter	481
7.8.2 Produktivkennwörter	483
7.8.3 Benutzersperrungen	484
7.8.4 Auswertung gesperrter Benutzer	487
7.8.5 Patterns in SAP Enterprise Threat Detection	488
7.8.6 Zugriffsrechte	489
7.8.7 Checkliste	491
<b>7.9 Benutzerstammsätze sperren und löschen</b>	492
7.9.1 Funktionsweise	493
7.9.2 Wiederanlage von Benutzer	494
7.9.3 Vetoprüfungen beim Löschen von Benutzern	495
7.9.4 Zugriffsrechte	497
7.9.5 Checkliste	498
<b>7.10 Kennwortverschlüsselung</b>	499
7.10.1 Verschlüsselungsalgorithmen	499
7.10.2 Schutz vor Hacking der Kennwörter	501
7.10.3 Patterns in SAP Enterprise Threat Detection	501
7.10.4 Zugriffsrechte	503
7.10.5 Checkliste	504
<b>7.11 Angemeldete Benutzer</b>	505
7.11.1 Informationen zu angemeldeten Benutzern – Transaktion AL08	505
7.11.2 Informationen zu den Benutzer-Terminals – Tabelle USR41	506
7.11.3 Administrative Überwachung – Transaktion SM04	507
7.11.4 Protokollierung von Benutzeranmeldungen – Security-Audit-Log	507
7.11.5 Patterns in SAP Enterprise Threat Detection	508
7.11.6 Zugriffsrechte	508
7.11.7 Checkliste	509
<b>7.12 Die Änderungshistorie zu Benutzern</b>	509
7.12.1 Zugriffsrechte	512
7.12.2 Checkliste	512

<b>8</b>	<b>Customizing des SAP-Systems</b>	515
<b>8.1</b>	<b>Das ABAP Dictionary</b>	515
8.1.1	Aufbau des ABAP Dictionarys	516
8.1.2	Domänen	518
8.1.3	Datenelemente	522
8.1.4	Zugriffsrechte	524
8.1.5	Checkliste	525
<b>8.2</b>	<b>Das Konzept der Tabellensteuerung</b>	526
8.2.1	Eigenschaften von Tabellen	526
8.2.2	Mandantenabhängige Tabellen	529
8.2.3	Mandantenunabhängige Tabellen	530
8.2.4	Transparente Tabellen	531
8.2.5	Dokumentationen zu Tabellen	532
8.2.6	ABAP-Dictionary-Views	533
8.2.7	ABAP-CDS-Views	538
8.2.8	Unternehmenseigene Tabellen und Views	541
8.2.9	Zugriffsrechte	542
8.2.10	Checkliste	545
<b>8.3</b>	<b>Zugriffe auf Tabellen</b>	546
8.3.1	Anzeige von Tabelleninhalten in der Datenbank	546
8.3.2	Ändern von Tabellen im SAP-System	549
8.3.3	Einführungsleitfaden	551
8.3.4	Laufende Einstellungen	553
8.3.5	Patterns in SAP Enterprise Threat Detection	555
8.3.6	Zugriffsrechte	555
8.3.7	Checkliste	557
<b>8.4</b>	<b>Berechtigungen für Tabellen und Views</b>	558
8.4.1	Berechtigungsgruppen	558
8.4.2	Berechtigungsobjekte	560
8.4.3	Schutz von Tabellen ohne Berechtigungsgruppe	566
8.4.4	Prüfen der Berechtigungen zum Zugriff auf einzelne Tabellen/Views	567
8.4.5	Prüfung der Tabellenberechtigungen für einzelne Rollen oder Benutzer	568
8.4.6	Abgleich von Tabellenberechtigungsgruppen	570
8.4.7	Zugriffsrechte	570
8.4.8	Checkliste	573

<b>8.5</b>	<b>Tabellenzugriffe auf Spalten und Feldwerte einschränken (GTB-Rollen)</b>	574
8.5.1	Berechtigungen auf Spalten eingrenzen	575
8.5.2	Berechtigungen auf Feldwerte eingrenzen	577
8.5.3	Zuordnung der GTB-Rollen	578
8.5.4	Prüfung der GTB-Rollen	579
8.5.5	Voraussetzungen zur Nutzung von GTB-Rollen	582
8.5.6	Zugriffsrechte	583
8.5.7	Checkliste	584
<b>9</b>	<b>Entwicklung in SAP-Systemen</b>	587
<b>9.1</b>	<b>Entwicklerrichtlinien</b>	587
<b>9.2</b>	<b>Entwickler- und Objektschlüssel</b>	590
9.2.1	Entwickler- und Objektschlüssel in SAP S/4HANA	590
9.2.2	Entwicklerschlüssel	591
9.2.3	Objektschlüssel	594
9.2.4	Umgehung der Abfrage von Entwickler- und Objektschlüsseln	594
9.2.5	Zugriffsrechte	596
9.2.6	Checkliste	596
<b>9.3</b>	<b>Systemänderbarkeit</b>	598
9.3.1	Prüfung der Systemänderbarkeit	599
9.3.2	Zugriffsrechte	602
9.3.3	Checkliste	603
<b>9.4</b>	<b>Das Transportsystem</b>	604
9.4.1	Der Transport Organizer	604
9.4.2	Transport Management System	612
9.4.3	Der Ablauf eines Transports	618
9.4.4	Zeitnähe der Importe	621
9.4.5	Zugriffsrechte	623
9.4.6	Checkliste	627
<b>9.5</b>	<b>Eigenentwicklungen in ABAP</b>	629
9.5.1	Die Programmiersprache ABAP	630
9.5.2	ABAP-Namensräume	635
9.5.3	Gefahrenpunkte in der ABAP-Programmentwicklung	636
9.5.4	Prüfen der Eigenschaften von ABAP-Programmen	652
9.5.5	Inhaltliches Prüfen einzelner ABAP-Programme	653

9.5.6	Programmübergreifende Analyse von Quelltexten .....	654
9.5.7	Code Inspector .....	660
9.5.8	Code Vulnerability Analyzer .....	663
9.5.9	Die Versionshistorie .....	665
9.5.10	Patterns in SAP Enterprise Threat Detection .....	665
9.5.11	Checkliste .....	665
<b>9.6</b>	<b>Transaktionen .....</b>	<b>667</b>
9.6.1	Transaktionsarten .....	668
9.6.2	Pflege von Transaktionen .....	669
9.6.3	Protokollierung von Änderungen an Tabellen .....	670
9.6.4	Suche nach verwandten Transaktionen .....	671
9.6.5	Suche nach Transaktionen mit generischem Tabellenzugriff .....	672
9.6.6	Zugriffsrechte .....	674
9.6.7	Checkliste .....	674
<b>9.7</b>	<b>Berechtigungen zur Anwendungsentwicklung .....</b>	<b>675</b>
9.7.1	Das Berechtigungsobjekt S_DEVELOP .....	675
9.7.2	Weitere Berechtigungsobjekte zur Anwendungsentwicklung .....	677
9.7.3	Schutz von ABAP-Programmen durch Berechtigungsgruppen (S_PROGRAM) .....	678
9.7.4	Schutz von ABAP-Programmen nach Namen (S_PROGNAM) .....	682
9.7.5	Zugriffsrechte – Einzelberechtigungen .....	683
9.7.6	Zugriffsrechte – Funktionstrennungen .....	684
9.7.7	Patterns in SAP Enterprise Threat Detection .....	686
<b>10</b>	<b>Berechtigungskonzept in ABAP-Systemen .....</b>	<b>687</b>
<b>10.1</b>	<b>Funktionsweise des Berechtigungskonzepts .....</b>	<b>688</b>
10.1.1	Berechtigungsobjekte .....	689
10.1.2	Rollen .....	696
10.1.3	Sammelrollen .....	702
10.1.4	Profile .....	704
10.1.5	Berechtigungen .....	707
10.1.6	Ablauf einer Berechtigungsprüfung .....	709
10.1.7	Patterns in SAP Enterprise Threat Detection .....	711
10.1.8	Checkliste .....	711
<b>10.2</b>	<b>Das Berechtigungskonzept in SAP S/4HANA .....</b>	<b>712</b>
10.2.1	Simplification List for SAP S/4HANA .....	713
10.2.2	SAP Fiori Apps Reference Library .....	714
10.2.3	Das Konzept der SAP-Fiori-Apps .....	717

10.2.4	Kachelgruppen und -kataloge .....	719
10.2.5	Berechtigungen auf dem Frontend-Server .....	722
10.2.6	Berechtigungen auf dem Backend-Server .....	724
10.2.7	Auswertung von App-Berechtigungen für Benutzer .....	726
10.2.8	Auswertung von App-Berechtigungen in Rollen .....	727
10.2.9	Zugriffsrechte .....	729
10.2.10	Checkliste .....	731
<b>10.3</b>	<b>Konzepte zum SAP-Berechtigungswesen .....</b>	<b>731</b>
10.3.1	Das Dateneigentümerkonzept .....	732
10.3.2	Das Antrags-, Test- und Freigabeverfahren .....	734
10.3.3	Der Ablauf der Benutzerverwaltung .....	738
10.3.4	Konzept für übergreifende Berechtigungen .....	739
10.3.5	Das interne Kontrollsystem .....	739
10.3.6	Namenskonventionen für Rollen .....	741
10.3.7	Konventionen für die technische Rollenausprägung .....	742
10.3.8	Rollenkonzepte .....	743
10.3.9	Pflege von Kachelgruppen und -katalogen .....	744
10.3.10	Komponenten- und systemspezifische Teilkonzepte .....	745
10.3.11	Berechtigungen in Eigenentwicklungen .....	745
10.3.12	Sicherheitskonzept zum Berechtigungskonzept .....	746
10.3.13	Checkliste .....	747
<b>10.4</b>	<b>Customizing zum Berechtigungskonzept .....</b>	<b>750</b>
10.4.1	Systemparameter .....	750
10.4.2	Benutzermenüs .....	753
10.4.3	Customizing-Schalter in Tabelle PRGN_CUST .....	755
10.4.4	Deaktivierte Berechtigungsobjekte .....	757
10.4.5	Deaktivierung von einzelnen Berechtigungsprüfungen .....	759
10.4.6	Transaktionsaufrufe durch CALL TRANSACTION .....	761
10.4.7	Zugriffsrechte .....	763
10.4.8	Checkliste .....	766
<b>10.5</b>	<b>Prüfung von Zugriffsrechten .....</b>	<b>768</b>
10.5.1	Referenzbenutzer .....	769
10.5.2	Kritische Standardprofile .....	769
10.5.3	Berechtigungsobjekte zu startbaren Anwendungen suchen .....	774
10.5.4	Zugriffsrechte für Benutzer auswerten .....	775
10.5.5	Zugriffsrechte für Rollen auswerten .....	782
10.5.6	Patterns in SAP Enterprise Threat Detection .....	786
<b>10.6</b>	<b>Trace von Benutzerberechtigungen .....</b>	<b>787</b>
10.6.1	Transaktion SU53 .....	787
10.6.2	Der Berechtigungs-Trace .....	788

10.6.3	Der Benutzer-Langzeit-Trace .....	790
10.6.4	Übernahme von Trace-Ergebnissen in eine Rolle .....	792
<b>10.7</b>	<b>Berechtigungen für Prüfer .....</b>	<b>794</b>
<b>11</b>	<b>Praktische Prüfung von Berechtigungen .....</b>	<b>797</b>
<b>11.1</b>	<b>Zugriffsrechte im Bereich der Berechtigungsverwaltung .....</b>	<b>797</b>
11.1.1	Zugriffsrechte zur Benutzerverwaltung .....	798
11.1.2	Zugriffsrechte zur Rollenverwaltung .....	803
11.1.3	Zugriffsrechte zu Profilen .....	804
11.1.4	Zugriffsrechte für Kachelkataloge und -gruppen .....	805
<b>11.2</b>	<b>Gesetzeskritische Berechtigungen .....</b>	<b>805</b>
<b>11.3</b>	<b>Kritische Basisberechtigungen .....</b>	<b>808</b>
11.3.1	Löschen von Sperreinträgen anderer Benutzer .....	808
11.3.2	Administration der Sperrverwaltung .....	808
11.3.3	LDAP-Zugriffe .....	809
11.3.4	Verwaltung der Ein- und Ausgabe-Queue .....	809
11.3.5	Administration der Datenarchivierung .....	810
11.3.6	Löschen von laufenden Prozessen .....	810
11.3.7	Verwaltung der TemSe-Dateien .....	811
11.3.8	Anlegen von Jobs unter anderem Benutzernamen .....	811
11.3.9	Verwaltung der Hintergrundjobs .....	812
11.3.10	Zurücksetzen und Löschen von Daten ohne Archivierung .....	812
11.3.11	Kopieren von Dateien vom SAP-Server auf den Client .....	813
11.3.12	Kopieren von Dateien vom Client auf den SAP-Server .....	814
<b>11.4</b>	<b>Berechtigungen für das Hacking von SAP-Systemen .....</b>	<b>815</b>
11.4.1	Datendiebstahl .....	815
11.4.2	Datenmanipulation .....	816
11.4.3	Password-Cracking .....	818
11.4.4	Verschleierung von Aktionen .....	820
11.4.5	Code-Insert .....	821
<b>11.5</b>	<b>Customizing-Berechtigungen .....</b>	<b>824</b>
11.5.1	Transaktionen zur Tabellen- und Viewpflege .....	824
11.5.2	Customizing im Finanzwesen .....	826
11.5.3	Customizing in der Materialwirtschaft .....	834
11.5.4	Customizing in SAP ERP HCM .....	836

<b>11.6</b>	<b>Analyse der Qualität des Berechtigungskonzepts .....</b>	<b>838</b>
11.6.1	Manuelle Berechtigungen .....	839
11.6.2	Manuell gepflegte Organisationsebenen .....	841
11.6.3	Offene Organisationsebenen in Rollen .....	844
11.6.4	Offene Berechtigungen in Rollen .....	845
11.6.5	Sternberechtigungen in Berechtigungswerten .....	846
11.6.6	Fehlende Pflege der Berechtigungen in Transaktion SU24 für kundeneigene Transaktionen .....	847
11.6.7	Quantitative Auswertungen zu Rollen und Rollenzuordnungen .....	848
<b>11.7</b>	<b>Analyse von Berechtigungen in SAP Business Warehouse .....</b>	<b>850</b>
11.7.1	Administrative Berechtigungen .....	850
11.7.2	Berechtigungen für PSA-Tabellen .....	853
11.7.3	Testen der Berechtigungen anderer Benutzer .....	855
11.7.4	Berechtigungen zur Datenmodellierung .....	856
11.7.5	Verwaltung von Analyseberechtigungen .....	860
11.7.6	Reportingberechtigungen .....	863
<b>12</b>	<b>SAP HANA .....</b>	<b>867</b>
<b>12.1</b>	<b>Einführung in SAP HANA .....</b>	<b>867</b>
12.1.1	Der Systemtyp einer SAP-HANA-Datenbank .....	868
12.1.2	Schemata .....	868
12.1.3	Zugriff auf Daten in der SAP-HANA-Datenbank .....	870
12.1.4	Entwicklungsumgebung SAP HANA XS (Repository) .....	873
12.1.5	Entwicklungsumgebung SAP HANA XSA .....	874
12.1.6	Aufruf von Tabellen und Views .....	875
12.1.7	Zugriff auf Daten in der SAP-HANA-Datenbank .....	875
<b>12.2</b>	<b>Systemsicherheit in SAP HANA .....</b>	<b>876</b>
12.2.1	Tenant-Datenbanken .....	876
12.2.2	Systemparameter .....	878
12.2.3	Verschlüsselung von Daten .....	882
12.2.4	Verschlüsselung der Kommunikation .....	885
12.2.5	Verbindungen zu anderen Systemen – Remote Sources .....	886
12.2.6	Checkliste .....	888
<b>12.3</b>	<b>Anmeldesicherheit .....</b>	<b>891</b>
12.3.1	Authentifizierungsmethoden .....	891
12.3.2	Systemparameter für Kennwortrichtlinien .....	892
12.3.3	Benutzergruppenspezifische Kennwortrichtlinien .....	895



12.3.4	Liste der verbotenen Kennwörter .....	896
12.3.5	Checkliste .....	897
<b>12.4</b>	<b>Benutzerverwaltung in SAP HANA .....</b>	<b>898</b>
12.4.1	Der Benutzerstammsatz .....	898
12.4.2	Restricted User (Eingeschränkte Benutzer) .....	901
12.4.3	Standardbenutzer in SAP HANA .....	903
12.4.4	Remotebenutzer .....	907
12.4.5	Benutzergruppen .....	909
12.4.6	Checkliste .....	910
<b>12.5</b>	<b>SAP HANA XSA .....</b>	<b>912</b>
12.5.1	Struktur in SAP HANA XSA .....	913
12.5.2	SAP HANA XSA Cockpit .....	914
12.5.3	SAP Web IDE .....	914
12.5.4	Benutzer in SAP HANA XSA .....	915
12.5.5	Berechtigungen in SAP HANA XSA .....	917
12.5.6	Checkliste .....	923
<b>12.6</b>	<b>Das Berechtigungskonzept von SAP HANA .....</b>	<b>924</b>
12.6.1	Berechtigungen in SAP HANA .....	924
12.6.2	System Privileges (Systemberechtigungen) .....	925
12.6.3	Object Privileges (Objektberechtigungen) .....	928
12.6.4	Package Privileges (Paketberechtigungen) .....	930
12.6.5	Analytic Privileges (Analyseberechtigungen) .....	933
12.6.6	Application Privileges (Anwendungsberechtigungen) .....	934
12.6.7	Privileges on Users (Debugging des eigenen Benutzers zulassen) .....	935
12.6.8	Weitergabe von Berechtigungen .....	936
12.6.9	Checkliste .....	937
<b>12.7</b>	<b>Das Rollenkonzept von SAP HANA .....</b>	<b>939</b>
12.7.1	Eigenschaften von Rollen .....	939
12.7.2	Runtime-Katalogrollen .....	941
12.7.3	Design-Time-Repository-Rollen in SAP HANA XS .....	942
12.7.4	Design-Time-HDI-Rollen in SAP HANA XSA .....	945
12.7.5	Standardrollen in SAP HANA .....	945
12.7.6	Checkliste .....	948
<b>12.8</b>	<b>Analyse des SAP-HANA-Berechtigungskonzepts .....</b>	<b>950</b>
12.8.1	Tabellen und Views zur Analyse von Berechtigungen .....	951
12.8.2	Benutzerauswertungen .....	951
12.8.3	Welche Berechtigungen haben einzelne Benutzer (View EFFECTIVE_PRIVILEGES)? .....	954
12.8.4	Welchen Benutzern und Rollen sind bestimmte Berechtigungen zugeordnet (View EFFECTIVE_PRIVILEGE_GRANTEES)? .....	956

12.8.5	Welche Rollen sind einem Benutzer oder einer Rolle zugeordnet (View EFFECTIVE_ROLES)? .....	958
12.8.6	Welchen Benutzern und Rollen sind bestimmte Rollen zugeordnet (View EFFECTIVE_ROLE_GRANTEES)? .....	959
12.8.7	Das Skript HANA_Security_GrantedRolesAndPrivileges .....	960
12.8.8	Checkliste .....	962
<b>12.9</b>	<b>Auditing in SAP HANA .....</b>	<b>963</b>
12.9.1	Konfiguration des Auditings in SAP HANA .....	963
12.9.2	Einrichten von Policies .....	966
12.9.3	Auswertung der eingerichteten Policies .....	971
12.9.4	Auswertung des Auditings .....	972
12.9.5	Löschen von Auditing-Protokollen .....	975
12.9.6	Konzept zur Auswertung .....	975
12.9.7	Checkliste .....	975

## Anhang

979

<b>A</b>	<b>Leitfäden zur SAP-Systemsicherheit .....</b>	<b>979</b>
<b>B</b>	<b>Glossar .....</b>	<b>981</b>

Der Autor .....	989
Index .....	991