



SAP AG
Neurottstr. 16
D-69190 Walldorf

R/3-Sicherheit

R/3-Sicherheitsleitfaden: BAND I

R/3-Sicherheitservices im Überblick

Version 2.0a: Deutsch

6. Juli 1999

Copyright

©Copyright 1999 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Dokumentation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Dokumentation enthaltene Informationen können ohne vorherige Ankündigung geändert und ergänzt werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehäuser enthalten.

Microsoft®, WINDOWS®, EXCEL®, NT® und SQL-Server® sind eingetragene Warenzeichen von Microsoft Corporation.

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® und AS/400® sind eingetragene Warenzeichen von IBM Corporation.

OSF/Motif® ist ein eingetragenes Warenzeichen von Open Software Foundation.

ORACLE® ist ein eingetragenes Warenzeichen der ORACLE Corporation, Kalifornien, USA.

INFORMIX®-OnLine *for SAP* und Informix® Dynamic Server™ sind eingetragene Warenzeichen der Informix Software Incorporated.

UNIX® und X/Open® sind eingetragene Warenzeichen der SCO Santa Cruz Operation.

ADABAS® ist ein eingetragenes Warenzeichen der Software AG.

SECUDE® ist ein eingetragenes Warenzeichen der GMD-Forschungszentrum Informationstechnik GmbH.

SAP®, R/2®, R/3®, RIVA®, ABAP/4®, SAPaccess®, SAPoffice®, SAPmail®, SAP-EDI®, SAP Business Workflow®, SAP EarlyWatch®, SAP ArchiveLink®, R/3 Retail®, ALE/WEB®, SAPTRONIC® sind eingetragene Warenzeichen der SAP AG.

Alle Rechte vorbehalten.

Inhaltsverzeichnis

KAPITEL 1: EINLEITUNG	1-1
KAPITEL 2: SICHERHEITSASPEKTE.....	2-1
Authentifizierung.....	2-1
Berechtigung.....	2-2
Integrität	2-2
Vertraulichkeit.....	2-3
Unleugbarkeit (Verbindlichkeit)	2-3
Prüfung und Protokollierung	2-3
KAPITEL 3: DIE R/3-SICHERHEITSSERVICES.....	3-1
Benutzerauthentifizierung.....	3-2
R/3-Kennwortregeln	3-2
Single Sign-On / Smartcard-Authentifizierung	3-3
Erkennen und Verhindern unberechtigter Anmeldungen	3-4
R/3-Berechtigungskonzept	3-5
Berechtigungsprüfungen.....	3-5
Profilgenerator.....	3-6
Info-System Berechtigungen	3-7
Netzwerkkommunikation	3-8
SAProuter	3-8
Secure Network Communications (SNC).....	3-9
Secure-Store-&-Forward-Mechanismen (SSF) und Digitale Signaturen.....	3-11
Public-Key-Technologie.....	3-11
Prüfung und Protokollierung	3-15
Das Audit Info System (AIS)	3-15
Das Security-Audit-Log	3-16
Sicherheit für R/3-Internet-Anwendungen	3-17
KAPITEL 4: KUNDENSERVICES	4-1
Security Consulting Team	4-1
SAP Audit User Group.....	4-3
Feedback.....	4-3

Abbildungen

Abbildung 3-1: Übersicht über die R/3-Sicherheitsservices	3-1
Abbildung 3-2: Kennwörter	3-2
Abbildung 3-3: Single Sign-On	3-3
Abbildung 3-4: Profile mit dem Profilgenerator generieren	3-6
Abbildung 3-5: Das Info-System Berechtigungen	3-7
Abbildung 3-6: SAProuter	3-8
Abbildung 3-7: SNC-gesicherter Netzwerkbereich	3-10
Abbildung 3-8: Digitale Signatur	3-12
Abbildung 3-9: Digitaler Umschlag	3-13
Abbildung 3-10: Der Internet Transaction Server	3-17
Abbildung 3-11: ITS-Sicherheit	3-18

Informationen zum R/3-Sicherheitsleitfaden

Der *R/3-Sicherheitsleitfaden* besteht aus drei Bänden:

R/3-Sicherheitsleitfaden BAND I: R/3-Sicherheitservices im Überblick

R/3-Sicherheitsleitfaden BAND II: R/3-Sicherheitservices im Detail

R/3-Sicherheitsleitfaden BAND III: Checklisten

R/3-Sicherheitsleitfaden BAND I: R/3-Sicherheitservices im Überblick

Der *R/3-Sicherheitsleitfaden BAND I* bietet einen allgemeinen Überblick über die in R/3 angebotenen Sicherheitservices. In *BAND I* können Sie sich mit diesen Services vertraut machen, z. B. bevor Sie ein Sicherheitskonzept ausarbeiten oder ein R/3-System installieren.

R/3-Sicherheitsleitfaden BAND II: R/3-Sicherheitservices im Detail

Der *R/3-Sicherheitsleitfaden BAND II* behandelt die technischen Aspekte der Sicherheit im R/3-System. Er beschreibt die erforderlichen Aufgaben und enthält unsere Empfehlungen zu den verschiedenen Komponenten des R/3-Systems. Verwenden Sie *BAND II*, sobald Sie ein Sicherheitskonzept ausgearbeitet haben und dieses für Ihr R/3-System implementieren wollen.

R/3-Sicherheitsleitfaden BAND III: Checklisten

Der *R/3-Sicherheitsleitfaden BAND III* enthält Checklisten zu den in *BAND II* behandelten Themen. Anhand dieser Checklisten können Sie die ergriffenen Maßnahmen erfassen, überprüfen und überwachen.

Aktualisierungen

Nach Bedarf veröffentlichen wir aktualisierte Versionen dieses Leitfadens, die Sie regelmäßig im SAPNet finden.




Gültige Releases

Diese Version des *R/3-Sicherheitsleitfadens* gilt für R/3-Release 3.0, 3.1 und 4.0. Verweise auf andere Releases sind ggf. explizit angegeben.

Typografische Konventionen

Die folgende Tabelle erklärt die Bedeutung der verschiedenen Formate und Symbole in diesem Leitfaden.

Tabelle 1: Typografische Konventionen

Diese Darstellung	wird verwendet
<i>Text auf Bildschirmbildern</i>	für Texte, die vom Bildschirmbild zitiert werden, z. B. Systemmeldungen, Feldnamen, Bildschirmüberschriften, Menütitel und Menütexte
Benutzereingabe	für fest vorgegebene Benutzereingaben. Diese Begriffe oder Zeichen können Sie direkt im System eingeben.
<Variable Benutzereingabe>	für variable Benutzereingaben. Diese Begriffe und Zeichen in spitzen Klammern sind jeweils durch geeignete Eingaben zu ersetzen.
NAMEN	für Reportnamen, Programmnamen, Transaktionscodes, Tabellennamen, ABAP-Schlüsselwörter, Dateinamen und Verzeichnisse.
<i>Buchtitel</i>	für Verweise auf andere Bücher oder Dokumente.
Tastenschlüssel	für Tasten auf Ihrer Tastatur. Dies können Funktionstasten wie z. B. F2 oder die ENTER-Taste sein.
Namen von technischen Objekten	für Namen von technischen Objekten außerhalb des R/3-Systems (z. B. UNIX- oder Windows-NT-Dateinamen oder Umgebungsvariablen).
Dieses Piktogramm	kennzeichnet
 Beispiel	ein Beispiel. Beispiele illustrieren komplexe Sachverhalte oder die Syntax von Benutzereingaben.
 Hinweis	einen Hinweis. Hinweise enthalten wichtige Informationen wie z. B. Ausnahmen oder Sonderfälle.
 Achtung	eine Warnung. Warnungen sollen dazu beitragen, Fehler zu vermeiden, die z. B. zu einem Verlust von Daten führen können.

Kapitel 1: Einleitung

Der zunehmende Einsatz verteilter Systeme zur Verarbeitung und Verwaltung von Geschäftsdaten führt auch zu steigenden Sicherheitsanforderungen. Bei einem verteilten System muß sichergestellt sein, daß die Daten und Prozesse die Bedürfnisse eines Unternehmens unterstützen, ohne unberechtigten Zugriff auf kritische Informationen zu ermöglichen. Benutzerfehler, Nachlässigkeit oder Manipulationsversuche am System dürfen nicht Informations- oder Verarbeitungszeitverluste nach sich ziehen. Diese Sicherheitsanforderungen gelten in gleichem Maße für das SAP-R/3-System. SAP bietet daher zahlreiche Services, um den Sicherheitsanforderungen an das R/3-System gerecht zu werden.

Um unsere Services wirklich effektiv zu nutzen, müssen Sie allerdings auch einen Beitrag leisten. Sie müssen bestimmen, welche spezifischen Sicherheitsanforderungen für Ihr System gelten. Es ist ratsam, die Anforderungen an die Systemsicherheit genau zu analysieren und Prioritäten zu definieren. Welche Sicherheitsregeln gelten in Ihrem Unternehmen? Welche Informationen stufen Sie als kritisch ein? Wo werden kritische Informationen abgelegt oder übertragen? Welche Sicherheitsoptionen sind zum Schutz Ihrer kritischen Daten und Ihrer Kommunikation verfügbar?

Sie sollten ein **Sicherheitskonzept** einführen, das diese Anforderungen und Prioritäten widerspiegelt. Ihr Sicherheitskonzept muß sowohl von der Geschäftsführung als auch von allen Mitarbeitern unterstützt und gefördert werden. Es sollte im gesamten Unternehmen angewandt werden und Ihre gesamte IT-Infrastruktur einschließlich des R/3-Systems abdecken. Das Sicherheitskonzept sollte alle für Ihr System wesentlichen Sicherheitsaspekte umfassen. Zu den wichtigsten Sicherheitsaspekten gehören:

- Benutzerauthentifizierung
- Berechtigungsschutz
- Integritätsschutz
- Vertraulichkeitsschutz
- Unleugbarkeit (Verbindlichkeit)
- Prüfung und Protokollierung

Um Ihr Sicherheitskonzept umzusetzen und Ihren Sicherheitsanforderungen an das R/3-System gerecht zu werden, bieten wir eine Reihe von **R/3-Sicherheitsservices** an. Dazu zählen:

- **Benutzerauthentifizierung**
 - R/3-Kennwortregeln
 - Single Sign-On / Smartcard-Authentifizierung
 - Erkennen und Verhindern unberechtigter Anmeldungen
- **R/3-Berechtigungskonzept**
 - Berechtigungsprüfung
 - Profilgenerator
 - Info-System Berechtigungen
- **Netzwerkcommunication**
 - SAProuter
 - Secure Network Communications (SNC)

Kapitel 1: Einleitung

- **Secure-Store-&-Forward-Mechanismen (SSF) und Digitale Signaturen**
- **Prüfung und Protokollierung**
 - Das Audit Info System (AIS)
 - Das Security-Audit-Log
- **Sicherheit für R/3-Internet-Anwendungen**

Unsere Services sind so konzipiert, daß Sie die R/3-Sicherheit individuell und flexibel gestalten können. Sie entscheiden anhand Ihrer Prioritäten, ob Sie alle oder nur einen Teil dieser Services einsetzen wollen.

Der *R/3-Sicherheitsleitfaden* soll Sie bei der Nutzung unserer Services in Verbindung mit dem R/3-System zu unterstützen. Der vorliegende Band des Leitfadens verschafft Ihnen einen Überblick über die sicherheitsrelevanten Services. Eine detaillierte Beschreibung der Konfigurierung und Verwaltung unterschiedlicher sicherheitsrelevanter Komponenten des R/3-Systems finden Sie im *R/3-Sicherheitsleitfaden BAND II: R/3-Sicherheitsservices im Detail*. *BAND III* enthält Checklisten zu *BAND II*.

Der wichtigste Aspekt der Systemsicherheit ist immer Ihr eigenes Sicherheitskonzept! Dieser Leitfaden soll Ihnen bei der Aufstellung eines Sicherheitskonzepts helfen, er kann jedoch nicht Ihren Beitrag an Zeit und Mitteln ersetzen. Wir empfehlen Ihnen, der Einführung Ihres Sicherheitskonzepts und der Erhaltung des gewünschten Sicherheitsniveaus ausreichend Zeit und Ressourcen zu widmen.

Kapitel 2: Sicherheitsaspekte

Bei der Einführung Ihres Sicherheitskonzepts müssen Sie festlegen, welche Informationen oder Prozesse als kritisch einzustufen sind und wie Sie diese schützen wollen. Ihr Sicherheitskonzept sollte z. B. folgende Aspekte umfassen:

- **Authentifizierung**

Es ist wichtig, daß nur berechtigte Benutzer Zugriff auf Ihr System haben und Unbefugte nicht einfach eine Identität vortäuschen können!

- **Berechtigung**

Es ist wichtig, daß Benutzer nur Aufgaben ausführen können, für die sie eine Berechtigung besitzen!

- **Integrität**

Es ist wichtig, daß Daten nicht unbemerkt geändert werden können!

- **Vertraulichkeit**

Es ist wichtig, Daten und Kommunikation vor unbefugtem Lesen und Abhören zu schützen!

- **Unleugbarkeit (Verbindlichkeit)**

Es ist wichtig, die Zuverlässigkeit und rechtliche Verbindlichkeit sicherzustellen!

- **Prüfung und Protokollierung**

Es ist wichtig, Aktivitäten und Ereignisse aufzuzeichnen, um später darauf zurückgreifen zu können (z. B. Audits)!



Diese Aspekte werden nachfolgend genauer beschrieben.

Authentifizierung

Eine grundlegende und notwendige Sicherheitsaufgabe ist, die Authentizität der Benutzer und Informationen in einem System zu gewährleisten. Sie müssen sicher sein, daß die im System operierenden Benutzer bekannte Benutzer sind, deren Identität nicht vorgetäuscht werden kann. In R/3 bieten wir verschiedene Mechanismen, um die Benutzerkonten vor Mißbrauch zu schützen. R/3 authentifiziert seine Benutzer standardmäßig anhand von Kennwörtern. Das R/3-System weist eine Reihe von vorinstallierten Kennwortregeln auf, die Sie nach Bedarf noch erweitern können. Beispielsweise können Sie Ihre Benutzer dazu veranlassen, regelmäßig die Kennwörter zu erneuern. Außerdem können Sie bestimmte Wörter und Zeichenkombinationen verbieten. R/3 sperrt Benutzer und Sitzungen nach einer bestimmten Anzahl erfolgloser Anmeldeversuche, um zu verhindern, daß unberechtigte Benutzer Zugang zum System erhalten. Darüber hinaus können Sie mit unseren Secure Network Communications (SNC) auch außerhalb des R/3-Systems eine Authentifizierung ermöglichen. Sie können z. B. mit SNC eine Single-Sign-On-Umgebung einrichten und dabei auch Smartcards zur Authentifizierung verwenden. (Weitere Informationen erhalten Sie im Abschnitt *Benutzerauthentifizierung*.)

Berechtigung

Es ist wichtig, daß Benutzer nur die Aufgaben ausführen können, für die sie eine Berechtigung besitzen. Die Organisation eines typischen Unternehmens ist in verschiedene Rollen unterteilt, und die Mitarbeiter, die diese Rollen übernehmen, erledigen bestimmte Aufgaben. Der Zugriff auf bestimmte Daten und Prozesse sollte nur für die entsprechenden Rollen möglich sein. Beispielsweise benötigt ein Mitarbeiter der Personalabteilung Zugriff auf die Abrechnungsprozesse und die Mitarbeiterdaten. Diese Informationen sollten Mitarbeitern anderer Abteilungen wie z. B. der Produktion oder des Verkaufs nicht zugänglich sein.

Das R/3-Berechtigungskonzept schützt vor unberechtigtem Zugriff. Benutzer können nur die Transaktionen und Programme verwenden, für die sie eine explizite Zugriffsberechtigung besitzen. Wenn ein Benutzer eine Transaktion oder ein Programm starten will, führt R/3 eine Berechtigungsprüfung durch, bevor dem Benutzer der Zugriff gestattet wird. Hat der Benutzer nicht die korrekten Berechtigungen, verweigert R/3 den Zugriff auf die entsprechenden Programme und Transaktionen.

Der **Profilgenerator** und das **Info-System Berechtigungen** erleichtern Ihnen die Arbeit mit dem R/3-Berechtigungskonzept. Der Profilgenerator bietet Ihnen für die Berechtigungsvergabe einen hierarchischen Aufbau. Das Info-System Berechtigungen bietet Ihnen eine leicht abrufbare Übersicht über Ihre Berechtigungen und deren Zuordnungen.

Integrität

Sie müssen die Informationen, die Sie täglich verarbeiten, vor unberechtigten – irrtümlichen oder beabsichtigten – Änderungen schützen. Wenn ein Benutzer eine Transaktion bearbeitet (z. B. eine Zahlung auf ein Konto), muß er sicher sein können, daß die Informationen während des gesamten Bearbeitungsvorgangs konsistent bleiben. Außerdem muß er beim Zugreifen auf Daten sicher sein können, daß es sich dabei um die zuletzt gespeicherten Daten handelt. Die Hard- und Software muß erwartungsgemäß funktionieren und darf keine nicht definierten oder unerwünschten Aktionen ausführen. Dieser Prozeß muß so gut funktionieren, daß das System als Ganzes störungsfrei und ohne Datenverfälschung arbeiten kann.

In R/3 werden zum Schutz der Integrität beispielsweise folgende Mechanismen verwendet (oder stehen zur Verfügung):

- R/3 schützt die Datenintegrität auf Datenbankebene über einen Sperrmechanismus.
- Die Präsentationssoftware überprüft die eigene Integrität, um sicherzustellen, daß sie nicht selbst Viren enthält.
- Über die Secure-Store-and-Forward-Mechanismen (SSF-Mechanismen) stehen digitale Signaturen zur Verfügung, die von bestimmten Anwendungen verwendet werden. Digitale Signaturen dienen nicht nur zum Nachweis der Identität des "Unterzeichners", sondern können auch zum Nachweis der Integrität eines signierten Datenpakets verwendet werden.
- Zum Schutz der Integrität des Datenaustauschs zwischen R/3-Komponenten können Sie SNC sowie ein externes Sicherheitsprodukt in Verbindung mit R/3 verwenden.
- R/3 protokolliert auch alle Importe und Exporte aus bzw. in das System.

Vertraulichkeit

Seit jeher ist es notwendig, sensible und vertrauliche Informationen vor dem Lesen durch Unbefugte zu schützen. Persönliche Informationen werden beispielsweise mit dem Vermerk "vertraulich" versehen, bevor sie weitergeleitet werden. Arbeitgeber sind verpflichtet, Informationen über Verträge und Mitarbeiter vertraulich zu behandeln. Datenschutzgesetze verbieten die Verbreitung personenbezogener Daten. Informationen über das Unternehmen, die Kunden, Produkte und Prototypen werden in einem Safe des Unternehmens verwahrt. Dieser Schutz wird auch auf Daten angewandt, die mit elektronischen Medien gesichert oder übertragen werden.

Das R/3-Berechtigungskonzept stellt sicher, daß die Benutzer nur auf die Daten zugreifen dürfen, die sie benötigen. Um den Schutz der Vertraulichkeit auf R/3-Datenübertragungen anzuwenden, können Sie mit SNC die zwischen den R/3-Komponenten übertragenen Daten verschlüsseln. Unsere SSF-Mechanismen verwenden die Verschlüsselung auch zum "Verpacken" der Daten in sichere Formate, den sogenannten **digitalen Umschlägen**, bevor die Daten übertragen oder gesichert werden.

Unleugbarkeit (Verbindlichkeit)

Der Beweis der Unleugbarkeit (Verbindlichkeit) elektronisch gesicherter oder übertragener Daten ist im elektronischen Handel (Electronic Commerce) unverzichtbar. Eine Nachricht wird als verbindlich angesehen, wenn Sie garantieren können, wer sie erstellt hat und daß sie korrekt ist. Nur so kann sich der elektronische Handel in der heutigen Geschäftswelt etablieren. Beispielsweise wollen Sie, bevor Sie einen elektronischen (nicht ausgedruckten) Vertrag abschließen, sicher sein, daß er verbindlich und gültig ist. Daher muß es möglich sein, die Authentizität des Dokumentenabsenders sowie die Aktualität des Dokumenteninhalts nachzuweisen.

Über die SSF-Mechanismen verwenden einige Anwendungen in R/3 **digitale Signaturen**, um die Unleugbarkeit sicherzustellen. In diesen Anwendungsgebieten werden handschriftliche Unterschriften durch digitale Signaturen ersetzt, wodurch die Arbeitsprozesse automatisiert werden und gleichzeitig bei der Unterzeichnung eine 100%ige Identifizierung des Unterzeichners erfolgt.

Einige Anwendungen, die derzeit zur Erstellung digitaler Signaturen SSF verwenden (ab Release 4.0), sind beispielsweise

- das Qualitätsmanagement
- das Produktdatenmanagement
- die Produktionsplanung für die Prozeßindustrie

Prüfung und Protokollierung

Das Aufzeichnen von Ereignissen und Aktivitäten ist auch für ein späteres Nachschlagen wichtig. Gewisse Informationen aufzubewahren ist nicht nur aus rechtlichen Gründen notwendig, Protokolle und Prüfungen können sich für die Überwachung der Systemsicherheit und die Verfolgung von Ereignissen bei Problemen als unentbehrlich erweisen. R/3 führt eine Vielzahl von Protokollen für die Systemverwaltung, Überwachung, Fehlerbehebung und Prüfung. Das **Audit Info System** und das **Security-Audit-Log** sind die zu den R/3-Sicherheitsservices gehörigen Auditing-Werkzeuge. Zu den zusätzlichen Protokollen zählen die Systemprotokolle, die statistischen Aufzeichnungen im CCMS (Computing Center Management System), Änderungsbelege für Business-Objekte und die Anwendungsprotokollierung.



Kapitel 2: Sicherheitsaspekte

Kapitel 3: Die R/3-Sicherheitsservices

Im letzten Kapitel haben wir die Sicherheitsaspekte der Authentifizierung, Berechtigung, Integrität, Vertraulichkeit, Unleugbarkeit sowie der Prüfung und Protokollierung beschrieben. Unsere R/3-Sicherheitsservices bieten auf der Basis dieser Aspekte Schutz. Abbildung 3-1 zeigt eine Übersicht über die R/3-Sicherheitsservices.

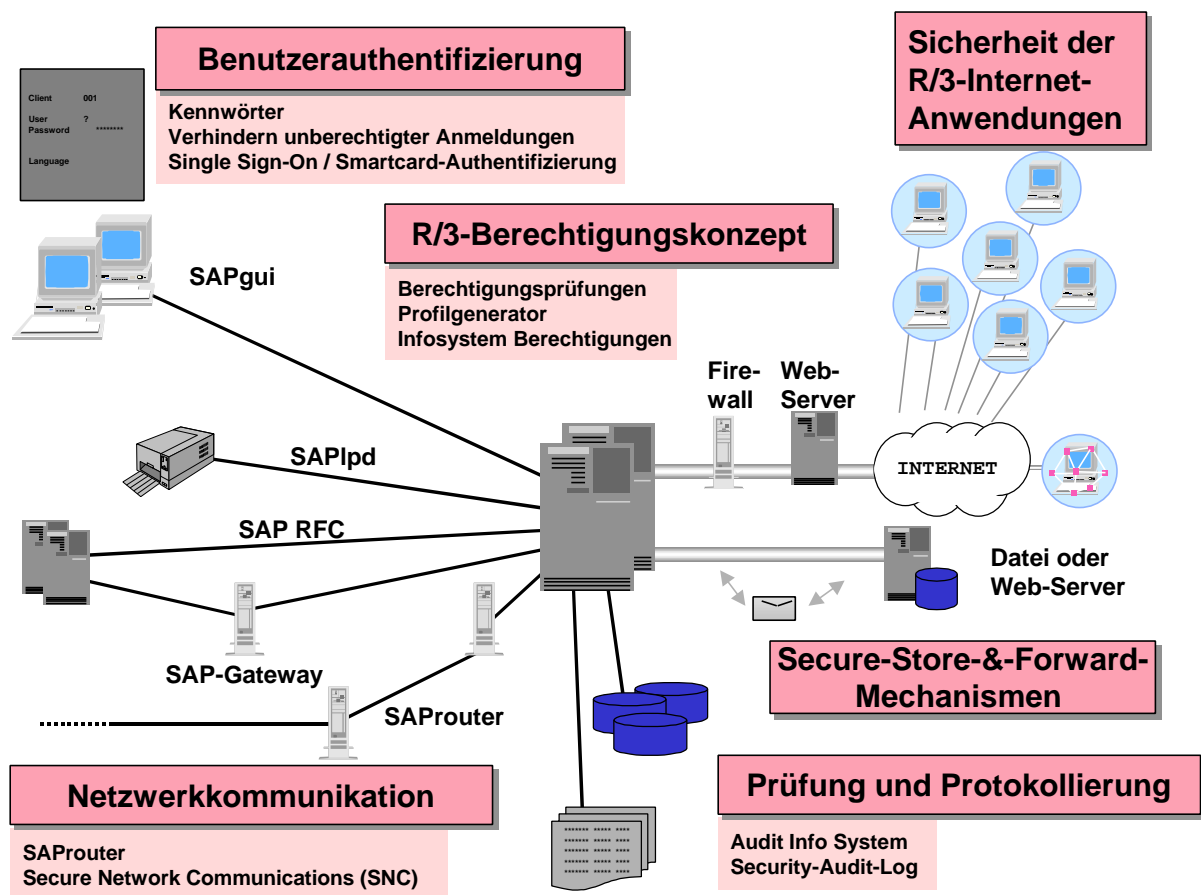


Abbildung 3-1: Übersicht über die R/3-Sicherheitsservices

In den folgenden Abschnitten werden die einzelnen Services genauer beschrieben.

Benutzerauthentifizierung

Das R/3-System wird mit eigenem Benutzerverwaltungsservice geliefert. Für jeden Benutzer führt das R/3-System ein separates Konto – den Benutzerstammsatz – das alle spezifischen Informationen über einen Benutzer enthält (z. B. Benutzernamen, Kennwort und Berechtigungen).

Um die Benutzer zu authentifizieren, verwendet das R/3-System als Standardmechanismus **Kennwörter**. Zur Authentifizierung außerhalb des R/3-Systems können Sie auch ein externes Sicherheitsprodukt in Verbindung mit R/3 verwenden. Damit können Sie Funktionen wie das **Single Sign-On** oder die **Authentifizierung mit Smartcards** nutzen. Außerdem verhindert R/3 **unberechtigte Anmeldungen** durch Benutzer- und Sitzungssperren. Diese Mechanismen werden im folgenden genauer beschrieben.

R/3-Kennwortregeln

Wir liefern eine Reihe von Standardregeln für Kennwörter in R/3. Viele dieser Regeln können Sie in Profilparametern den Anforderungen Ihres Sicherheitskonzepts anpassen.

Einige der Standardregeln für Kennwörter lauten

- Erstbenutzer erhalten ein Initialkennwort, das sie bei der ersten Anmeldung ändern müssen.
- Kennwörter haben eine Standardmindestlänge von drei Zeichen. (Sie können diesen Wert in einem Profilparameter erhöhen.)
- Kennwörter können maximal acht Zeichen lang sein.
- Das erste Zeichen darf nicht ? oder ! sein.
- Die ersten drei Zeichen des Kennworts dürfen in dieser Folge nicht im Benutzernamen vorkommen.
- Die ersten drei Zeichen dürfen nicht identisch sein.
- Keines der ersten drei Zeichen darf ein Leerzeichen sein.
- Das Kennwort darf nicht **PASS** oder **SAP*** lauten.
- Die letzten fünf Kennwörter dürfen nicht wieder benutzt werden.
- Der Benutzer kann sein Kennwort nur bei der Anmeldung ändern.
- Sie können veranlassen, daß Benutzer ihre Kennwörter regelmäßig ändern müssen.
- Sie können bestimmte Zeichenkombinationen verbieten.

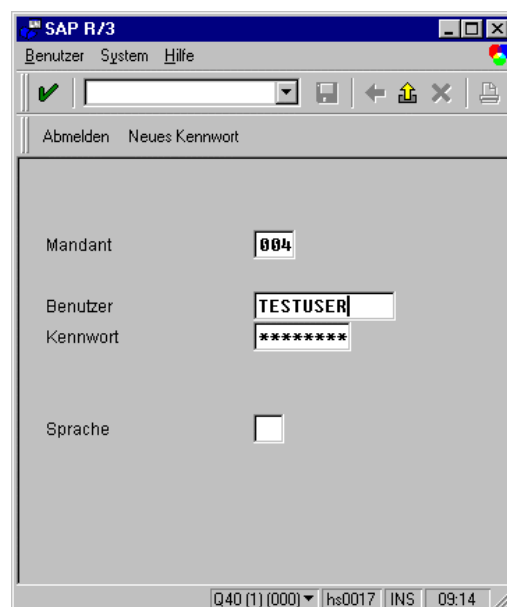


Abbildung 3-2: Kennwörter

Single Sign-On / Smartcard-Authentifizierung

Wenn Sie unsere Secure Network Communications und ein externes Sicherheitsprodukt (siehe Abschnitt *Netzwerkkommunikation*) einsetzen, können Sie eine **Single-Sign-On-Umgebung** nutzen. Diese muß durch ein externes Sicherheitsprodukt aufgebaut werden, damit SNC sie benutzen kann.

Mit Single Sign-On brauchen sich Ihre Benutzer nur einmal zu authentifizieren, selbst wenn sie in mehreren Systemen arbeiten. Sie melden sich bei einem externen Sicherheitsprodukt an; das Sicherheitsprodukt erstellt "Beglaubigungsinformationen" für die Benutzer, die es dann an andere Systeme wie R/3 weitergibt. Greift ein Benutzer auf ein durch ein Sicherheitsprodukt geschütztes System zu, z. B. ein R/3-System, wird er auf der Grundlage der vom Produkt gelieferten Authentifizierungsinformationen automatisch bei dem System angemeldet (siehe Abbildung 3-3). Das Produkt versendet keine Kennwortinformationen über das Netzwerk, sondern einen Nachweis darüber, daß es den Benutzer authentifiziert hat.

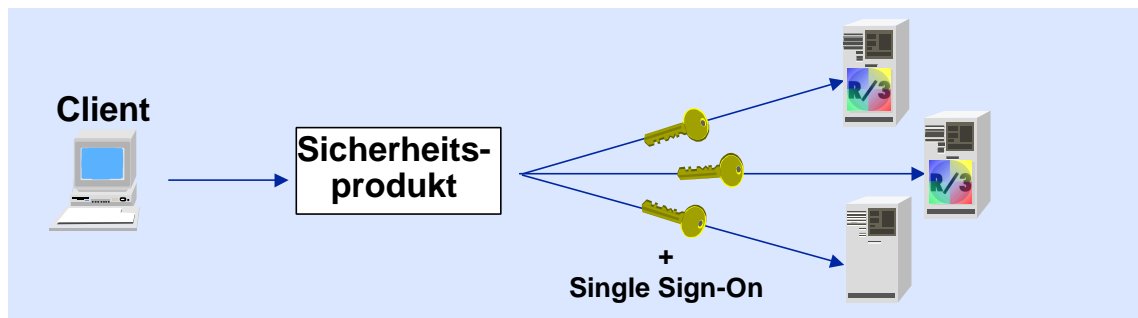


Abbildung 3-3: Single Sign-On

SNC bietet mehr als nur Single Sign-On, nämlich zusätzliche Integrität und Schutz der Vertraulichkeit für Datenübertragungen. Diesen Schutz kann SNC nur mit Hilfe eines von SAP zertifizierten externen Sicherheitsprodukts bieten. Für eine "reine Single-Sign-On"-Umgebung unter Windows NT können Sie den Microsoft NTLMSSP (NT LAN Manager Security Support Provider) als Sicherheitsprodukt verwenden. Mit dieser Lösung müssen Sie kein von SAP zertifiziertes Produkt kaufen. Weitere Informationen finden Sie im Online Service System in Hinweis 138498 [2] sowie im *SNC-Benutzerhandbuch* [10].

Je nach dem mit SNC verwendeten Sicherheitsprodukt können Sie auch **Smartcards** für die Authentifizierung nutzen. (Sie benötigen ein externes Sicherheitsprodukt, um Smartcards benutzen zu können; sie werden allerdings nicht von allen Sicherheitsprodukten unterstützt). Bei den Smartcards werden die Authentifizierungsinformationen des Benutzers auf dessen persönlicher Karte abgelegt. Solche Karten werden oft auch durch eine PIN (Personal Identification Number) geschützt. Da der Benutzer sowohl die Karte **besitzt** als auch die PIN **kennt**, ist die Wahrscheinlichkeit, daß jemand die Informationen kopiert oder sich aneignet, stark eingeschränkt. Bei der Authentifizierung mit Smartcard ist es ebenfalls nicht mehr notwendig, Kennwortinformationen über das Netzwerk zu übertragen.

Hinweis

Obwohl die Authentifizierung bei Single Sign-On außerhalb des R/3-Systems stattfindet, gibt es in R/3 weiterhin Berechtigungsschutz.

Erkennen und Verhindern unberechtigter Anmeldungen

Neben der Authentifizierung der Benutzer bei der Anmeldung verhindert R/3 auch unberechtigte Anmeldungen und zwar mit folgenden Mechanismen, die Sie fast alle in Profilparametern den Anforderungen Ihres Sicherheitskonzepts anpassen können.

- R/3 beendet eine Sitzung, wenn eine Reihe erfolgloser Anmeldeversuche mit demselben Benutzernamen erfolgte.
- R/3 sperrt einen Benutzernamen nach einigen erfolglosen Anmeldeversuchen.
- R/3 kann automatisch inaktive Benutzer abmelden.

Als zusätzlichen Schutz empfehlen wir, daß Sie

- Ihre Benutzer zur Verwendung von Bildschirmschonern mit Kennwörtern veranlassen
- Ihr System regelmäßig überwachen und auf unberechtigte Anmeldeversuche überprüfen

R/3-Berechtigungskonzept

Das R/3-Berechtigungskonzept schützt Transaktionen und Programme vor unberechtigter Verwendung. R/3 verhindert, daß Benutzer ohne ausdrücklich definierte Berechtigungen Transaktionen oder Programme ausführen. Sie entscheiden, welche Programme und Transaktionen die Benutzer aufrufen dürfen, und weisen ihnen in den Benutzerstammsätzen die entsprechenden Berechtigungen zu. Wenn ein Benutzer ein Programm startet oder eine Transaktion aufruft, führt R/3 **Berechtigungsprüfungen** durch und stellt damit sicher, daß der Benutzer über die korrekten Berechtigungen verfügt.

Um Ihnen die Arbeit mit dem R/3-Berechtigungskonzept zu erleichtern, bieten wir den **Profilgenerator** und das **Info-System Berechtigungen** als Teil unserer R/3-Sicherheitsservices an.

Berechtigungsprüfungen

Für die Umsetzung des R/3-Berechtigungskonzept führt R/3 Berechtigungsprüfungen durch, sobald Benutzer Programme oder Transaktionen ausführen wollen. Bei diesen Berechtigungsprüfungen stellt R/3 sicher, daß im Benutzerstammsatz des Benutzers die entsprechenden Berechtigungen eingetragen sind, bevor der Benutzer fortfahren kann. Zu den verschiedenen Arten der Berechtigungsprüfungen zählen:

- **R/3-Berechtigungsprüfung bei Transaktionsstart**

Ein Benutzer benötigt die entsprechenden Berechtigungen, um Transaktionen starten zu können. Dies gilt sowohl für Transaktionen, die über das Menü gestartet werden, als auch für Transaktionen, die über die Kommandozeile aufgerufen werden.

- **Spezielle Berechtigung für eine Transaktion**

Neben der R/3-Berechtigungsprüfung bei Transaktionsstart sind SAP-Transaktionen durch zusätzliche Berechtigungsprüfungen geschützt. Wenn Sie eigene Transaktionen erstellen, können Sie diesen ebenfalls zusätzliche Berechtigungsprüfungen zuweisen, z. B. indem Sie der Transaktion eine spezielle Berechtigung zuweisen. Dies ist sinnvoll, wenn Sie die Transaktion mit einer einzigen Berechtigung schützen können. Ist dies nicht der Fall, stehen noch weitere Methoden für die Zuweisung von Berechtigungsprüfungen zur Verfügung.

- **AUTHORITY-CHECK auf Programmebene**

Eine weitere Methode für die Zuweisung zusätzlicher Berechtigungsprüfungen ist das Einfügen der Anweisung AUTHORITY-CHECK auf Programmebene. Dadurch können Sie einzelne Programme auf Coding-Ebene schützen. Die SAP-Programme verwenden diese Schutzmethode, und wir raten Ihnen sehr dazu, sie auch für Ihre eigenen Entwicklungen zu verwenden.

- **Reportklassen und Tabellenberechtigungsgruppen**

Zusätzlich zu den Programm- und Transaktionsberechtigungsprüfungen können Sie Reports Reportklassen und Tabellen Berechtigungsgruppen zuweisen. Selbst wenn Benutzer die Transaktionen zum Ausführen von Reports oder zum Zugriff auf Tabellen benutzen können, dürfen sie damit nur auf die Reports und Tabellen zugreifen, für die sie die entsprechende Berechtigung besitzen.

Profilgenerator

Der Profilgenerator erleichtert Ihnen die Arbeit, indem er verschiedene Prozesse automatisiert und Ihnen bei der Zuweisung von Berechtigungen mehr Flexibilität ermöglicht. Der Grundgedanke dabei ist, sich von den technischen Aspekten der Berechtigungen und Berechtigungsobjekte zu lösen, und Ihre Berechtigungszuweisungen entsprechend den Rollen, Aktivitätsgruppen und Aufgaben zu konfigurieren.

Der Profilgenerator verwendet zur Generierung von Berechtigungszuweisungen einen hierarchischen Ansatz. Sie beginnen bei Ihrem Firmenmenü und arbeiten sich nach unten zu den einzelnen Benutzerstammsätzen durch. Sie definieren Ihre Stellenbeschreibungsmatrix, legen Aktivitätsgruppen an und entscheiden, welche Transaktionen und Funktionen die einzelnen Rollen benötigen. Den Rest übernimmt der Profilgenerator, einschließlich der Auswahl der für die verschiedenen Aufgaben notwendigen Berechtigungsobjekte. Abbildung 3-4 zeigt diesen Prozeß und erläutert ihn kurz.



Abbildung 3-4: Profile mit dem Profilgenerator generieren

Der Profilgenerator bietet Ihnen Flexibilität und einen Automatisierungsgrad, der Ihnen die Berechtigungsverwaltung wesentlich erleichtert. Wir empfehlen Ihnen, den Profilgenerator zur Pflege der Benutzerberechtigungen zu verwenden.

Verfügbarkeit

Der Profilgenerator ist Teil der Standardauslieferung von Release 3.1G und läuft auf allen unterstützten Plattformen.

Info-System Berechtigungen

Mit dem Info-System Berechtigungen können Sie sich einen Überblick über Ihre Berechtigungen, Profile, Benutzer und Berechtigungszuweisungen verschaffen. Mit dem Info-System können Sie schnell und einfach Berechtigungsinformationen des R/3-Systems anzeigen.

Das Info-System Berechtigungen ist ein Berichtsbaum (vergleichbar mit dem Einführungsleitfaden). Damit können Sie eine Reihe von Listen erstellen, z. B.:

- Benutzer mit bestimmten Berechtigungen
- Berechtigungen eines bestimmten Benutzers
- alle Berechtigungen
- Profilvergleiche
- Transaktionen, die ein bestimmter Benutzer ausführen kann
- Änderungen im Berechtigungsprofil eines Benutzers

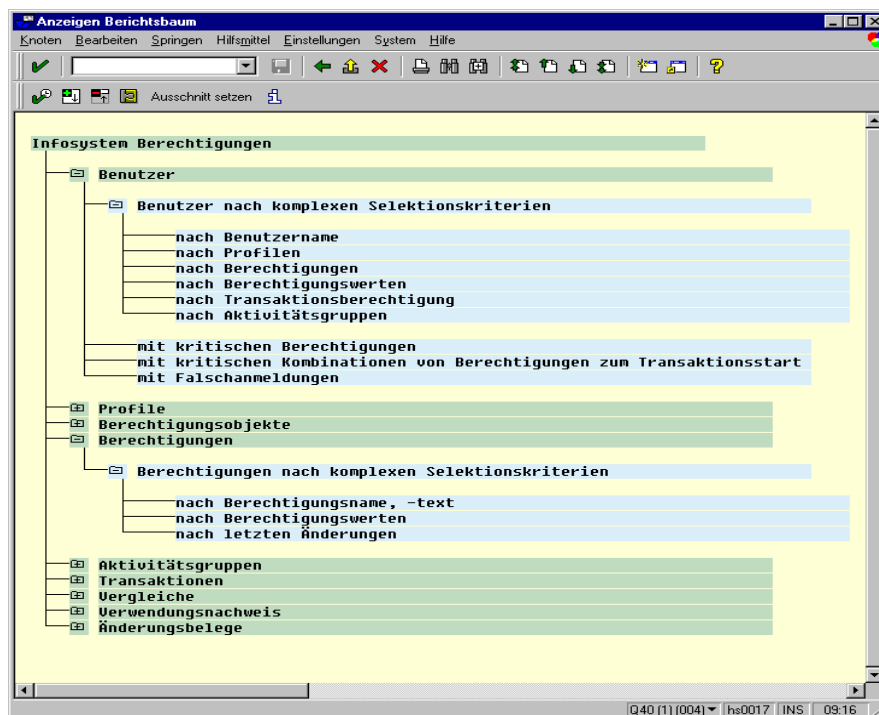


Abbildung 3-5: Das Info-System Berechtigungen

Das Info-System Berechtigungen bietet Ihnen eine schnell und leicht zugängliche Informationsquelle über Ihre Benutzer und Berechtigungszuweisungen.

Verfügbarkeit

Das Info-System Berechtigungen ist ebenfalls ab Release 3.1G verfügbar.

Netzwerkkommunikation

Für die Sicherheit Ihres Systems ist die Netzwerkinfrastruktur von großer Bedeutung. Sie müssen in der Lage sein, Ihre Netzwerkkommunikation zu unterstützen, ohne dabei unberechtigten Zugriff auf Ihr Netzwerk zu gestatten. Wenn Sie beim Aufbau Ihrer Netzwerktopologie der Sicherheit höchste Priorität geben, reduzieren Sie viele mögliche Gefahrenquellen.

Die wichtigsten Faktoren bei der Entscheidung über das aus Ihrer Sicht notwendige Niveau der Netzwerksicherheit sind auch hier Ihre Strategie und Ihre Prioritäten. Wir geben allgemeine Empfehlungen für die Einrichtung Ihrer Netzwerktopologie und empfehlen Ihnen, sich bei Bedarf an unser Security Consulting Team zu wenden (siehe *Kapitel 4: Kundenservices*).

Die wichtigsten R/3-Sicherheitsservices, die wir für die Netzwerksicherheit anbieten, sind **SAProuter** und **Secure Network Communications (SNC)**.

SAProuter

Der SAProuter ist ein Proxy auf Anwendungsebene, das Sie zusammen mit einer Firewall verwenden können, um Ihr Netzwerk wirksam gegen unberechtigten Zugriff zu schützen. Mit einer Firewall unterbinden Sie unerwünschten Zugriff auf Ihr internes Netzwerk. Für die erwünschte Kommunikation müssen Sie entsprechende "Türen" in der Firewall öffnen, um die Kommunikationsanfragen passieren zu lassen. Sie können den SAProuter dann als "Wachposten" hinter diesen Türen einsetzen, um den Zugriff innerhalb Ihres Netzwerks für die SAP-Systeme noch genauer zu steuern. Der SAProuter stellt außerdem sicher, daß die Anfrage gültig ist, allerdings auf einer viel detaillierteren Ebene, da er die SAP-Protokolle versteht. Er kann Anfragen eines bestimmten Benutzers oder einer bestimmten Maschine akzeptieren oder ablehnen oder sie nur an eine bestimmte Maschine leiten. Wenn Sie den SAProuter zusammen mit der Firewall verwenden, können Sie Ihr R/3-LAN-System wirksam vor unberechtigtem Zugriff schützen.



Beispiel

In Abbildung 3-6 lehnt die Firewall alle `telnet`-Anfragen ab und die Anfrage von Benutzer Z ist gesperrt. Allerdings ist die Firewall für das SAP-Protokoll `DIAG` geöffnet, das für `SAPgui`-Verbindungen benutzt wird. Der SAProuter stellt dann sicher, daß nur bestimmte Benutzer mit `DIAG` auf das R/3-LAN-System zugreifen können. Die Firewall akzeptiert sowohl die `DIAG`-Anfrage von Benutzer X als auch von Benutzer Y, aber der SAProuter akzeptiert jedoch nur die Anfrage von Benutzer Y.

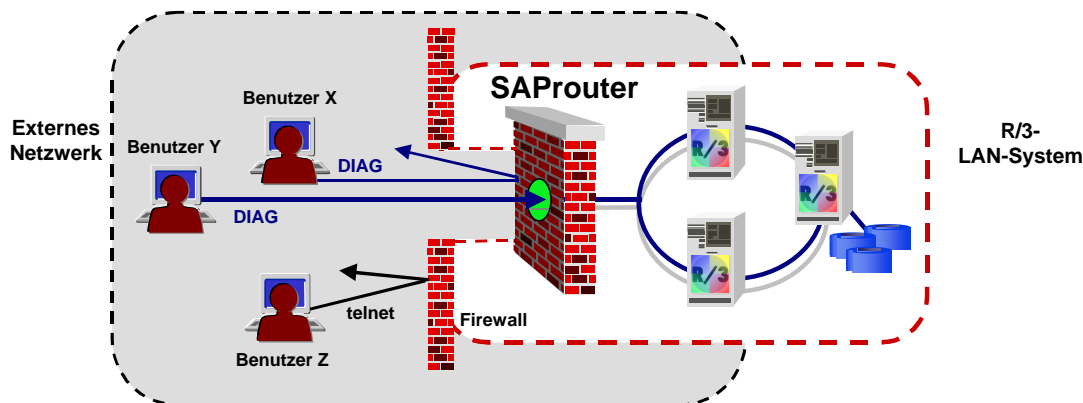


Abbildung 3-6: SAProuter

**Hinweis**

Der SAProuter allein genügt nicht, um den Zugriff auf Ihr Netzwerk zu steuern. Sie müssen ihn in Verbindung mit einem Firewall-System einsetzen.

Sie können den SAProuter auch einsetzen, um

- die Verbindungen zu Ihrem R/3-System (z. B. von einem SAP Service Center) zu steuern und zu protokollieren
- eine indirekte Verbindung herzustellen, wenn die an der Verbindung beteiligten Programme sich aufgrund der Netzwerkkonfiguration nicht direkt miteinander kommunizieren können
- die Netzwerksicherheit zu verbessern, indem Sie
 - Ihre Verbindung und Ihre Daten durch ein Kennwort gegen unberechtigte Zugriffe von außen schützen
 - den Zugang nur von bestimmten SAProutern aus zulassen
 - nur verschlüsselte Verbindungen von einem sicher authentifizierten Partner durch Verwendung von SNC zulassen
- die Performance und die Stabilität zu erhöhen, indem Sie die Belastung des R/3-Systems innerhalb eines Local Area Network (LAN) bei der Kommunikation mit einem Wide Area Network (WAN) verringern

**Hinweis**

Obwohl die Kombination SAProuter und Firewall häufig verwendet wird, um ein internes Netzwerk von externen Netzwerken zu trennen, raten wir Ihnen dringend dazu, daß Sie es auch zur Zugriffssteuerung zwischen verschiedenen internen Netzwerken einsetzen!

**Hinweis**

Wenn Sie die R/3-Online-System-Services verwenden, **müssen** Sie einen SAProuter einsetzen!

Secure Network Communications (SNC)

SNC schützt die Kommunikation zwischen den verteilten Komponenten des R/3-Systems. Jede R/3-Komponente enthält eine Softwareschicht, die SNC-Schicht, über die R/3 mit einem externen Sicherheitsprodukt zusammenarbeiten kann. R/3 kommuniziert mit dem externen Produkt über die Standardschnittstelle GSS-API V2 (Generic Security Services Application Programming Interface Version 2). Die GSS-API V2 wurde von der IETF (Internet Engineering Task Force) unter Beteiligung von SAP entwickelt.

Mit der SNC-Option können Sie ein externes Sicherheitsprodukt in Verbindung mit R/3 verwenden und die Sicherheitsfunktionen des Produkts nutzen, die in R/3 nicht direkt verfügbar sind. Daher können Sie das Produkt mit den Funktionen wählen, die Ihren Bedürfnissen am besten gerecht werden. Sicherheitsprodukte bieten beispielsweise folgende Funktionen:

- Single Sign-On
- Smartcard-Authentifizierung
- Verschlüsselung von Datenströmen zwischen R/3-Komponenten (Schutz der Integrität und Vertraulichkeit)

Kapitel 3: Die R/3-Sicherheitsservices

Das externe Produkt ist in der SAP-R/3-Software nicht enthalten, sondern muß über den entsprechenden Anbieter eingekauft werden. Informationen über die Produkte und deren Verfügbarkeit finden Sie im Complementary Software Program im SAPNet unter dem Alias "csp" (z. B. <http://sapnet.sap.com/csp>); dort befindet sich der Verweis *Complementary Solutions* → *Network security*.

In einigen Ländern ist die Verwendung der Kryptografie gesetzlich geregelt. Sie sollten sich regelmäßig über die Auswirkungen dieser Gesetze auf Ihre Anwendungen informieren und sicherstellen, daß Ihnen alle weiteren Entwicklungen bekannt sind.

Sicherheit auf Anwendungsebene

SNC bietet Sicherheit auf der Anwendungsebene. Das heißt, daß unabhängig vom Transportmedium eine sichere Verbindung zwischen den Kommunikationspartnern (z. B. zwischen dem SAPgui und dem R/3-Anwendungsserver) garantiert ist.

SNC bietet Sicherheit zwischen R/3-Anwendungsservern, Clients und SAProutern. Allerdings können Sie die durch SNC gebotene Sicherheit nicht auf den Kommunikationspfad zwischen den Anwendungsservern und Ihrer Datenbank anwenden. Aus diesem Grund empfehlen wir, daß Sie Ihre Datenbank- und Anwendungsserver in einem sicheren LAN betreiben. Abbildung 3-7 zeigt die durch SNC geschützten Bereiche Ihres LAN bzw. WAN.

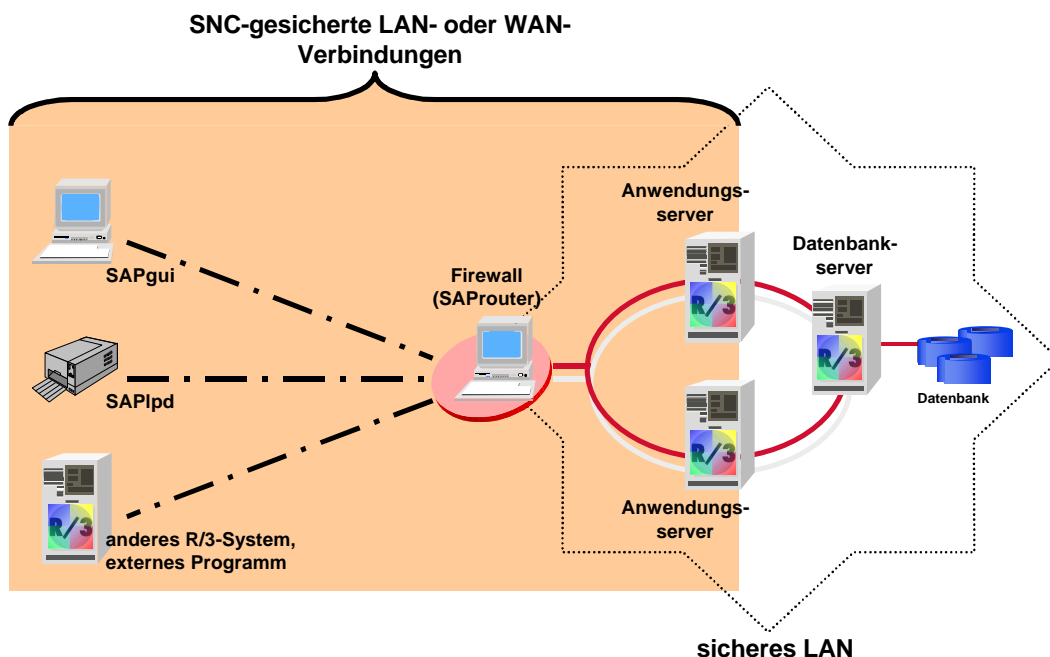


Abbildung 3-7: SNC-gesicherter Netzwerkbereich

Verfügbarkeit

Ab Release 3.1G ist der SNC-Schutz für SAPgui- und SAPipd-Verbindungen verfügbar und ab Release 4.0 zusätzlich auch für RFC und CPI-C. Ab SAProuter Version 30 können Sie den SNC-Schutz auch für die Sicherung der SAProuter-Kommunikation verwenden.

Secure-Store-&-Forward-Mechanismen (SSF) und Digitale Signaturen

Ab Release 4.0 können R/3-Anwendungen Secure-Store-&-Forward-Mechanismen (SSF) verwenden, um im R/3-System beliebige Daten zu sichern. R/3-Anwendungen können mit den SSF-Mechanismen die Integrität, Echtheit und Vertraulichkeit der Daten sichern. Die Daten sind selbst dann geschützt, wenn sie das R/3-System verlassen. Zu den ersten Anwendungen, die SSF verwenden, gehören

- Produktionsplanung – Prozeßindustrie
- Produktdatenmanagement
- SAP ArchiveLink – SAP-Content-Server-HTTP-Schnittstelle 4.5

Mit der Zeit werden immer mehr Anwendungen SSF verwenden, um die Sicherheit zu erhöhen.

SSF benötigt zur Ausführung seiner Funktionen ein Sicherheitsprodukt. Ab Release 4.5 wird R/3 mit der SAPSECULIB (SAP Security Library) als Standardanbieter des SSF-Service geliefert. SAPSECULIB ist eine Softwarelösung, deren Funktionalität auf digitale Signaturen begrenzt ist. Für die Unterstützung kryptografischer Hardware (z. B. Smartcards, Sicherheitsboxen usw.) oder digitaler Umschläge benötigen Sie ein von SAP zertifiziertes externes Sicherheitsprodukt.



Hinweis

In einigen Ländern wird die Verwendung der Kryptografie und digitaler Signaturen gesetzlich geregelt. Diese Gesetze sind noch sehr unterschiedlich und können sich ändern. Sie sollten sich regelmäßig über die Auswirkungen dieser Gesetze auf Ihre Anwendungen informieren und sicherstellen, daß Ihnen alle weiteren Entwicklungen bekannt sind.

Public-Key-Technologie

SSF verwendet **digitale Signaturen** und **digitale Umschläge** zum Sichern digitaler Dokumente. Die digitale Signatur identifiziert den Unterzeichner eindeutig. Sie kann nicht gefälscht werden und schützt die Integrität der Daten. Jede nach der Unterzeichnung vorgenommene Änderung der Daten führt dazu, daß die digitale Signatur für die geänderten Daten ungültig ist. Der digitale Umschlag sorgt dafür, daß der Dateninhalt nur für den Empfänger lesbar ist, für den er bestimmt ist.

Digitale Signaturen und digitale Umschläge basieren auf der Public-Key-Technologie. Ein Benutzer, der diese digitalen Signaturen oder Umschläge erstellt, besitzt ein Schlüsselpaar mit folgenden Eigenschaften:

- Die Schlüssel sind Paare und gehören zusammen.
- Keiner der beiden Schlüssel kann aus dem anderen berechnet werden.
- Wie der Name schon sagt, wird der öffentliche Schlüssel veröffentlicht. Der Empfänger eines signierten Dokuments muß diesen Schlüssel kennen, um die digitale Signatur prüfen zu können, und der Absender eines vertraulichen Dokuments benötigt den öffentlichen Schlüssel des Empfängers, um das Dokument zu verschlüsseln und seinen Inhalt zu verbergen.

Kapitel 3: Die R/3-Sicherheitsservices

Der Besitzer der Schlüssel verteilt den öffentlichen Schlüssel nach Bedarf. Normalerweise besitzt er ein **Public-Key-Zertifikat**, das alle zur Verteilung notwendigen Informationen enthält (z. B. den Namen, die Organisation, seinen öffentlichen Schlüssel, die Gültigkeitsdauer des Zertifikats und den Namen der das Zertifikat ausstellenden Organisation). Den öffentlichen Schlüssel verteilt er über das Public-Key-Zertifikat.

- Der private Schlüssel muß geheimgehalten werden. Der Schlüsselbesitzer verwendet den privaten Schlüssel zum Generieren seiner digitalen Signatur. Daher muß er sicherstellen, daß **weder** eine unbefugte Person **noch** ein unbefugtes System auf seinen privaten Schlüssel zugreifen kann.

Digitale Signaturen

Mit dem privaten Schlüssel wird die digitale Signatur eines digitalen Dokuments erstellt. Solange der Besitzer des privaten Schlüssels diesen geheimhält, kann niemand anderes eine identische digitale Signatur für das Dokument erstellen.

Abbildung 3-8 zeigt, wie ein digital signiertes Dokument erstellt wird. Beachten Sie, daß Sie üblicherweise nur angeben, daß Sie ein Dokument "signieren" wollen, und daß das System alles Weitere erledigt.

 **Hinweis**

Zum "Signieren" eines Dokuments müssen Sie dem System ausdrücklich Zugriff auf Ihren privaten Schlüssel einräumen. Wenn Ihr privater Schlüssel z. B. auf einer Smartcard abgelegt ist, müssen Sie erst eine PIN oder Kennphrase eingeben, damit das System auf die Smartcard zugreifen kann.

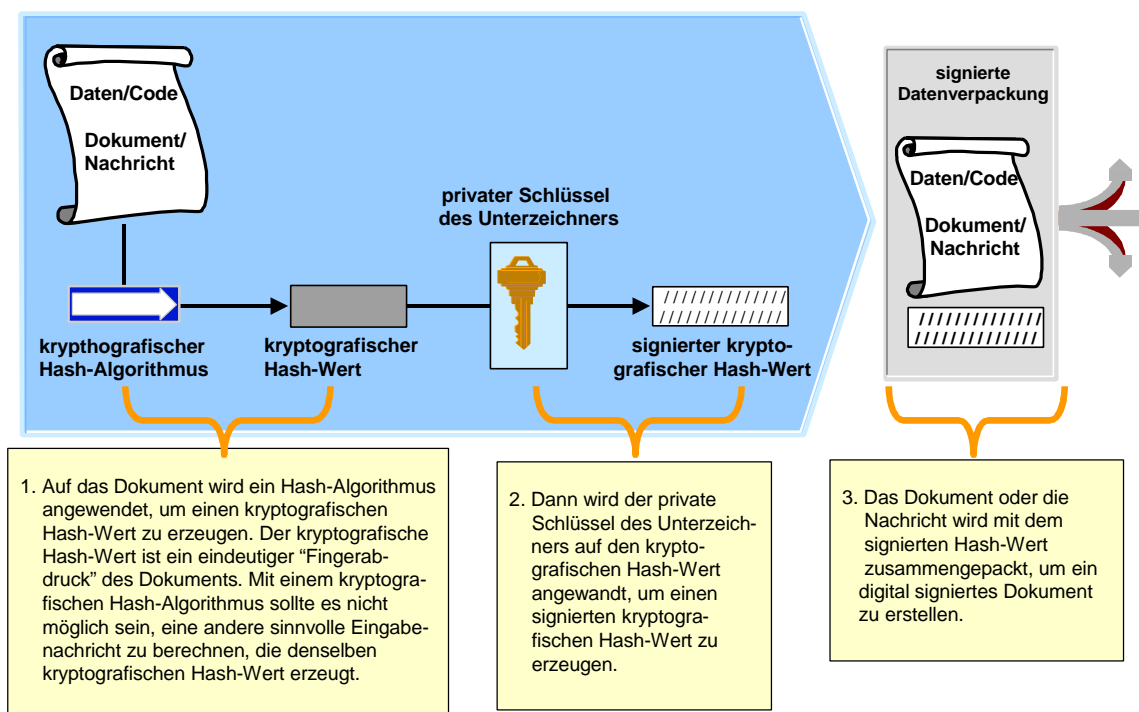


Abbildung 3-8: Digitale Signatur

Secure-Store-&-Forward-Mechanismen (SSF) und Digitale Signaturen

Jeder, der Zugriff auf den öffentlichen Schlüssel des Unterzeichners hat, kann die Umwandlung rückgängig machen und aus dem signierten kryptografischen Hash-Wert einen kryptografischen Hash-Wert erhalten. Um die Echtheit der digitalen Signatur und die Integrität der Daten zu prüfen, wird dieselbe Hash-Funktion auf das Dokument angewandt und das Ergebnis mit dem kryptografischen Hash-Wert verglichen. Stimmen die beiden kryptografischen Hash-Werte überein, ist die digitale Signatur gültig.

Nur der öffentliche Schlüssel, der zum privaten Schlüssel gehört, mit dem signiert wurde, liefert eine positive Überprüfung der digitalen Signatur. Die Überprüfung ist ebenfalls nicht erfolgreich, wenn die digitale Signatur oder das Dokument nach der Signierung verändert wurden. Somit beweist eine positive Überprüfung sowohl die Authentizität des Unterzeichners als auch die Integrität des Dokuments.

Digitale Umschläge

Mit digitalen Umschlägen können Sie sicherstellen, daß der Dokumenteninhalte nur von den Empfängern gelesen werden kann, für die er bestimmt war. Sie erstellen einen digitalen Umschlag, indem Sie einen geheimen Nachrichtenschlüssel zum "Verpacken" des Dokuments in einen "Umschlag" verwenden. Der Empfänger der Nachricht muß diesen Schlüssel ebenfalls kennen, um das Dokument entschlüsseln zu können. Daher verschlüsseln Sie als Teil des digitalen Umschlages den Nachrichtenschlüssel mit dem öffentlichen Schlüssel des Empfängers und versenden diesen zusammen mit dem Dokument. Dieser Vorgang wird in Abbildung 3-9 dargestellt.

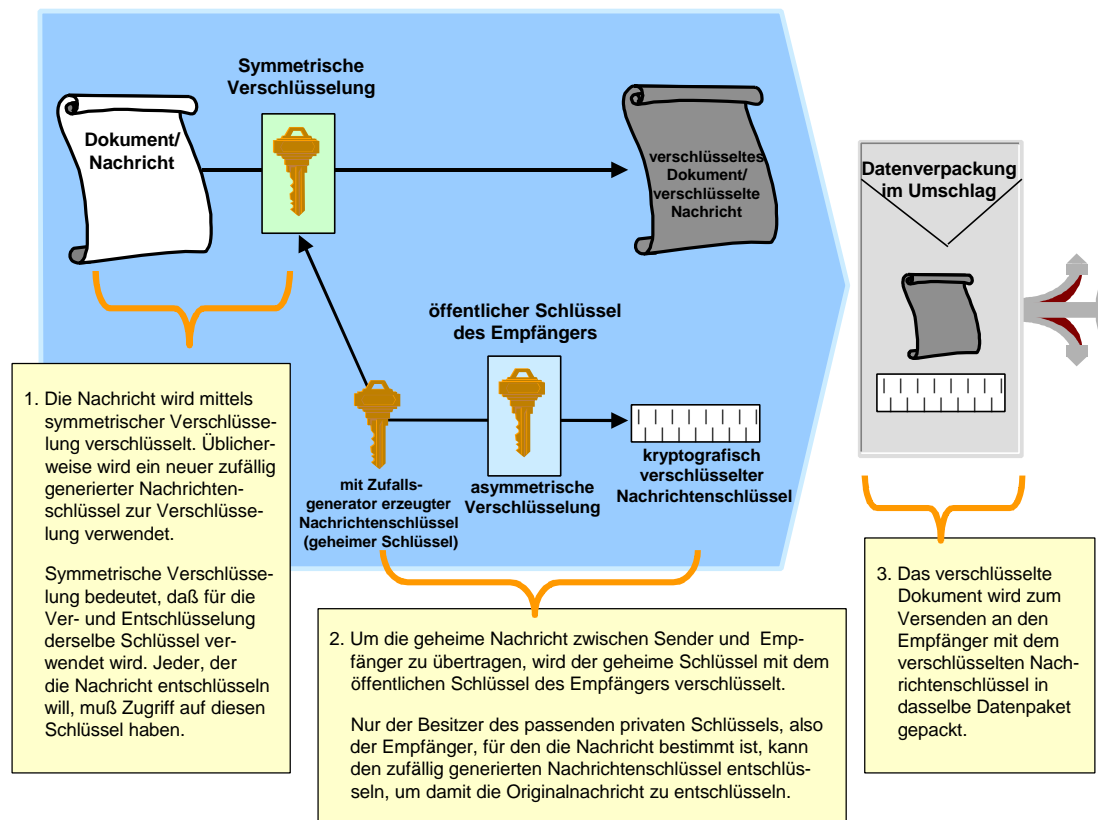


Abbildung 3-9: Digitaler Umschlag

Der Empfänger des Dokuments entschlüsselt mit seinem privaten Schlüssel den Nachrichtenschlüssel, mit dem er dann das Dokument entschlüsseln kann.

Public-Key-Infrastruktur

Damit Sie digitale Signaturen erfolgreich einsetzen können, muß eine Public-Key-Infrastruktur (PKI) eingerichtet werden. Die PKI generiert und verteilt die Schlüsselpaare. Da PKI noch nicht weltweit verfügbar ist, müssen Sie entweder Ihre eigene PKI einrichten oder sich auf ein Trust Center als PKI-Serviceanbieter verlassen. Ob sich Ihre eigene lokale PKI für eine sehr begrenzte Anzahl von Benutzern einfach einrichten läßt, hängt von dem verwendeten externen Sicherheitsprodukt ab. Selbst wenn die Einrichtung einer lokalen PKI relativ einfach ist, kann die Verbindung Ihrer PKI mit der Ihres Kunden bzw. Geschäftspartners weitaus aufwendiger sein. Wenn Sie und Ihre Partner sich auf ein gemeinsames Trust Center einigen, können Sie viele PKI-Probleme vermeiden.

Anwendungsszenarios

Die SSF-Funktionen können in verschiedenen Szenarios zur Sicherung von Daten und Dokumenten angewandt werden. Sie können digitale Signaturen zum Unterzeichnen verschiedener Arten elektronischer Dokumente wie Zahlungsanforderungen, Bestellungen oder Verträgen verwenden. Zu den typischen R/3-Anwendungsszenarios zählen:

- Die SSF verwendende Anwendung konvertiert die Klartextdaten des SAPgui in das sichere Format und speichert sie in der R/3-Datenbank. Wenn die Anwendung später auf die Daten zugreift, liest sie die Daten aus der Datenbank und entschlüsselt sie, wobei sie ebenfalls SSF-Funktionen verwendet. Wenn die Daten mit einer digitalen Signatur unterzeichnet wurden, kann die Anwendung auch die digitale Signatur überprüfen.
- Die Anwendung liest Daten aus der R/3-Datenbank und bereitet sie für einen externen Transport oder ein externes Ablegen vor. Dazu konvertiert sie zunächst die Daten in das entsprechende externe Format und macht sie dann unter Verwendung der SSF-Funktionen sicher. Existieren die Daten erst einmal in dem sicheren Format, kann die Anwendung sie gefahrlos auf einem Speichermedium speichern (z. B. auf einer Platte oder in einem Archiv) oder sie über (möglicherweise) unsichere Kommunikationsverbindungen (wie das Internet) übertragen. Der Empfänger, für den die Daten bestimmt sind, kann entweder ein weiteres R/3-System oder ein anderes System sein, das das verwendete sichere Format unterstützt.
- Die Anwendung erhielt sichere oder digital signierte Daten von einer externen Quelle und importiert sie in das R/3-System. Werden die Daten mit einem SSF-kompatiblen Format sicher gemacht, kann die Anwendung die SSF-Funktionen einsetzen, um sie zu entschlüsseln oder die Signatur zu überprüfen. Beachten Sie, daß die Daten nicht unbedingt von einem R/3-System sicher gemacht werden mußten, allerdings in einem von SSF unterstützten Format.

Externe Sicherheitsprodukte

Auch SSF verwendet ein externes Sicherheitsprodukt mit den PKCS#7-Standards und X.509-Zertifikate zum Signieren und Verschlüsseln von Daten. Das von Ihnen für SSF verwendete Sicherheitsprodukt muß diese Standards unterstützen.

Das externe Produkt ist in der SAP-R/3-Software nicht enthalten. Sie müssen beim entsprechenden Hersteller ein von SAP zertifiziertes Produkt kaufen. Weitere Informationen zur Verwendung digitaler Signaturen in R/3 finden Sie in Hinweis 86927 [14] des Online Service System.

Verfügbarkeit

Die SSF-Mechanismen (digitale Signaturen und digitale Umschläge) sind ab R/3-Release 4.0 verfügbar. Die SAPSECULIB ist ab Release 4.5 verfügbar.

Prüfung und Protokollierung

Die Prüfung und Protokollierung sind ebenfalls wichtige sicherheitsrelevante Aspekte. Nicht nur aus rechtlichen Gründen ist es notwendig, bestimmte Informationen aufzubewahren – Protokolle und Prüfungen sind auch für die Überwachung der Sicherheit Ihres Systems und die Verfolgung von Ereignissen im Fehlerfall wichtig. R/3 führt eine Vielzahl von Protokollen für die Systemverwaltung, Überwachung, Fehlerbehebung und Prüfung. Das **Audit Info System** und das **Security-Audit-Log** sind Teile des Sicherheitsservices in R/3.

Zu den zusätzlichen Protokollen zählen das Systemprotokoll, die statistischen Aufzeichnungen im CCMS (Computing Center Management System), Änderungsbelege für Business-Objekte und die Anwendungsprotokollierung. In der folgenden Beschreibung haben wir diese Protokolle zwar nicht berücksichtigt, aber Sie finden Informationen dazu im *R/3-Sicherheitsleitfaden: BAND II*.

Das Audit Info System (AIS)

Das Audit Info System (AIS) ist ein Auditing-Werkzeug, mit dem Sie die Sicherheitsaspekte Ihres R/3-Systems genau analysieren können. AIS ist ein Werkzeug für Revisoren, die in folgenden Bereichen tätig sind:

- interne oder externe Revisionen
- Systemrevision
- Datensicherheit

Das AIS ist für kaufmännische Revisionen und Systemrevisionen konzipiert. Ein Revisor (oder Systemverwalter) kann mit AIS die Sicherheit des R/3-Systems überprüfen. AIS kann z. B. für folgende Revisionsarten sinnvoll eingesetzt werden:

- das laufende Controlling
- Zwischenprüfungen
- Realtime-Prüfung Ihres Produktivsystems

Das AIS zeigt die Informationen in der Audit-Info-Struktur (ähnlich dem IMG) an, damit Sie einfach ermitteln können, welche Aktivitäten Sie durchführen müssen und welche Sie beendet haben. AIS arbeitet prozeßorientiert mit einem hierarchischen Aufbau, so daß Sie Zugriff auf hochverdichtete Daten bis hin zu einzelnen Dokumenten haben. Da die Revisoren mit AIS direkt im Dialog in einem Produktivsystem arbeiten, erhalten sie Realtime-Informationen.

Verfügbarkeit

AIS ist ab Release 3.11 und 4.6 als Standardkomponente verfügbar. Sie können es auch in andere Releases (ab 3.0D) importieren. Weitere Informationen über das AIS und seine Verfügbarkeit finden Sie im Online Security System in den Hinweisen 77503 [15] und 100609 [16].

Das Security-Audit-Log

Sie können das Security-Audit-Log verwenden, um sicherheitsrelevante Systeminformationen wie z. B. Änderungen an Benutzerstammsätzen oder erfolglose Anmeldeversuche aufzuzeichnen. Das Security-Audit-Log ist auch ein Werkzeug für Revisoren oder Systemverwalter, die sich die Ereignisse im SAP-R/3-System detailliert ansehen müssen. Durch Aktivierung des Audit-Logs werden die Aktionen aufgezeichnet, die Sie für Ihr Audit angeben. Sie können dann in Form eines Audit-Analysereports auf diese Informationen zugreifen und sie auswerten.

Das Security-Audit-Log ermöglicht einen langfristigen Zugriff auf Daten. Die Audit-Dateien werden so lange aufbewahrt, bis Sie sie explizit löschen oder archivieren. Momentan unterstützt das Security-Audit-Log die automatische Archivierung der Protokolldateien nicht. Sie können diese jedoch jederzeit manuell archivieren.

Im Security-Audit-Log können Sie folgende Informationen aufzeichnen:

- erfolgreiche und erfolglose Anmeldeversuche im Dialog
- erfolgreiche und erfolglose Anmeldeversuche per RFC
- RFC-Aufrufe von Funktionsbausteinen
- Änderungen an Benutzerstammsätzen
- erfolgreiche und erfolglose Transaktionsstarts
- Änderungen an der Audit-Konfiguration

Verfügbarkeit

Das Security-Audit-Log ist ab Release 4.0 verfügbar.

Sicherheit für R/3-Internet-Anwendungen

R/3-Internet-Anwendungskomponenten (IACs) ermöglichen Benutzern die Abwicklung von Geschäftsprozessen im R/3 mit einem World-Wide-Web-Browser statt des SAPgui als Benutzungsoberfläche.

Wir stellen verschiedene IACs zur Verfügung, die Sie direkt nutzen oder Ihren eigenen Bedürfnissen anpassen können. Sie können z. B. die Web-Benutzungsoberfläche unternehmensspezifisch gestalten. Des Weiteren können Sie Ihre eigenen Internet-Anwendungskomponenten entwickeln.

Der Internet Transaction Server (ITS) fungiert als Verbindung zwischen dem R/3-System und dem Web. Er ermöglicht eine effiziente Kommunikation zwischen den beiden Systemen trotz deren technischer Unterschiede.

ITS-Architektur

Der Aufbau des ITS sorgt für sichere R/3-Internet-Anwendungen. Der Internet Transaction Server befindet sich zwischen dem Web-Server und dem R/3-Anwendungsserver. Er steuert den Datenfluß zwischen dem R/3-System und dem Internet und bietet Zugriff auf die Internet-Anwendungskomponenten.

Der ITS besteht aus zwei Komponenten, dem WGate und dem AGate. Das WGate befindet sich auf dem Web-Server und verbindet ihn mit dem ITS. Das AGate befindet sich meist auf einem anderen Server und ist für die Kommunikation zwischen dem ITS und R/3 verantwortlich. Es baut die Verbindung auf, generiert HTML-Dokumente und verwaltet den Sitzungskontext sowie die Anmeldedaten.

Dieser Aufbau wird in Abbildung 3-10 gezeigt.

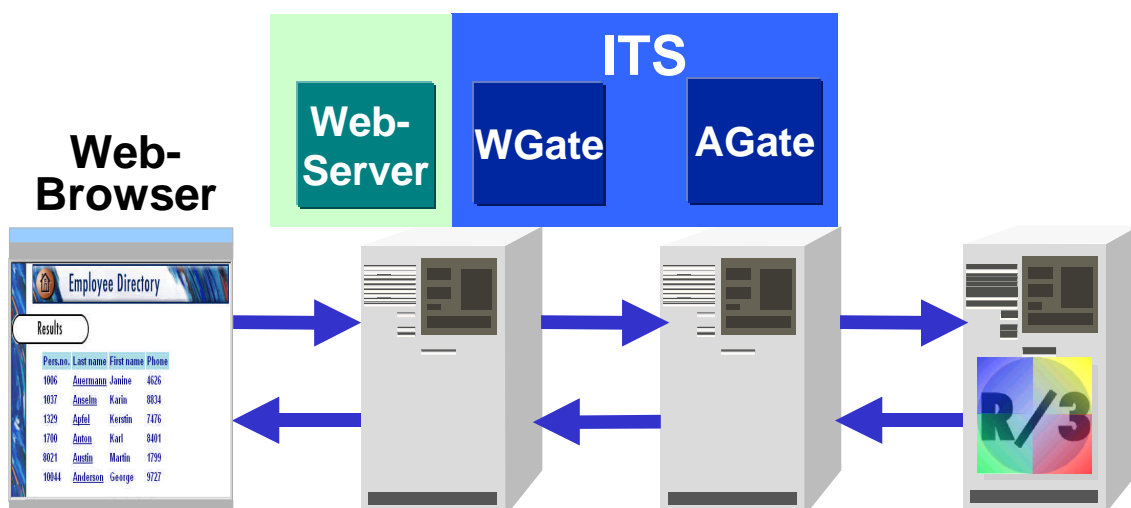


Abbildung 3-10: Der Internet Transaction Server

Kapitel 3: Die R/3-Sicherheitsservices

Die R/3-Internet-Architektur enthält viele Sicherheitsfunktionen wie z. B. die Möglichkeit, das WGate und das AGate auf verschiedenen Hosts zu betreiben. Wir empfehlen Ihnen dringend, eine Netzwerk-Infrastruktur aufzubauen, die diese Funktionen verwendet, um den Zugriff aus dem Internet auf interne Netzwerke zu kontrollieren. Außerdem empfehlen wir Ihnen die Verwendung weiterer Sicherheitskomponenten wie z. B. Firewalls, Paketfilter und SAProuter, um die einzelnen Bestandteile des Netzwerks voneinander zu trennen. Abbildung 3-11 zeigt einige Komponenten, mit denen Sie eine sichere Netzwerkarchitektur aufbauen können, wenn Sie den ITS verwenden.

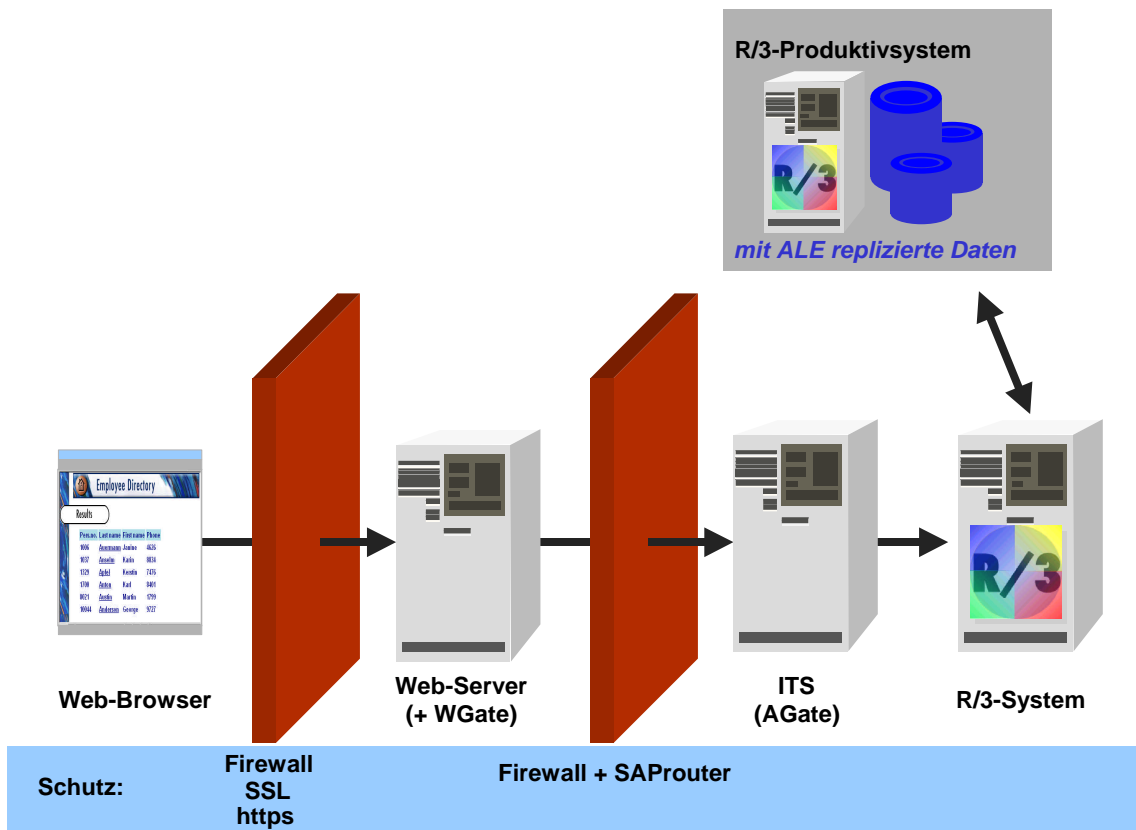


Abbildung 3-11: ITS-Sicherheit

Abhängig von Ihrem Sicherheitskonzept können Sie einige oder alle dieser Komponenten implementieren.

Hinweis

Um die Performance zu verbessern und die Datenmenge, die Ihren Internet-Anwendungen zur Verfügung steht, zu verringern, empfehlen wir Ihnen, anstelle Ihres Produkktivsystems ein separates (mit Application Link Enabling repliziertes) System für Ihr "Internet-System" zu verwenden.

Verwendung von Sicherheitsservices / Vertraulichkeit

Üblicherweise werden im Internet alle Daten in Klartext übertragen. Durch Verschlüsselung können Sie die Vertraulichkeit dieser Daten erhalten. Folgende Verschlüsselungsmethoden können bei Verwendung des ITS eingesetzt werden:

- **zwischen dem Web-Browser und dem Web-Server**
 - das Secure-Sockets-Layer-Protokoll (SSL)
- **zwischen dem WGate und dem AGate**
 - ITS 1.0 und 1.1: statischer Schlüssel
 - ITS 2.0: SNC
- **zwischen dem AGate und R/3**
 - SNC (ab Release 4.5)

Verfügbarkeit

Ab Release 3.1G ist das ITS Teil der Standardauslieferung.

WGate unterstützt folgende Web-Server-Standardschnittstellen:

- Microsoft Information Server API (ISAPI) unter Windows NT
- Netscape Server API (NSAPI) unter Windows NT
- Common Gateway Interface (CGI) unter UNIX und AS/400 (ab Release 4.5)

AGate ist nur als Windows-NT-Service verfügbar.

Kapitel 4: Kundenservices

Wir bieten Ihnen die R/3-Sicherheitsservices und den *R/3-Sicherheitsleitfaden* an, um Sie bei der Analyse und Einbindung von Sicherheitsaspekten in das R/3-System zu unterstützen. Zusätzlich zu diesen R/3-Services bieten wir im Zusammenhang mit Sicherheit spezielle Kundenservices an. Dazu zählen

- das **Security Consulting Team**, das Teil der SAP Technical Consulting Services ist und individuelle Beratungsleistungen in Sicherheitsfragen anbietet
- die **SAP Audit User Group**, die verschiedene Richtlinien herausgegeben hat, die Sie zur Prüfung Ihres R/3-Systems verwenden können
- unsere **Feedback-Bogen**. Wir empfehlen, uns hierin mitzuteilen, inwieweit der R/3-Sicherheitsleitfaden und die damit verbundenen Sicherheitsservices Ihren Bedürfnissen entsprechen.

Diese Kundenservices werden im folgenden genauer beschrieben.

Security Consulting Team

Die Erstellung, Verwaltung und Einhaltung eines effektiven Sicherheitskonzepts erfordert unterschiedlichste Erfahrung und Fachkenntnisse. Um Sie bei der Einführung und Einhaltung Ihres Sicherheitskonzepts zu unterstützen, steht Ihnen unser Security Consulting Team, ein Teil der SAP Technical Consulting Services, zur Seite. Das Team verfügt über weitreichende Erfahrung in Sicherheitsfragen. Wenn der *R/3-Sicherheitsleitfaden* nicht alle Ihre Fragen in gewünschtem Maße beantwortet oder wenn Sie weitere Fragen haben, wenden Sie sich an unser Security Consulting Team.

Die Services des Security Consulting Team umfassen die Sicherheitsanalyse Ihres Systems, die Beratung bei der Ausarbeitung Ihres Sicherheitskonzepts, die Einführung in Techniken der Berechtigungskonzepte und die individuelle Beratung in Sicherheitsfragen.

Die folgenden Services sind verfügbar:

- **Umfassende Sicherheitsanalyse**

Wir führen eine detaillierte Sicherheitsanalyse Ihres R/3-Systems unter technischen Gesichtspunkten durch. Die Analyse umfaßt

- die Analyse der technischen Systemsicherheit auf allen Ebenen (insbesondere der R/3-Systeme)
- die Analyse aller sicherheitsrelevanten Verfahren.

- **Sicherheitsreview**

Wir führen nach technischen Aspekten ein Sicherheitsreview eines R/3-Systems durch. Die Analyse umfaßt

- die Analyse der technischen Systemsicherheit, auf kritische Bereiche begrenzt
(Diese Prüfung ist auf ein einziges R/3-System begrenzt.)

Kapitel 4: Kundenservices

- **Betreuung für firmenspezifischen Sicherheitsleitfaden**

Wir beraten bei der Ausarbeitung und Einführung eines eigenen, firmenspezifischen R/3-Sicherheitsleitfadens. Unsere Beratung umfasst

- die Analyse der sicherheitsrelevanten Workflows
- die Entwicklung sicherheitsfördernder Verfahren
- die Dokumentation der Verfahren in Ihrem firmenspezifischen Sicherheitsleitfaden
- die Beratungsleistung während der Einführung des Leitfadens

- **Workshop: Berechtigungskonzept**

Wir helfen Ihnen bei der Planung einer optimalen Einführung des Berechtigungskonzepts. Wir erklären

- die Berechtigungsprüfungen und wie sie funktionieren
- die Werkzeuge zur Profilgenerierung
- die Konzepte für Verfahren der Profiltzuweisung in der Einführungsphase
- die Verteilung der Benutzerverwaltungsaufgaben

- **NT-Domänenkonzept**

Wir helfen Ihnen beim Aufbau eines kundenspezifischen Domänenkonzepts zur Sicherung Ihres Betriebssystems, Ihrer Datenbank sowie Ihrer weiteren Ressourcen. Die Inhalte umfassen

- das Definieren eines Benutzerkonzepts (Benutzergruppen und Zugriffsprivilegien)
- das Erstellen von Einführungsleitfäden
- das Sicherstellen der Einbindung der R/3-Umgebung unter einer Windows-NT-Domäne

- **Schulung CA900 Technical System Security**

Wir bieten die Schulung CA900 Technical System Security an. Dieser Kurs umfasst

- das Sicherheitskonzept
- die technische Umgebung des R/3-Systems
- die Zugriffskontrolle in der R/3-Umgebung
- die Entwicklungsumgebung in R/3
- das R/3-Transportsystem
- die Sicherheitsaspekte der R/3-Verwaltung
- den Internet Transaction Server (ITS)
- die System-Audit-Werkzeuge

- **Sicherheitsaspekte bei der Verwendung des Internet Transaction Server**

Wir erklären alle sicherheitsrelevanten Aspekte bezüglich ITS, einschließlich

- der Architektur des ITS
- der Integration des ITS in eine bestehende Systemlandschaft
- der Schutzmechanismen des R/3-Systems und des ITS
- der sicherheitsrelevanten Aspekte beim Konfigurieren des ITS

Weitere Informationen erhalten Sie beim Security Consulting Team in der Abteilung Technische Beratung (Technical Consulting Department) unter

Tel. **+49 6227 / 7-41537**

Fax: **+49 6227 / 7-44640**

SAP Audit User Group

Die Audit User Group ist ein Forum für die Diskussion verfahrensorientierter Audits sowie Systemprüfungen, die auf SAP-Installationen und -systemen durchgeführt werden. Die User Group besteht aus Revisoren und IT-Auditoren, die entweder SAP-Anwendungen prüfen oder deren Firmen SAP-Software einsetzen. Ihre Aufgabe ist es, die Benutzeranforderungen zu diskutieren und die Empfehlungen, wie der Einsatz der SAP-Software zu verbessern wäre, zu überprüfen.

Die Audit User Group (und ihre Arbeitskreise) hat folgende Richtlinien und Dokumentation für die Prüfung der SAP-Systeme erstellt:

- *SAP-Prüfleitfaden R/2 RF*, Materialnummer 50019056 [22]
- *SAP-Prüfleitfaden R/3 FI/MM*, Materialnummer 50014633 [23]
- *SAP-Leitfaden Datenschutz R/3*, Materialnummer 50024598 [24]
- *AIS Fact Sheet*, Materialnummer 50024770 [25]

Außerdem bieten wir die Schulung AC900 Interne und Externe Revision an.

Weitere Informationen über die SAP Audit User Group und die entsprechenden Richtlinien finden Sie unter dem Link www.sap.com/germany/contact/user.htm, dort wählen Sie *Arbeitskreis "Revision R/2 und R/3"*. [26]

Feedback

Wir möchten wissen, wie gut der R/3-Sicherheitsleitfaden Ihren Bedürfnissen entspricht. Verwenden Sie für Ihre Anmerkungen zu Inhalt oder Qualität des Leitfadens den Feedback-Bogen im Anhang und senden Sie ihn an folgende Adresse bzw. Faxnummer:

SAP AG
Abteilung CCMS & Security
Postfach 1461
D-69190 Walldorf

Fax: **+49-6227 / 7-41198**



Kapitel 4: Kundenservices

Anhang A: Zusatzinformationen

In der folgenden Dokumentation finden Sie Zusatzinformationen über die einzelnen R/3-Sicherheitsservices:



Hinweis

Für die R/3-Online-Dokumentation werden die Pfade für Release 3.1H und 4.0B angegeben. In anderen Releases können die Menüpfade leicht abweichen.

Tabelle 2: Zusatzinformationen

Nr.	Beschreibung
Benutzerauthentifizierung	
[1]	<u>Online-Service-System-Hinweis 2467</u> : Antworten zum Thema Sicherheit bei SAP
[2]	<u>Online-Service-System-Hinweis 138498</u> : Single Sign-On Solutions
R/3-Berechtigungskonzept	
[3]	<u>SAP-Dokumentation: Authorizations Made Easy Guide</u> : Materialnummer 50020475 (Release 3.0F) Materialnummer 50021412 (Release 3.1G/3.1H) Materialnummer 50023994 (Release 4.0A/4.0B)
[4]	<u>R/3-Online-Dokumentation: BC – Benutzer und Berechtigungen</u> Release 3.1H: <i>Basis → Systemverwaltung → Benutzer und Berechtigungen</i> Release 4.0B: <i>BC – Basis → Computing Center Management System → BC – Benutzer und Berechtigungen</i>
[5]	<u>Einführungsleitfaden</u> <i>Basis → Systemadministration → Benutzer und Berechtigungen → Berechtigungen und Profile mit dem Profildgenerator pflegen</i>
[6]	<u>SAP ASAP Implementation Roadmap: (Work-package 3.11) Phase 3: Realisierung – Berechtigungskonzept erarbeiten</u>
Netzwerkinfrastruktur	
[7]	<u>BC SAProuter</u> Release 3.1H: <i>R/3 Service und Support → SAProuter</i> Release 4.0B: <i>BC – Basis → Kernel-Komponenten → BC – SAProuter</i>
[8]	<u>Online-Service-System-Hinweis 30289</u> : SAProuter-Dokumentation
[9]	<u>SAP-Dokumentation: Secure Network Communications und Secure-Store-&-Forward-Mechanismen mit R/3</u> , Materialnummer 50014335
[10]	<u>SAP-Dokumentation: SNC-Benutzerhandbuch</u> , ITS-Präsentations-CD im Verzeichnis <i>Docu → SNC</i> oder unter dem SAPNet-Alias "systemmanagement" (z. B. http://sapnet.sap.com/systemmanagement) und dann <i>Media Center → Security → Literature</i>
[11]	<u>Online-Service-System-Hinweis 66687</u> : Einsatz von Netzwerksicherheitsprodukten
[12]	<u>Complementary Software Program</u> : Im SAPNet den Alias "csp" (z. B.: http://sapnet.sap.com/csp) eingeben und auf den Link <i>Complementary Solutions → Network security</i> klicken

Tabelle 2: Zusatzinformationen (Fortsetzung)

Nr.	Beschreibung
Secure-Store-&-Forward-Mechanismen (SSF) und Digitale Signaturen	
[13]	<u>SAP-Dokumentation: Secure Network Communications und Secure-Store-&-Forward-Mechanismen mit R/3</u> , Materialnummer 50014336
[14]	<u>Online-Service-System-Hinweis 86927</u> : Benutzung der digitalen Signatur im R/3-System
Prüfung und Protokollierung	
[15]	<u>Online-Service-System-Hinweis 77503</u> : Audit Information System (AIS) Version 1.5
[16]	<u>Online-Service-System-Hinweis 100609</u> : Audit Information System (AIS) – Installation
[17]	<u>BC – Systemdienste → Security-Audit-Log</u> Release 3.1H: nicht verfügbar Release 4.0B: <i>BC – Basis → Kernel-Komponenten → BC – Systemdienste → Security-Audit-Log</i>
Sicherheit für R/3-Internet-Anwendungen	
[18]	<u>R/3-Internet-Anwendungskomponenten</u> Release 3.1H: <i>Anwendungsübergreifende Funktionen → SAP@WEB → R/3-Internet-Anwendungskomponenten</i> Release 4.0B: <i>CA – Anwendungsübergreifende Komponenten → Business Framework Architecture → Internet-Anwendungen → R/3-Internet-Anwendungskomponenten</i>
[19]	<u>Online-Service-System-Hinweis 60058</u> : Sicherheit für R/3-Release 3.1 im Internet
[20]	<u>Online-Service-System-Hinweis 104576</u> : Paketfilter (Firewall) zwischen ITS und R/3
Damit verbundene Richtlinien	
[21]	<u>SAP Audit User Group</u> : Unter www.sap.com/germany/contact/user.htm dann wählen Sie <i>Arbeitskreis Revision R/2 und R/3</i>
[22]	<u>SAP-Dokumentation: SAP-Prüfleitfaden R/2 RF</u> , Materialnummer 50019056
[23]	<u>SAP-Dokumentation: SAP-Prüfleitfaden R/3 FI / MM</u> , Materialnummer 50014633
[24]	<u>SAP-Dokumentation: SAP-Leitfaden Datenschutz R/3</u> , Materialnummer 50024598
[25]	<u>SAP-Dokumentation: AIS Fact Sheet</u> , Materialnummer 50024770

Index

A

AGate	3-17, 3-18, 3-19
AIS	Siehe Audit Info System
Analyse, System (Beratungsservices)	4-1
Aspekte, Sicherheit	1-1, 2-1–2-4
Authentifizierung	2-1
Berechtigung	2-2
Integrität	2-2
Prüfung und Protokollierung	2-3
Unleugbarkeit (Verbindlichkeit)	2-3
Vertraulichkeit	2-3
Audit Info System (AIS)	2-3, 3-15
Authentifizierung	2-1, 3-2–3-4

B

Beratung	4-2, 4-1–4-3
Berechtigung	2-2
Berechtigungsprüfungen	2-2, 3-5
Bildschirmschoner	3-4

C

Complementary Software Program	3-10
--------------------------------	------

D

Datenschutz	4-3
Digitale Signaturen	2-2, 2-3, 3-11–3-14
Digitale Umschläge	2-3, 3-11, 3-13

F

Feedback	4-3
Firewall	3-8, 3-18

G

GSS-API V2	3-9
------------	-----

I

Info-System Berechtigungen	2-2, 3-7
Integrität	2-2
Internet Transaction Server (ITS)	3-17, 3-18, 3-19
Beratungsservices	4-3
Internet-Anwendungen, Sicherheit für	3-17, 3-16–3-19
ITS	Siehe Internet Transaction Server

K

Kennwörter	2-1, 3-2
Kundenservices	4-1–4-3

N

Netzwerkkommunikation	3-8–3-10
mit Internet-Anwendungen	3-18

NT LAN Manager Security Provider (NTLMSSP)	3-3
NT-Domänenkonzept (Beratungsservices)	4-2

Ö

Öffentlicher Schlüssel	3-11
------------------------	------

P

PKI	Siehe Public-Key-Infrastruktur
Privater Schlüssel	3-12
Profilgenerator	2-2, 3-6
Protokollierung	2-2, 2-3, 3-14–3-16
Prüfung	2-3, 3-14–3-16
User Group	4-3
Public-Key-Infrastruktur (PKI)	3-14
Public-Key-Technologie	3-11
Public-Key-Zertifikat	3-12

R

R/3-Berechtigungskonzept	2-2, 2-3, 3-4–3-7
Workshop zum	4-2
Richtlinien	
Datenschutz	4-3
Prüfung R/2	4-3
Prüfung R/3 FI	4-3
Prüfung R/3 MM	4-3

S

SAP Audit User Group	4-3
SAP Security Library (SAPSECULIB)	3-11, 3-14
SAP Technical Consulting Services	
	4-1, 4-2, 4-1–4-3
SAP*	3-2
SAProuter	3-8–3-9
Einsatz von SNC-Sicherung	3-10
mit dem ITS	3-18
SAPSECULIB	Siehe SAP Security Library
Schulung CA900 Technical System Security	4-2
Secure Network Communications (SNC)	3-9–3-10
Authentifizierung	2-1
Integritätsschutz	2-2, 3-9
mit dem ITS	3-19
mit dem SAProuter	3-10
Schutz der Vertraulichkeit	2-3, 3-9
Single Sign-On	3-3, 3-9
Smartcards	3-3, 3-9
Secure Store and Forward (SSF)	3-11–3-14
Siehe auch Digitale Signaturen oder digitale Umschläge	
Verbindlichkeit	2-3
Secure-Sockets-Layer-Protokoll (SSL)	3-19
Secure-Store-and-Forward-Mechanismen (SSF-Mechanismen)	
Schutz der Integrität	2-2

Index

Security Consulting Team	4-1, 4-2, 4-1-4-3	U	
Security-Audit-Log	2-3, 3-16	Unleugbarkeit	2-3
Sicherheitskonzept	1-1, 1-2, 2-1	V	
als Teil des CA900	4-2	Verbindlichkeit	2-3
Sicherheitsleitfaden, firmenspezifisch	4-2	Verschlüsselung	2-3, 3-9, 3-11
Single Sign-On	2-1, 3-3, 3-9	mit Internet-Anwendungen	3-19
Smartcards	2-1, 3-3, 3-9	Vertraulichkeit	2-3
SNC	Siehe Secure Network Communications	Viren	2-2
Sperren, Benutzer und Sitzung	2-1, 3-4	W	
Sperrmechanismus	2-2	Web-Server	3-17, 3-19
SSF	Siehe Secure Store and Forward	WGate	3-17, 3-18, 3-19
T			
Trust Center	3-14		

