SSONET
Sicherheit und Schutz in offenen Datennetzen

Projektnummer: 110602/13
Förderungskennzeichen: QIT 2005

Projektleiter: Prof. Dr. Andreas Pfitzmann
Prof. Dr. Alexander Schill

Autoren: Dipl.-Wirtsch.-Inf. Guntram Wicke
Dipl.-Inform. Gritta Wolf
Dipl.-Inform. Jan Zöllner

Sicherheitskonzepte am Beispiel konkreter Anwendungen

Anforderungsanalyse bezüglich Sicherheit und Schutz am Beispiel konkreter Anwendungen mit Einbettung in Grob-Sicherheitsarchitektur für mehrseitige Sicherheit

1. Zwischenbericht
zum 31.08.1996

Inhaltsverzeichnis

ABSTRACT ..... **III**

EXECUTIVE SUMMARY ..... **V**

1 MOTIVATION **1**

2 ANFORDERUNGSANALYSE **2**

2.1 ANWENDUNGSBEISPIEL: ELEKTRONISCHER ZAHLUNGSVERKEHR 2

2.1.1 Abgrenzung des Themengebietes *2*

2.1.2 Identifizierte Rollen *3*

2.1.3 Interessen und Sicherheitsanforderungen *6*

2.1.4 Beispiele für digitale Zahlungssysteme *10*

2.2 ANWENDUNGSBEISPIEL: WORKFLOW MANAGEMENT 12

2.2.1 Abgrenzung und Einordnung der Begriffe *12*

2.2.2 Identifizierte Rollen *18*

2.2.3 Interessen und Sicherheitsanforderungen *20*

2.2.4 Beispiele konkreter Systeme *26*

2.3 ANWENDUNGSBEISPIEL: MEDIZIN 28

2.3.1 Einleitung *28*

2.3.2 Identifizierte Rollen *29*

2.3.3 Interessen und Sicherheitsanforderungen *30*

2.3.4 Konkrete Problemsituationen *31*

3 GROB-SICHERHEITSARCHITEKTUR **34**

3.1 EINFÜHRUNG 34

3.2 GROB-SICHERHEITSARCHITEKTUR-VARIANTEN 35

3.2.1 Variante mit SW-Schirmungsschicht *35*

3.2.2 Variante mit sich selbst schützendem Betriebssystemkern *36*

3.2.3 Gegenüberstellung *37*

3.2.4 Verteilte Architektur *37*

4 AUSBLICK **40**

5 LITERATUR **41**

Abstract

Bei herkömmlicher Betrachtung von Sicherheit werden meist nur die Schutzinteressen eines - im allgemeinen stärkeren Partners oder des Systembereitstellers gewahrt. Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen nicht nur einer der beteiligten Parteien. Ausgehend von Anwendungsszenarien aus den Bereichen der Zahlungssysteme, der Workflow Management Systeme und der Medizin werden Rollen identifiziert, die die jeweils einander gegenübertretenden Seiten einer Kommunikationsbeziehung repräsentieren können. Aus den bezüglich der Rollen existierenden Sicherheitsinteressen ergeben sich Anforderungen an die zu konzipierende Architektur für mehrseitige Sicherheit.

Executive Summary

Warum mehrseitige Sicherheit?

Menschen verfolgen in ihrem täglichen Leben bestimmte Interessen. Naturgemäß stimmen diese nicht immer mit denen anderer Menschen überein, so daß sich Konflikte ergeben. Das Konfliktpotential führt zu Sicherheitsinteressen und entsprechenden Sicherheitsanforderungen.
Dies kann man bei vielen rechtlich relevanten Aktivitäten wie z.B. Vertragsabschlüssen beobachten. In diesen Anwendungsfeldern wird mehrseitige Sicherheit praktiziert: Alle Beteiligten haben eine gleichberechtigte Chance, ihre Interessen zu formulieren und einen Aushandlungsprozeß durchzuführen, um zu einer gemeinsamen Lösung zu gelangen.
Wenn man solche Aktivitäten mittels EDV-Systemen realisiert, ergeben sich keine grundsätzlichen Änderungen, auch wenn sich die technischen Rahmenbedingungen verschieben: Es gibt weiterhin Beteiligte und deren Interessen, die ggf. durch die IT-Systeme erweitert werden.
Das Ziel beim Einsatz von Rechentechnik ist es, den gewohnten Sicherheitsstandard mindestens beizubehalten. So wird versucht, bewährte Konzepte wie die eigenhändige Unterschrift oder die Beglaubigung durch Dritte umzusetzen.
Die üblicherweise gebotene Sicherheitsfunktionalität von IT-Systemen beachtet jedoch den Aspekt der Mehrseitigkeit von Sicherheit nur wenig. Dieser Aspekt gewinnt aber zunehmend Bedeutung; nicht zuletzt für die Akzeptanz eines Systems beim Anwender, da er eigene Entscheidungen bezüglich der von ihm geforderten und durchgesetzten Sicherheit treffen möchte.

Drei Anwendungsszenarien

Um eine Vorstellung von Sicherheitsinteressen von Beteiligten zu erhalten, wurden verschiedene Aanwendungsszenarien betrachtet. Dabei sind die Akteure und ihre jeweiligen Sicherheitsinteressen herauszuarbeiten. Im vorliegenden Bericht wurden die Anwendungsgebiete digitale Zahlungssysteme, Workflow Management und Medizin exemplarisch untersucht. Das Rollenkonzept wurde als wesentliches Instrument zur Komplexitätsreduzierung und abstrakten Darstellung jedes Szenarios angewendet.

1. Bei *Zahlungssystemen* ist grundsätzlich zwischen den Rollen auszahlende Bank, einnehmende Bank, Händler und Kunde zu unterscheiden. Da digitaler Zahlungsverkehr auf elektronischem Datentransfer basiert, kommen zwei weitere Rollen ins Spiel: der Zahlungssystembetreiber und der Kommunikationsnetzbetreiber.
   Als Hauptinteressen der Beteiligten wurden der Schutz vor Betrug und die Verfügbarkeit des Systems identifiziert. Das Interesse an Verfügbarkeit des Systems ist für alle Rollen gleich, die Interpretation des Betrugsschutzes erfolgt jedoch unterschiedlich:
   - Die *Banken* sind vornehmlich an der Beweisbarkeit von Transaktionen (wie Geldeinnahme und -ausgabe) sowie der Nichtvermehrbarkeit des Geldes interessiert.
   - Der *Kunde* hingegen ist weniger an Nichtvermehrbarkeit interessiert, fordert jedoch Beweisbarkeit von Transaktionen sowie den Werterhalt des in seinem Besitz befindlichen Geldes.
   - *Händler* sind ebenfalls an beweisbaren Transaktionen interessiert und wollen eine Überprüfung des Geldes auf Gültigkeit, bevor sie Waren übergeben.
   - Für den *Zahlungssystembetreiber* sind Beweisbarkeit sowie Nichtvermehrbarkeit (um nicht für unberechtigte Forderungen aufkommen zu müssen) wichtig.
   - Der *Kommunikationsnetzbetreiber* hat primär keine Interessen bezüglich Betrugssicherheit, da er nur die Kommunikationsfähigkeit sicherstellt.

Eine besonders von den Kunden und Händlern (wenn auch aus unterschiedlichen Motiven) geschätzte Eigenschaft von Bargeld ist die hochgradige Anonymität und Unbeobachtbarkeit

von Transaktionen. Da es sich hierbei um ein wichtiges Akzeptanzkriterium handelt, wird bei vielen aktuellen Entwicklungen auf dem Gebiet der digitalen Zahlungssysteme versucht, diese Eigenschaft zu realisieren.

2. *Workflow Management* befaßt sich mit der Steuerung von Vorgängen über mehrere Arbeitsplätze unter Einbeziehung technischer Basiskomponenten. Diese Vorgänge bestehen in der Regel aus mehreren Teilschritten. Workflow Management soll es ermöglichen, verschiedene Teilschritte nach einem organisatorischen Regelwerk zu koordinieren, zu überwachen und bei Bedarf zu synchronisieren. Die Programme zur Realisierung dieses Konzepts sind Workflow Management Systeme.
   Büromitarbeiter entwickeln bestimmte Interessen bei der Arbeit mit einem Workflow Management System. Das heißt, sie haben neben den Interessen, die sich generell aus dem Arbeitsumfeld (Büroabläufe und -strukturen) ergeben, zusätzliche Interessen, die erst durch den Einsatz eines Workflow Management Systems im Unternehmen entstehen.
   Es treten auch bereits vorhandene Interessen stärker in den Vordergrund, so z.B. Interessen bezüglich des Datenschutzes. Das beruht auf der Tatsache, daß mit der Einführung von Workflow Management Systemen eine minutiöse Überwachung des Arbeitsverhaltens technisch möglich wird.
   Ein weiterer Problempunkt ist die normalerweise durch eigenhändige Unterschrift gegebene Rechtsverbindlichkeit und Eindeutigkeit von Dokumenten. Hier muß bei Workflow Management Systemen der gleiche Status erreicht werden, der in der Papierwelt üblich ist.
3. Die *Medizin* ist traditionell eines der Aufgabengebiete mit höchsten Datenschutzanforderungen, die sich aus der hohen Vertraulichkeit der anfallenden medizinischen und persönlichen Daten ergeben. Weiterhin wird großer Wert auf Verfügbarkeit, Integrität und Zurechenbarkeit von Daten gelegt.
   Bei der Diskussion medizinischer Anwendungen stellte sich heraus, daß alle Rollen ähnliche Interessen bezüglich Integrität und Zurechenbarkeit haben. Aufgrund dieser Tatsache ist die Medizin ein Vorreiter bei der Anwendung digitaler Signaturen.
   Das im medizinischen Umfeld gegebene Konfliktpotential beruht vor allem auf den unterschiedlichen Interessen verschiedener Gruppen in bezug auf Vertraulichkeit bestimmter Daten und ihrer Verfügbarkeit für andere.

Grob-Sicherheitsarchitektur

Das Gesamtziel des Projektes SSONET ist die Konzipierung und prototypische Realisierung einer Architektur für mehrseitige Sicherheit in verteilten Systemen.
Hier werden Systeme betrachtet, an denen mehrere Nutzer beteiligt sind. Üblicherweise verfolgt jeder Nutzer in Abhängigkeit von seiner Rolle, die er im System einnimmt, unterschiedliche Ziele. Das System sollte ihm daher ermöglichen, im eigenen Interesse zu handeln und z.B. bei Nutzung verteilter Anwendungssysteme Sicherheitsinteressen und -bedürfnisse zu formulieren, bei Bedarf auszuhandeln und durchzusetzen.
Es wurden verschiedene Ansätze diskutiert, die sich zunächst mit dem Zusammenspiel zwischen Anwendungen, Betriebssystemen und Sicherheitsmechanismen befassen. Eine Variante ist es, die Sicherheitsfunktionaliät in das Betriebssystem zu integrieren. Alternativ ist es denkbar, eine Schirmungsschicht zu konzipieren, die sich zwischen Anwendungen und dem Betriebssystem befindet. Beide Varianten können auf verteilte Systeme angewendet werden.

Eine besondere Herausforderung besteht in der Balance zwischen freiwilliger oder gar erzwungener Kooperation einerseits und uneingeschränkter bzw. einschränkbarer Autonomie andererseits.

1 Motivation

Menschen verfolgen in ihrem täglichen Leben bestimmte Interessen. Diese stimmen nicht immer mit denen anderer Menschen überein, woraus sich die Zielstellung der Sicherung eigener Interessen ergibt.
Mehrseitige Sicherheit ist gegeben, wenn alle Beteiligten gleichberechtigt an einem Prozeß teilnehmen und ihre jeweiligen Interessen sichern sowie ihre legitimen Ansprüche auch durchsetzen können.
Ein Beleg dafür, daß mehrseitige Sicherheit in wichtigen Bereichen schon immer eine große Rolle spielte, ist die übliche Praxis, alle rechtlich relevanten Aktivitäten zusätzlich zur Speicherung auf elektronischen Datenträgern immer auch auf Papier zu bestätigen. Dabei ist insbesondere die Möglichkeit, allen Beteiligten ein von Hand unterschriebenes Exemplar zur Verfügung zu stellen, von besonderer Bedeutung. Dadurch, daß jeder eine gleiche Kopie besitzt, sind Mißbrauchsmöglichkeiten stark eingeschränkt. Jeder kann sich mit dem ihm vorliegenden Papier auf die darauf fixierten Aussagen (meistens Ergebnisse von Aushandlungsprozessen) stützen und ihre Erfüllung einfordern. Da das jeder Beteiligte tun kann, ist mehrseitige Sicherheit realisiert, wobei ein wichtiger Punkt die Beweisfähigkeit der Dokumente gegenüber Dritten ist. Diese gewährleistet im Normalfall eine gerechte Austragung von Streitfällen.
Eine technische Möglichkeit zur Realisierung dieser Beweismöglichkeit sind digitale Signaturen, deren rechtsverbindliche Anwendung momentan Gegenstand vieler Diskussionen ist.
Man kann an weiteren Beispielen zeigen, daß in vielen „Anwendungen“ des täglichen Lebens üblicherweise mehrseitige Sicherheit realisiert wird. Wenn diese Anwendungen auf (vernetzten) Rechnersystemen ablaufen sollen, so muß das Ziel der Entwickler lauten, die bisherigen Sicherheitsstandards zumindest zu halten oder im günstigen Fall sogar zu verbessern.
Es wird auch versucht, übliche Rechtsprozesse EDV-technisch nachzubilden wie z.B. die eigenhändige Unterschrift durch digitale Signaturen. Ein weiteres Beispiel ist die Einrichtung von sogenannten „Trust-Centern“, die gewisse Notariatsfunktionen (Beglaubigung, Hinterlegung) wahrnehmen können.
Akteure in solchen Szenarien können als in bestimmten Rollen auftretend betrachtet werden; so z.B. als Kunde, Händler, Bank etc. Dieses Rollenkonzept ist ein Mittel zur Komplexitätsreduzierung bei der Sicherheitsbewertung von verschiedenen Anwendungsgebieten und kann zur Abstraktion und Gewinnung allgemeiner Erkenntnisse verwendet werden. Diese ergeben sich vor allem aus der Betrachtung der Sicherheits- und Schutzinteressen verschiedener Rollen und ihrer Gegenüberstellung.
In den nachfolgend aufgeführten Beispielszenarien ist die Identifizierung von Rollen und die Darstellung ihrer Interessen ein wesentliches Instrument zur abstrakten Darstellung des Szenarios und des enthaltenen Konfliktpotentials. Zur Einschätzung des Konfliktpotentials wird dabei vor allem die Gegenüberstellung der Sicherheitsanforderungen der Rollen herangezogen.

2 Anforderungsanalyse

2.1 Anwendungsbeispiel: Elektronischer Zahlungsverkehr

2.1.1 Abgrenzung des Themengebietes

Die durch Einführung von Diensten wie Teleshopping und Electronic Banking gekennzeichnete Entwicklung, die im Umfeld eines entstehenden sog. elektronischen Marktes zu sehen ist, wirft die Frage nach der genügenden Berücksichtigung der Sicherheitsinteressen aller an der Erbringung und Nutzung dieser Dienste Beteiligten auf.

Zur Verdeutlichung wird näher auf den für die Funktion eines modernen Marktes grundlegenden Aspekt der Zahlung eingegangen. Im bekannten elektronischen Zahlungsverkehr schreitet die Entwicklung gegenwärtig rapide fort. Zum Beispiel tritt zu den seit längerem bekannten Point-of-Sale-(POS)-Zahlungen die Verwendung digital gespeicherten Geldes in sog. elektronischen Geldbörsen hinzu. Kreditkartenzahlungen werden z.B. durch Secure Electronic Transactions (SET) für Zahlungen in Netzen interessant.

Von der digitalen Darstellung von Zahlungsmitteln, die Bezug auf Bankkonten nehmen, hin zur digitalen Banknote erscheint alles wünschenswert, was sich bisher schon als Zahlungsmittel bewährt hat, um die Dienstleistungspotentiale eines offenen Kommunikationsnetzes wirtschaftlich zu nutzen. Der Einsatz digitaler Zahlungssysteme im sog. elektronischen Markt sollte jedoch mindestens ebenso sicher möglich sein, wie es Zahlungen auf konventionellem Wege sind. Die einfache Übertragung des Zahlungsmittels in eine digitale Repräsentation für das offene Kommunikationsnetz ist mit zwei schwerwiegenden Nachteilen verbunden. Im Gegensatz zu den meisten herkömmlichen Zahlungsmitteln kann digital dargestelltes Geld ohne weiteres vervielfältigt werden, ohne daß sich die Kopie vom Original unterscheidet. Außerdem kann jede Information, z.B. der repräsentierte Betrag eines Schecks, manipuliert werden, ohne daß das nachzuweisen wäre. Hier sind also Schutzmaßnahmen, insbesondere aus dem Bereich der Kryptographie bekannte, notwendig, die von bisherigen Zahlungsverfahren nicht verwendet werden brauchten.

Zahlungsmittel tragen, um ihre Funktionen wahrnehmen zu können, Information über den repräsentierten Wert und gegebenenfalls über Eigentumsrechte. Diese Information läßt sich digital speichern, übertragen und verarbeiten. Ein **digitales Zahlungssystem (ZS)** kann also als ein informationstechnisches System, angesehen werden, mit dessen Hilfe Zahlungsmittel zwischen Teilnehmern transferiert werden können.

Da das Zahlungssystem mit ökonomischen Werten operiert, muß das Systemverhalten besonders gegen Betrug abgesichert werden. So ein Betrug kann darin bestehen, Teilnehmern bewußt Schaden zuzufügen; meist mit dem Ziel, sich auf Kosten anderer Teilnehmer zu bereichern. Ein digitales Zahlungssystem kann dann als betrugssicher gelten, wenn es niemandem möglich ist, das Systemverhalten dahingehend negativ zu beeinflussen. Ausführlicher heißt das, daß nachdem das System initialisiert wurde, die Kriterien der folgenden Tabelle erfüllt sein müssen:

B1a (Transferierbarkeit)	Zahlungsmittel sind für Transfer (Zahlung) verwendbar
B1b (Konvertierbarkeit)	Zahlungsmittel sind zur Umwandlung durch Banken verwendbar (Gutschrift)
B2 (Wertaufbewahrung)	Quantitative Verringerung des Zahlungsmittelbestandes eines Teilnehmers erfolgt nur mit seinem Einverständnis
B3 (Transaktionalität)	Empfänger erhält bei einer Übertragung von Zahlungsmitteln genau soviel, wie sein Partner bei der Transaktion abgibt
B4 (Beweisbarkeit)	Jede vollzogene Transaktion ist gegenüber einem Dritten nachweisbar (Quittung)
B5 (Nichtvermehrbarkeit)	Der Bestand an Zahlungsmitteln im System kann auch bei Zusammenarbeit mit anderen Teilnehmern nicht vermehrt werden (klassische Fälschungssicherheit)

Tab. 2-1: Kriterien für die Sicherheit von Zahlungssystemen

2.1.2 Identifizierte Rollen

Rollen und Transaktionen

Für das hier zugrundegelegte allgemeine Modell für digitale Zahlungssysteme in offenen Kommunikationsnetzen vgl. [ChPe_93a], [JaWa_95], [BGHH_95] und [BCMM_95]. Dieses Modell beschreibt den Zusammenhang zwischen den Beteiligten anhand eines Transfers von Zahlungsmitteln.

Neben dem Anbieter des Zahlungssystems (Zahlungssystembetreiber) und dem Anbieter des offenen Kommunikationsnetzes (Netzbetreiber) nehmen weitere Wirtschaftssubjekte in verschiedenen **Rollen** am System teil, um bestimmte Transaktionen (s.u.) auszuführen. Dabei lassen sie sich in die zwei Klassen *Banken* und *Nichtbanken* aufteilen. Rollen der Banken sind *auszahlende Bank* und *einnehmende Bank*. Banken sind miteinander über ein geschlossenes Kommunikationsnetz verbunden. Rollen, die Nichtbanken übernehmen können, sind *Kunde* (Zahlender bzw. Zahlungspflichtiger) und *Händler* (Zahlungsempfänger bzw. Zahlungsberechtigter); sie agieren im offenen Kommunikationsnetz. Innerhalb ihrer Klasse sollten die Teilnehmer ihre Rollen wechseln können, d.h. zu verschiedenen Zeitpunkten verschiedene Rollen einnehmen können. Kunden und Händler gehen mit ihren Banken statische Beziehungen ein, während sie in der Regel mit ihren Geschäftspartnern dynamische Beziehungen aufnehmen. Zwischen zwei Teilnehmern in verschiedenen Rollen können **Transaktionen** stattfinden: Abheben, Transfer, Gutschrift und Clearing. Diese Transaktionen sind durch den übertragenen Betrag, den Zeitpunkt und durch die Transaktionspartner näher bestimmt.

Weitere Transaktionen sind die Initialisierung bzw. Kontoeröffnung und Gerichtstransaktionen. Die Initialisierung des Systems durch den Zahlungssystembetreiber entspricht dabei der Emission von Bargeld durch die Zentralbank. Die Kontoeröffnung ist eine Teilnahmeerklärung von Wirtschaftssubjekten an speziellen digitalen Zahlungssystemen mit Konten.

Die Abbildung zeigt das generische Zahlungssystemmodell mit den Parteien Kunde und Händler sowie Bank des Kunden und Bank des Händlers. Zwischen den Teilnehmern in den Rollen *Kunde* und *Händler* und in der Folge auch zwischen ihren Banken bilden sich dynamische Beziehungen aus (und führen zu Transaktionen *Transfer* bzw. *Clearing*), gekennzeichnet durch unterbrochene Linien. Statische Beziehungen sind durch durchgezogene Linien gekennzeichnet (Transaktionen *Abheben* und *Gutschrift*).

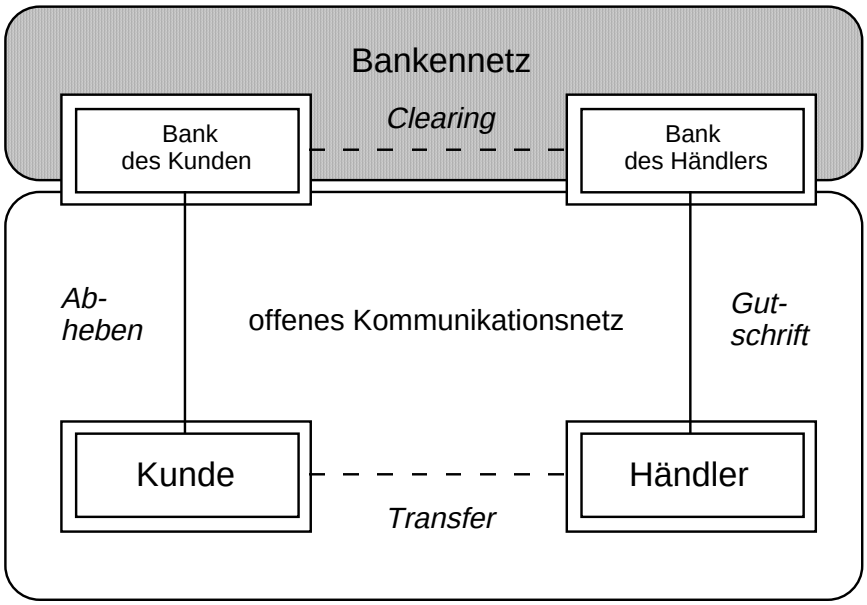


Abb.2-1: Generisches Zahlungssystemmodell

Durch die Transaktion **Abheben** erhält ein Kunde von seiner Bank digitale Zahlungsmittel im Austausch gegen andere Zahlungsmittel wie Giralgeld.

Verschiedene Identifizierungen sind notwendig, um das Abheben wechselseitig autorisieren zu können. Das wird bei Betrachtung des Abhebens (wie auch der Gutschrift) als eine Transaktion über die Schnittstelle zwischen zwei Zahlungssystemen deutlich. Die Bankenseite nimmt die Konvertierung der Zahlungsmittel vor.

1. Identifizierung des Kunden gegenüber der Bank:

   Der Kunde muß sich für den Zugriff auf sein Konto als berechtigt zu erkennen geben, um der Bank zu ermöglichen, für auszugegebende Zahlungsmittel ein Äquivalent zu erhalten. Wenn das nachgewiesen ist, autorisiert die Bank die Transaktion Abheben.

2. Identifizierung der Bank gegenüber dem Kunden:

   Die Bank muß sich gegenüber dem Kunden als berechtigt zu erkennen geben, Äquivalente für auszugebene Zahlungsmittel zu fordern. Wenn das nachgewiesen ist, autorisiert der Kunde die Transaktion Abheben.

Die Transaktion *Abheben* sollte erst beendet sein, wenn beide Autorisierungen positiv ausfallen. Das ist bei herkömmlichen Transaktionen auf einfache Weise gewährleistet. Wenn ein Kunde sich am Bankschalter einen Betrag aus seinem Girokonto bar auszahlen läßt, quittiert er der Bank den Erhalt des Geldes. Die Bank ist sich über die Identität des Kontoinhabers sicher, da sie die Unterschrift des Kunden mit einer bei Kontoeröffnung hinterlegten vergleichen kann oder dieser sich mit einem Personaldokument ausgewiesen hat, und sie erhält ein Beweisstück vom Kunden, daß er das Geld richtig empfangen hat. Der Kunde erkennt seine Hausbank natürlich und weiß über seinen Kontostand bescheid. Seine Kontonummer

kennt er noch von der Kontoeröffnung und trägt sie ins Auftragsformular ein. Er zweifelt nicht daran, daß der Bankangestellte seinen Auftrag bearbeitet.

Durch den **Transfer** findet die Übergabe digitaler Zahlungsmittel vom Kunden zum Händler statt. Dabei autorisiert der Kunde die Übergabe seiner Zahlungsmittel an den Händler gegenüber diesem und/oder gegenüber seiner Bank.

Das Modell ist insofern generisch, als sich aus ihm ein Modell für ein konkretes Zahlungssystem gewinnen läßt, beispielsweise durch Festlegung des Teilnehmerkreises für die einzelnen Parteien. So läßt sich beispielsweise ein **geschlossenes Zahlungssystem** darstellen für den Fall, daß die Rolle der Bank nur ein einziger Teilnehmer einnehmen kann (z.B. als zentraler Bankserver). Ein weiterer einschränkender Fall eines geschlossenen Zahlungssystems liegt vor, wenn der Betreiber des Systems (Bank) und der Händler identisch sind, wie z.B. bei Telefonwertkarten-Systemen, vgl. [WiMö_96].

Das Modell sieht die Möglichkeit eines Wechsels der Rollen Kunde und Händler für Teilnehmer, die Zahlungsmittel transferieren, vor. Soll dieser Wechsel in offline-Systemen möglich sein, so wird ein Zahlungsmittel benötigt, welches nach erfolgter Zahlung nicht nur Konvertierbarkeit (B1b der Betrugssicherheitsdefinition für Zahlungssysteme) gewährleistet, sondern sich im Sinne der Transferierbarkeit (B1a) für weitere Zahlungen verwenden läßt. Zur Beschreibung dieser Eigenschaft dient der Begriff **Transferabilität**. Er gibt an, wie oft ein und dasselbe Zahlungsmittel durch Zahlung weitergegeben werden kann, bevor es von einer einnehmenden Bank konvertiert wird. Dagegen meint Transferierbarkeit nur die Tatsache, daß ein Zahlungsmittel aus Sicht des Kunden während des Zahlungsvorgangs auf den Händler übergehen kann. Es lassen sich höchstens einmal transferierbare oder mehrmals transferierbare Zahlungsmittel unterscheiden. Einen hohen Grad an Transferabilität weist beispielsweise Bargeld auf. Die meisten digitalen Systeme hingegen sind auf Einmaltransferierbarkeit beschränkt. Beispiele dafür sind die GeldKarte des Zentralen Kreditausschusses (ZKA) oder Ecash von DigiCash.

Transferabilität in Zahlungssystemen im Sinne der Verwendung mehrmals transferierbarer Zahlungsmittel ist nur bei offline-Systemen interessant (vgl. [ChPe_93a]), da andernfalls digitale Zahlungsmittel schon nach dem ersten Transfer im Zuge der Gutschrift durch die Bank in Giralgeld konvertiert werden und sich für den Händler anschließend die Möglichkeit ergibt, seine Rolle zu wechseln und als Kunde wieder digitale Zahlungsmittel abzuheben. So gesehen wäre mit einem zwischengeschalteten Wechsel des Zahlungssystems über die Kombination der Transaktionen *Gutschrift* und *Abheben* jedes Zahlungssystem eines mit Transferabilität über einmalige Verwendung hinaus.

Die Anzahl der mit ein und demselben Zahlungsmittel möglichen Transfers kann jedoch auch durch die Gültigkeitsdauer der Zahlungsmittel beschränkt sein. So sind herkömmliche Wechsel üblicherweise nach drei Monaten einzulösen. Zeitlich eingeschränkte Gültigkeit bei digitalen Systemen ist beispielsweise von DigiCash in Ecash implementiert worden.

Über die **Gutschrift** kann der Händler digitale Zahlungsmittel von seiner Bank in andere Zahlungsmittel umwandeln lassen.

Das **Clearing** zwischen den Banken der Geschäftspartner dient der Aufrechnung von Forderungen mit Übertragung verbleibender Salden an Giralgeld.

2.1.3 Interessen und Sicherheitsanforderungen

Sachziele der Teilnehmer

In diesem Kapitel werden, ausgehend von den Definitionen in Kap. 1.3, für die einzelnen Rollen der Teilnehmer nach dem generischen Modell Sachziele formuliert, die mit der Nutzung des Zahlungssystems verbunden sind. Danach folgt die Darstellung des für Betrugssicherheit und Anonymität eines Zahlungssystems wesentlichen Vertrauensmodells der Teilnehmer in ihren Rollen.

Je nach der Rolle, die die im digitalen Zahlungssystem teilnehmenden Wirtschaftssubjekte einnehmen, verfolgen sie mit der Nutzung des Zahlungsmittels bzw. Zahlungsverfahrens Ziele, die sich voneinander unterscheiden können.

Dabei sei die Rolle des *Betrügers*, der unter dem Deckmantel einer der im generischen Modell aufgezeigten Rollen auftritt, hier nicht explizit betrachtet. Seine Ziele in Bezug auf andere Teilnehmer sollten jedoch bei den anderen Rollen in der Form von entgegengerichteten Schutzzielen Berücksichtigung finden.

Je nachdem, welches konkrete digitale Zahlungssystem Verwendung findet, können mehrere Rollen von ein- und demselben Teilnehmer übernommen werden. Dann fallen auch die entsprechenden Ziele zusammen. Zum Beispiel kann eine digitales Geld auszahlende Geschäftsbank gleichzeitig auch der Betreiber des digitalen Zahlungssystems sein. Weiterhin können Teilnehmer auch unabhängig von der Struktur des gegebenen Zahlungssystems nacheinander verschiedene Rollen ausüben, so z.B. zunächst als Kunde, dann als Händler oder als auszahlende und einnehmende Bank. In jeder Rolle sind die Ziele wiederum andere.

Da es neben Interessen, die sich decken oder aber nicht gegenseitig stören auch solche gibt, die einander widersprechen, ist durch eine Verhandlungsphase zu klären, inwieweit Ziele verfolgt werden können (Behandlung und ggf. Auflösung von *Interrollenkonflikten*). Durch die Übernahmemöglichkeit mehrerer Rollen durch einen Teilnehmer können jedoch auch *Intrarollenkonflikte* entstehen, die bei Nichtauflösbarkeit die Ausübung gewisser Rollen unmöglich machen.

Unterschieden werden die Sachziele nach dem Zweck der Nutzung und der interessierenden Art der Sicherheit des Zahlungssystems. Aus Wirtschaftlichkeitserwägungen heraus sind alle Teilnehmer an einem Zahlungssystem interessiert, daß ihre Ziele auch effizient verwirklicht.

Ziele in der Rolle *auszahlende Bank* (Bank des Kunden)

- Nutzung des Systems: Die digitale Zahlungsmittel auszahlende Bank will das System zum gewünschten Zeitpunkt nutzen, um Zahlungsmittel in Umlauf zu bringen. Daraus resultiert die Forderung nach Verfügbarkeit an die Betreiber des Zahlungssystems und des Kommunikationsnetzes.
- Schutz vor Betrug: Die auszahlende Bank ist bei der Nutzung primär an B4 (Beweisbarkeit) interessiert, weil ihr sonst in jedem Fall Schaden durch ungerechtfertigte Forderungen bei der Ausgabe digitaler Zahlungsmittel entstehen kann. An B5 (Nichtvermehrbarkeit) ist die Bank in ihrer Rolle als auszahlende Bank höchstens sekundär interessiert, soweit sie nämlich Rücksicht auf andere Rollen nehmen muß, die sie eventuell auch noch einnimmt, wie die der einnehmenden Bank und die des Zahlungssystembetreibers.

  Sie hat primäres Interesse daran, daß die Herausgabe digitaler Zahlungsmittel stets unter ihrem Einfluß geschieht, also B2 (Wertaufbewahrung), weil ihr sonst Äquivalente z.B. an Gi-

ralgeld bei prepaid-Systemen verloren gehen. (Unter dem Blickwinkel der Nutzung digitaler Zahlungsmittel für Transfers ist sie jedoch nicht an B2 interessiert, da sie in ihrer Rolle diese Zahlungsmittel nicht zur Zahlung einsetzen kann, sondern nur zum Ausgeben an Kunden.)

Ziele in der Rolle *einnehmende Bank* (Bank des Händlers)

- Nutzung des Systems: Die Bank, der digitale Zahlungsmittel vorgelegt werden, will zum gewünschten Zeitpunkt im System tätig werden, um das Clearing durchführen zu können und Zahlungsmittel gutzuschreiben (d.h., Verfügbarkeit wird gefordert).
- Schutz vor Betrug: Die Bank ist, wenn sie digitale Zahlungsmittel zur Gutschrift entgegennimmt, primär wieder an B4 (Beweisbarkeit) interessiert. Sekundärziel im Zusammenhang mit der Beweisbarkeit ist B3 (Transaktionalität). Ist Clearing erforderlich, um den Kreislauf zu schließen, besteht für die einnehmende Bank primäres Interesse an B2 (Wertaufbewahrung).

  Da kopierte und bei anderen Banken gleichzeitig eingelöste Zahlungsmittel nur einer der einnehmenden Banken beim Clearing verrechnet werden können, verfolgt sie in Abhängigkeit von ihren Rollen sekundär auch das Ziel B5 (Nichtvermehrbarkeit).

Ziele in der Rolle *Kunde* (*Zahlender* bzw. *Zahlungspflichtiger*)

- Nutzung des Systems: Um zur Begleichung einer Geldschuld einen Transfer vornehmen zu können, ist für ihn die Verfügbarkeit zum gewünschten Zeitpunkt von Bedeutung. Ohne Betrugsabsicht erlittene Verluste durch technischen Ausfall oder Verlust (beispielsweise durch Diebstahl der Geldbörse) sollten vom System ausgeglichen werden können. Wichtig ist hier neben der Verfügbarkeit also auch Verlusttoleranz.
- Schutz vor Betrug: Der Zahlende ist vor allem an B1a (Transferierbarkeit), B1b (Konvertierbarkeit), B2 (Wertaufbewahrung) und B4 (Beweisbarkeit) interessiert, nicht jedoch an B5 (Nichtvermehrbarkeit). Der Kunde möchte sicher sein, Zahlungsmittel in Besitz zu haben, welche er in voller Höhe gemäß seiner Rolle zur Bezahlung von Gütern verwenden kann. Er möchte sowohl die Abbuchung wie auch den Transfer gegenüber Dritten beweisen können, um falschen Anschuldigungen begegnen zu können. Sekundärziel im Zusammenhang mit der Beweisbarkeit ist wieder B3 (Transaktionalität).
- Anonymität und Unbeobachtbarkeit: Soweit nicht durch das Zahlungsverfahren ökonomisch anders bedingt, soll das Zahlungssystem von sich aus Anonymität gewährleisten, und zwar die Anonymität des Transfers (Kunde-Händler-Beziehung) gegenüber der ausgebenden Bank (und den anderen Banken), wie sie vom Bargeld bekannt ist, sowie, falls gewünscht, die Anonymität gegenüber dem Händler. Die Transaktionen sollen auch über einen längeren Zeitraum hinweg von Dritten und gegebenenfalls auch vom Händler nicht miteinander in Beziehung zu setzen sein.

Ziele in der Rolle *Händler* (*Zahlungsempfänger* bzw. *Zahlungsberechtigter*)

- Nutzung des Systems: Ist wiederum zum gewünschten Zeitpunkt wichtig, um Zahlungsmittel empfangen zu können bzw. gutschreiben zu lassen.
- Schutz vor Betrug: Für den Händler sind B1b (Konvertierbarkeit), B2 (Wertaufbewahrung) und B4 (Beweisbarkeit) primäre Ziele. Der Händler möchte sicher sein, daß Kunden mit einem Zahlungsmittel bezahlen, welches er zur Einlösung in der entsprechenden Höhe bei seiner Bank verwenden kann. Er möchte die Einreichung zur Gutschrift gegenüber Dritten beweisen können. B3 (Transaktionalität) ist Sekundärziel.

- Anonymität und Unbeobachtbarkeit: Das Zahlungssystem soll von sich aus Anonymität gewährleisten, und zwar die Anonymität des Transfers (Kunde-Händler-Beziehung) wie bei Bargeld gegenüber der gutschreibenden Bank (und den anderen Banken) sowie die Anonymität gegenüber dem Kunden, falls er seine Dienstleistung anonym anbietet. Die Transaktionen sollen ebenfalls über einen längeren Zeitraum hinweg von Dritten nicht miteinander in Beziehung zu setzen sein.

Ziele in der Rolle *Zahlungssystembetreiber*

Der Zahlungssystembetreiber ist an der Aufrechterhaltung der vollen Funktionsfähigkeit seines Zahlungssystems interessiert und er möchte, daß die von ihm ausgegebenen Zahlungsmittel die zugesicherten Eigenschaften behalten, bis sie ihm wieder vorgelegt werden. Das bedeutet:

- Das digitale Zahlungssystem für alle Teilnehmer, die es wünschen, verfügbar halten, d.h. insbesondere gültige Zahlungsmittel einzulösen bzw. deren Gültigkeit zu prüfen, ist Sachziel.
- Schutz vor Betrug: Gegenüber den Empfängern ausgegebener Zahlungsmittel will der Zahlungssystembetreiber nachweisen können, wieviel Zahlungsmittel er in Umlauf gebracht hat, d.h. er verfolgt B4 (Beweisbarkeit) als ein Primärziel. Um nicht durch ungerechtfertigte Forderungen geschädigt zu werden, akzeptiert er nur von ihm emittierte Zahlungsmittel, d.h. daß als Primärziel natürlich B5 (Nichtvermehrbarkeit) verlangt wird. Wenn es mehrere Stellen mit Zahlungsmittelemissionsfähigkeit gibt, denen Kopien eingereicht werden könnten, ist Nichtvermehrbarkeit für alle gleichermaßen wichtiges Primärziel. Alle übrigen Ziele in Bezug auf Betrugssicherheit verfolgt der Betreiber sekundär, d.h. im Sinne der Bereitstellung eines sicheren Zahlungssystems.

Ziele in der Rolle *Kommunikationsnetzbetreiber*

- Sein Ziel ist, das Netz für alle Teilnehmer, die es wünschen, bereitzustellen und verfügbar zu halten. An Betrugssicherheit der über das Kommunikationsnetz abgewickelten Zahlungssystemtransaktionen ist er nicht interessiert. (Das gilt nur solange, wie er nicht zusätzlich noch sicherheitsbezogene Mehrwertdienste im Rahmen eines sog. Value Added Network - VAN - anbietet.)

Folgende Übersicht faßt die Ziele der Teilnehmer in den einzelnen Rollen in Bezug auf die Betrugssicherheit zusammen und gibt an, welche Bedeutung ihnen zukommt:

Schutz vor Betrug *** primäres Interesse + sekundäres Interesse	auszahlende Bank	einnehmende Bank	Kunde	Händler	Zahlungssystembetreiber
B1a/b (Transf./Konvert.)			***	***	+
B2 (Wertaufbewahrung)	***	***	***	***	+
B3 (Transaktionalität)		+	+	+	+
B4 (Beweisbarkeit)	***	***	***	***	***
B5 (Nichtvermehrbarkeit)	+	+			***

Tab.2-2: Sachziele in den Rollen bezüglich Betrugssicherheit

Damit sind die Rahmenbedingungen für die Gestaltung eines betrugssicheren Zahlungssystems gegeben.

Nun ist die Frage zu klären, warum außer der Forderung nach Betrugssicherheit auch die Forderung nach Anonymität und Unbeobachtbarkeit gestellt wird. Die Frage nach der Notwendigkeit der Betrugssicherheit läßt sich noch unmittelbar beantworten, wenn man den Gegenstand des Zahlungsverkehrs vor Augen hat. Ein Zahlungssystem stellt ein lohnendes Ziel für Betrüger dar, die sich bereichern wollen. Die zweite Forderung ergibt sich aus der Berücksichtigung der Notwendigkeit des Schutzes personenbezogener Daten: Zahlungssysteme werden von einer Vielzahl von Personen und Unternehmen für die Abwicklung von Geschäften eingesetzt, und außerdem von jedem Teilnehmer öfter beansprucht. Das wird auch mit etablierten digitalen Systemen der Fall sein. Dabei entstehen neben den unmittelbaren Transaktionsdaten auch Kontextinformationen. Die Auswertung beider ergibt über einen längeren Beobachtungszeitraum hinweg Profile der Teilnehmer, insbesondere durch Verkettung der Daten verschiedener Transfers, wie des Zahlungsbetrags und solcher Kontextinformationen (evtl. auch als Transaktionsdaten vorliegend) wie Händler und Zeitpunkt. Diese (personenbezogenen) Daten können, wenn nichts zur Wahrung der Anonymität und der Unbeobachtbarkeit getan wird, selbst nicht am Zahlungssystem aktiv teilnehmenden Parteien bekannt werden (durch Beobachtung der Inhaltsdaten und der Verkehrsdaten der Kommunikation) und sind für die Verfolgung unterschiedlichster Ziele nutzbar, s.u. (weitere Ziele). Selbst einzelne Transaktionsdaten, die aus digitalen Zahlungssystemen ohne entsprechenden Schutz leicht gewonnen werden könnten, verletzen berechtigte Interessen der Teilnehmer, z.B. bei Transfers zwischen Unternehmen wie Groß- und Einzelhandel. Der Großhändler könnte sich beispielsweise dafür interessieren, bei welchen Konkurrenten der Einzelhändler ebenfalls kauft und zu welchen Konditionen das geschieht usw. Die anonymitätsbezogenen Ziele erscheinen deshalb gerechtfertigt, vgl. [PfWP_90].

Weitere Ziele

Hinzu kommen noch gewisse Sachziele, die nicht direkt die Nutzung des Zahlungssystems als solches betreffen. So sind Banken und Händler an einer Erweiterung ihres Kundenkreises interessiert, um höhere Umsätze zu erzielen. Zu diesem Zweck benötigen sie Informationen über das Verhalten ihrer Kunden, die sie möglicherweise auch durch das digitale Zahlungssystem zu erhalten hoffen. Personenbezogene Transaktionsdaten, die gespeichert werden, um z.B. eine monatliche Abrechnung vornehmen zu können, lassen sich ebensogut für die Erstellung von Kundenprofilen auswerten. Diese Ziele können in Konflikt mit denen der Kunden geraten, zumal sie auch die Ziele von nicht am System teilnehmenden Instanzen sein können, denen an viel Information über die Nutzer gelegen ist.

Zentral anfallende Buchungsdaten erlauben komplette Persönlichkeitsanalysen. Deren Mißbrauch als Entscheidungsgrundlage für Versicherungen, Kreditvergabe oder Personaleinstellung kann nicht ausgeschlossen werden. Für prepaid-Systeme sollte deshalb z.B. bei Clearingverfahren keine individuelle Kartennummer benutzt werden, noch ein anderer Bezug zum Karteninhaber hergestellt werden können, vgl. [Weic_96]. Ebenso ist bei ordentlicher Kredit- oder Debitkartenverwendung keine Veröffentlichung der Identität des Kunden gegenüber dem Händler notwendig.

Beim Einsatz von mit dem Girokonto verknüpftem Bargeldersatz könnten nichtkreditwürdige Personen oder solche ohne Bankverbindung benachteiligt sein, da auch sie auf alltägliches Zahlungsmittel angewiesen sind, eine negative SCHUFA-Eintragung jedoch oft die Eröffnung eines Girokontos verhindert; vgl. [Baue_96].

2.1.4 Beispiele für digitale Zahlungssysteme

Ecash (DigiCash)

Ecash von DigiCash ist ein online-Zahlungssystem, welches digitale Münzen benutzt, die von der Bank signiert werden, und zwar blind, d.h. sie gewähren Nichtzurückverfolgbarkeit der vom Kunden benutzten Zahlungsmittel. Um Ecash zu erhalten, muß der Kunde zunächst einen entsprechenden Betrag von seinem Girokonto abbuchen lassen, es ist also ein *prepaid*-System.

In der für das Internet vorgesehenen Implementierung benutzen sowohl Händler als auch Kunden gleiche Software. Das Abheben digitalen Geldes geschieht gegen Abbuchung vom Girokonto bzw. gegen Einlösung bereits transferierter Münzen beim Zahlungsserver der Bank. Sobald digitale Münzen vom Bankkonto abgehoben wurden, trägt der Kunde das Risiko eines eventuellen Verlustes.

Der Kunde kann dann mit dem gewünschten Händler in Kontakt treten (über die Nutzung eines WWW-Browsers beispielsweise) und ein Geschäft abschließen. Nun sendet der Server des Händlers eine Zahlungsaufforderung an die Client-Software beim Kunden, die daraufhin zur Genehmigung der Zahlung durch den Kunden auffordert. Ist das geschehen, so wird eine dem Betrag entsprechende Anzahl digitaler Münzen zum Server des Händlers übertragen. Dieser baut eine online-Verbindung zum Zahlungsserver der Bank auf, der die Signatur testet und die Notennummer auf bereits erfolgte Einlösung prüft (double spending detection). Ist die Prüfung erfolgreich abgeschlossen, wird dem Händler der entsprechende Betrag gutgeschrieben und eine Bestätigung an den Server des Händlers versandt.

Besonders hervorzuheben ist die Berücksichtigung der Interessen vom Betreiber und Kunden des Systems, die das Konzept der blinden Signatur erlaubt.

Mondex

Entwickelt wurde Mondex in Großbritannien von der National Westminster Bank, der Midland Bank und von British Telecom. Dieses offline-System beruht auf manipulationssicherer Hardware, die den Kunden als sog. Elektronische Geldbörse mit Chipkarte ausgehändigt wird. Sie kann sowohl mit anderen Mondex-Geldbörsen als auch mit den Terminals der Mondex-Akzeptanzstellen (Händler) kommunizieren.

Mondex ist ein prepaid-System. Jede Karte gehört zu einem Girokonto. Um Geld vom Girokonto abzuheben und auf die Chipkarte zu laden, benötigt der Kunde ein Telefongerät mit Kartenterminal. Nach Kontaktierung der Bank und Autorisierung des Kunden durch Eingabe der PIN können bis zu 500 Pfund (etwa 1250 DM) aufgeladen werden (vgl. [Krön_95]). Ein Transfer von digitalem Geld zwischen Kunde und Händler erfolgt offline entweder von Chipkarte zu Chipkarte über ein taschenrechnerähnliches Gerät mit Kartenschlitz (das sog. Electronic Wallet) oder von Chipkarte zu Händlerkasse mit Mondexterminal. Es erfolgt keinerlei online-Autorisierung der Zahlung durch die Bank. Mondex ist ein System mit offline-Transferabilität und kommt damit den Bargeldeigenschaften sehr nahe. Der Händler kann sich empfangenes Zahlungsmittel telefonisch auf sein Girokonto gutschreiben lassen.

Den aktuell zur Verfügung stehenden Betrag an Mondex-Geld kann man mit einem leicht handhabbaren Miniatur-Kartenleser, der am Schlüsselbund tragbar ist, ermitteln. Das Electronic Wallet erlaubt die Eingabe eines PIN-Codes durch den Nutzer zur Sperrung der Chipkarte, was gegen unbefugte Verwendung des geladenen Geldbetrags durch Dritte schützt. Der Kunde muß in dieser Hinsicht jedoch dem Betreiber vertrauen, da dieser sämtliche Geräte bei online-Kommunikation unter Kontrolle hat. Unter dieser Annahme kann bei Verlust der Chipkarte

also zwar kein Dritter etwas mit dem digitalen Geld anfangen, dem Kunden kann es jedoch auch nicht erstattet werden, denn der aktuelle Geldbetrag ist einzig auf der Chipkarte in einem sicheren Zähler gespeichert (was zumindest während der offline-Transfers von Wallet zu Wallet auch der Fall ist). Damit wären Kunden bei ihren Transfers vor der Bank anonym und der Weg des Geldes ist, ausgehend von der Einlösung, auch nicht zum Kunden zurückverfolgbar. Diese Angabe läßt sich zur Zeit nicht nachprüfen, da nicht bekannt ist, welche Daten auf der Karte gespeichert und vom Händlerterminal zur Bank übermittelt werden.

Es sind fünf verschiedene Währungen speicherbar. Von den Kunden werden für die Nutzung der Mondex-Geldbörse Gebühren erhoben, von den Akzeptanzstellen nicht, vgl. [BaFo_95]. Geplant ist die Ausdehnung von Mondex als Zahlungsmittel in Kommunikationsnetzen bei sog. Teleshopping und Video on Demand sowie für die Bezahlung des Empfangs digitalisierter Fernsehprogramme über Telefonkabel. Mondex erscheint insgesamt als ein flexibles und praktisches Bargeldsubstitut. Allerdings weist es Mängel bezüglich erreichbarer Sicherheit für die Anwender des Systems auf. So ist nichts über die verwendeten kryptographischen Protokolle bekannt (vgl. [JaWa_95]).

2.2 Anwendungsbeispiel: Workflow Management

2.2.1 Abgrenzung und Einordnung der Begriffe

Computer Supported Cooperative Work - CSCW

Als wesentlicher Oberbegriff für das gesamte Gebiet der wissenschaftlichen Forschung, das sich mit der rechnergestützten Gruppenarbeit beschäftigt, gilt **Computer Supported Cooperative Work - CSCW**. Dieses Forschungsgebiet, welches nicht nur Probleme aus der Informatik sondern auch aus Wirtschaftsinformatik, Psychologie und Soziologie beinhaltet, erlangt immer mehr Bedeutung durch die verschärften Wettbewerbsbedingungen zwischen den Unternehmen. Sie fordern Systeme, die flexible Formen der Zusammenarbeit in Organisationen wirkungsvoll unterstützen. Dabei soll die Zusammenarbeit der Menschen durch den Einsatz von Rechentechnik effizienter, flexibler, humaner und sozialer gestaltet werden (vgl. [Hase_94], S. 15ff.).

Ein wesentlicher Aspekt dieser Betrachtungen ist, daß die Mitglieder der Gruppen bzw. Unternehmen nicht nur organisationsintern, sondern auch organisations- und landesübergreifend miteinander kooperieren, d.h. die Abläufe sind räumlich und zeitlich verteilt. Daraus ergeben sich Forderungen an CSCW-Systeme: Unterstützung geographisch verteilter Arbeitsgruppen sowie die zusätzliche Berücksichtigung heterogener Arbeitsumgebungen und verschiedener Organisationsmodelle der Kooperationspartner.

Weiterhin sind eine Reihe formaler Anforderungen zu erfüllen. Dazu zählen:

- die Effizienz, bei der es um vereinfachte, weniger personal- und zeitaufwendige Koordinationstätigkeiten, reduzierte Durchlaufzeiten, beschleunigte Entscheidungsprozesse sowie verbesserte Entscheidungsqualität geht,
- die Flexibilität, d.h. Anpassung der organisatorischen Regelungen an sich ständig ändernde Anforderungen,
- die Transparenz, die es erlaubt, laufende Prozesse jederzeit zu kontrollieren und das System damit durchschaubar zu machen,
- Offenheit und Integration, bereits existierende CSCW-Systeme sollen mit denen, die sich noch in der Entwicklungsphase befinden , kooperieren können und
- die Ergonomie, d.h. bei der Gestaltung ist den humanen und sozialen Bedürfnissen der Organisationsmitglieder gerecht zu werden.

Wie bereits erwähnt, umfaßt Compter Supported Cooperative Work die theoretischen Grundlagen der Gruppenarbeit und deren Rechnerunterstützung. Die Begriffe Workflow Management und Groupware stehen dagegen für konkrete Ausprägungen der CSCW-Konzepte.

Workflow Management - WfM

Workflow Management befaßt sich mit der Steuerung von Vorgängen über mehrere Arbeitsplätze unter Einbeziehung technischer Basiskomponenten. Der Fokus liegt auf der Unterstützung und Kopplung der einzelnen Sachbearbeitervorgänge. Diese Vorgänge bestehen in der Regel aus mehreren Teilschritten. Workflow Management soll es ermöglichen, verschiedene Teilschritte nach einem organisatorischen Regelwerk zu koordinieren, zu überwachen und bei Bedarf zu synchronisieren.

Workflow Management Systeme - WfMS

Zur Realisierung von Workflow Management haben sich in den letzten Jahren die sogenannten Workflow Management Systeme (auch: Vorgangs-, Vorgangssteuerungs-, Bürovorgangs- oder Workflow-Systeme) herausgebildet. Jablonski zitiert in [Jabl_95] die folgende seiner Meinung nach „...unter den oftmals sehr mangelhaften Versuchen einer Begriffsdefinition ... noch treffendste Umschreibung“ für ein Workflow Management System von McCarthy und Bluestein:

> **„Workflow management software is a proactive computer system which manages the flow of work among participants, according to a defined procedure consisting of a number of tasks. It co-ordinates user and system participants, together with the appropriate data resources, which may be accessible directly by the system or off-line, to achieve defined objectives by set deadlines. The co-ordination involves passing tasks from participant to participant in correct sequence, ensuring that all fulfil their required contributions, taking default actions when necessary.“**

Solche Systeme bieten also die Möglichkeit, Vorgänge ohne professionelle Anwendungsentwicklung in einer Form zu spezifizieren, die maschineninterpretierbar ist. Auf dieser Basis wird eine aktive Steuerung arbeitsteiliger Prozesse erlaubt [Hase_94]. Die Steuerungskomponente eines Workflow Management Systems ermittelt die jeweils nächsten Bearbeiter, benachrichtigt diese und stellt ihnen die notwendigen Informationen und Werkzeuge zur Verfügung. Das System steuert aber nicht die eigentliche Ausführung der Aktionen (Teilschritte), die vom Benutzer meist unter Zuhilfenahme gebräuchlicher Werkzeuge zur Dokumentenbearbeitung ausgeführt werden.

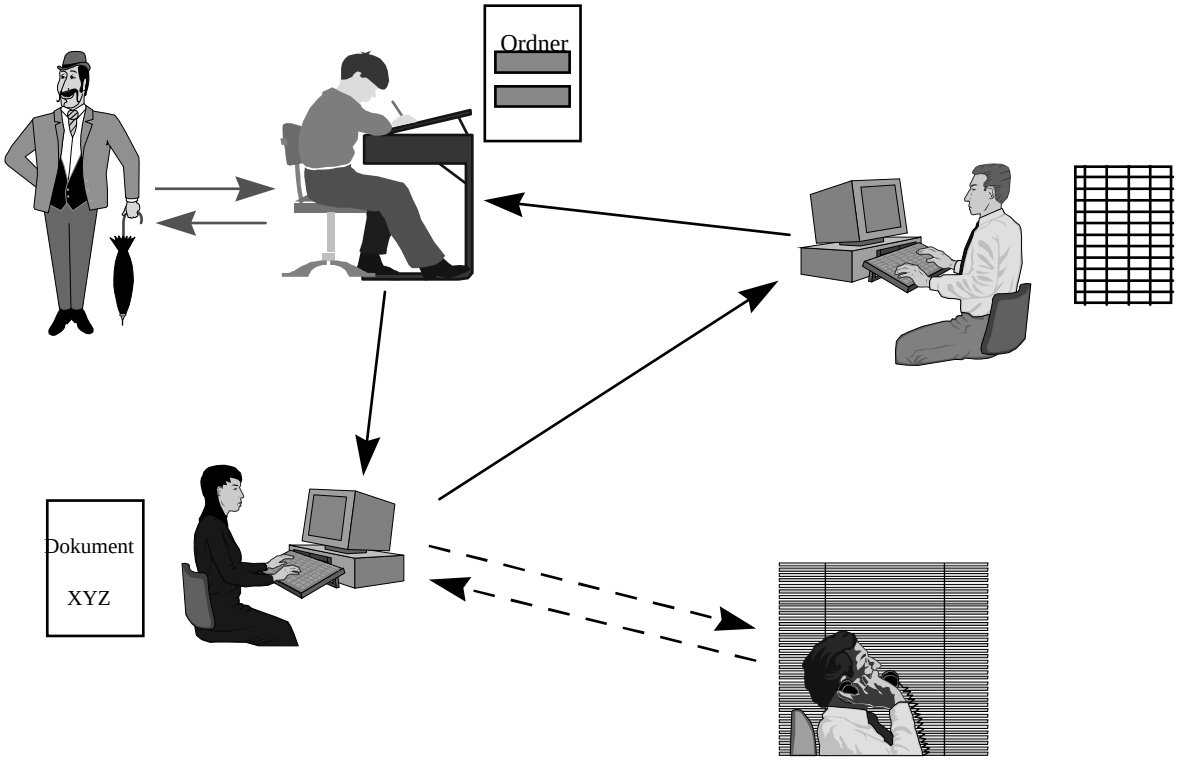


Abb. 2-2: Beispiel für einen durch ein WfMS gesteuerten Bürovorgang

Groupware - GW

Das Ziel von **Groupware** besteht darin, Gruppen bei der Kommunikation, bei der Zusammenarbeit und der Koordinierung ihrer Aktivitäten zu unterstützen. Nach [Ellis_91] kann man daher Groupware definieren als

> **„computer-based systems that support groups of people engaged in a common task (or goal) and that provide an interface to a shared environment".**

Somit unterscheidet sich Groupware schon von der Zielrichtung her klar von Workflow Management. Wird bei Groupware die Gruppe als solche unterstützt, so steuern Workflow Management Systeme das koordinierte Bearbeiten von Geschäftsprozessen durch einzelne Personen, die als Teil einer Gruppe oder Organisation eine bestimmte Aufgabe erfüllen.

Groupware-Systeme besitzen folgende Merkmale (vgl. Abb 2-2):

1. ein expliziter Gruppenbezug,
2. elektronische Kommunikationsmöglichkeiten ➔ aktenlose Kommunikation der Mitarbeiter aller Hierarchieebenen und
3. Informationsmanagement-Funktionen ➔ unternehmensweite Bereitstellung von Informationen mit komfortablen Suchfunktionen

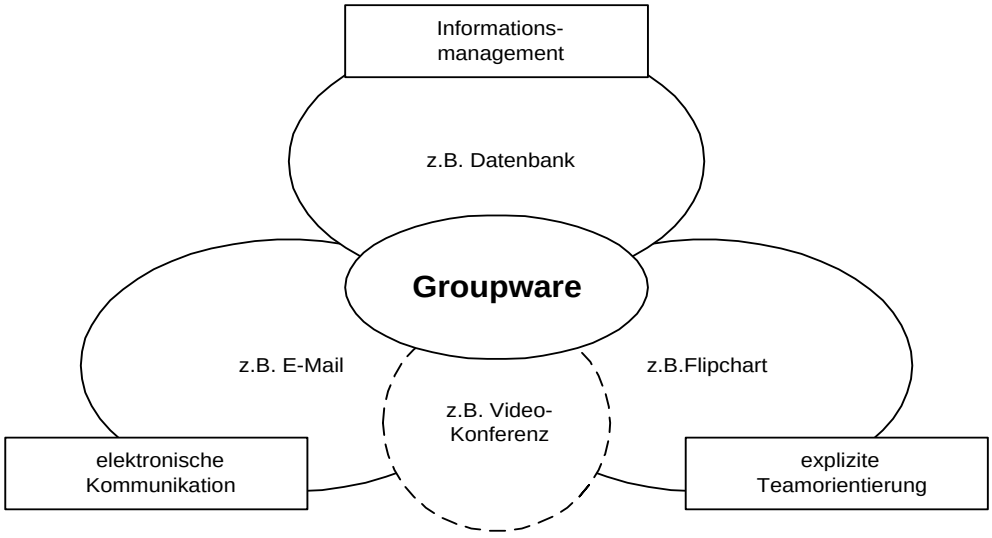


Abb. 2-3: Merkmale von Groupware-Systemen [Dier_94]

Dokumentenmanagement - DM

Dokumentenmanagementsysteme (DMS) und Workflow Management Systeme werden oft in einem Atemzug genannt. Das begründet sich darin, daß Dokumentenmanagementsysteme eine sinnvolle Ergänzung für die Verwaltung der von den Workflow Management Systemen durch die Unternehmen geleiteten Dokumente darstellt. So ist in vielen WfMS ein Dokumentenmanagementsystem oder eine Dokumentendatenbank integriert.
Dokumentenmanagementsysteme dienen der Verwaltung von Dokumenten und ihrer Archivierung. Sie unterstützen somit informationstechnisch [Zila_95]:

- das Ablegen von und Wiederzugreifen auf Dokumente,
- das Archivieren von Dokumenten

in Unternehmen oder in organisatorischen Bereichen.

Business Process Reengineering - BPR

Business Process Reengineering stellt die planerische Seite der Geschäftsprozeßgestaltung in Unternehmen in den Vordergrund. Die allgemein anerkannte Definition des Begriffes „Business Process Reengineering“ von Mike Hammer besagt:

> **„Unter Business Process Reengineering bzw. Vorgangsanalyse wird das fundamentale Überdenken und radikale Umformen von geschäftlichen Prozessen verstanden mit dem Ziel, Leistungsdaten wie Kosten, Qualität, Service und Geschwindigkeit drastisch zu verbessern.“**
>
> **[Ham_94]**

Das Business Process Reengineering wird breits seit geraumer Zeit durch Softwaresysteme verschiedenster Hersteller unterstützt.

Zusammenfassung

In der Tabelle 2-3 wird versucht, eine Einordnung und Abgrenzung der verschiedenen vorgestellten Konzepte hinsichtlich der unten erläuterten Merkmale vorzunehmen. Bei der Merkmalsfindung wurde vom Konzept des Workflow Management ausgegeangen, um die anderen Gebiete dagegen abgrenzen zu können:

- *Rechnernetze*
  Kopplung von mehreren, möglicherweise räumlich getrennten Rechenanlagen bzw. Computern, die so miteinander verbunden sind, daß sie Informationen austauschen können.
- *außerorganisatorisch*
  Das System wird nicht nur intern in einer Firma, sondern auch über Unternehmensgrenzen hinaus eingesetzt.
- *mehrere Beteiligte*
  Im Verlauf eines durch das System realisierten bzw. unterstützten Arbeitsganges müssen typischerweise mehrere Menschen direkt mit dem Softwaresystem interagieren.
- *eingebundene Anwendungen*
  Das System kooperiert direkt mit anderen Anwendungen. Dabei werden Daten zwischen der Anwendung und dem System ausgetauscht.
- *entscheidungsrelevante Daten*
  Aufgrund von Vergleichen zwischen vorgegebenen Bedingungen und während eines Arbeitsganges entstandenen (entscheidungsrelevanten) Daten entscheidet das System zur Laufzeit über weitere Arbeitsschritte.
- *Historie*
  Werden alle bzw. die wesentlichen Ereignisse bei der Arbeit mit dem System protokolliert und stehen somit für Auswertungen und Fehlerbehandlungen zur Verfügung?
- *Abbildung der Organisationsstruktur*
  Im System wird ein Abbild der real existierenden Organisationsstruktur geschaffen.

Systeme / Merkmale	CSCW	WfMS	GW-Systeme	DMS	BPR-Systeme
Rechnernetze	**x**	**x**	**x**	**x**	**-**
außerorganisatorisch	**x/-**	**x**	**-**	**-**	**-**
mehrere Beteiligte	**x**	**x**	**x**	**-**	**-**
eingebundene Anwendungen	**x/-**	**x**	**-**	**-**	**-**
entscheidungsrelevante Daten	**x/-**	**x**	**-**	**-**	**-**
Historie	**x/-**	**x**	**x/-**	**x**	**-**
Abbildung der Organisationsstruktur	**x/-**	**x**	**-**	**-**	**x**

Legende: x → wird unterstützt, - → wird nicht unterstützt, x/- → beides kann auftreten

Tab. 2-3: Einteilung von CSCW-Systemen und Abgrenzung zu DMS und BPR-Systemen

Workflow Management Coalition - WfMC

Eine Vielzahl von Herstellern bietet Workflowprodukte an, die sich stark in ihren funktionalen Fähigkeiten, der Bedienoberfläche als auch der Hard- und Softwarebasis unterscheiden. Standards bezüglich der zugrundeliegenden Methoden und der Interoperabilität von Workflow Management Systemen haben sich allerdings bisher nicht entwickeln können.
Um diese für Anwender und Hersteller unbefriedigende Situation durch die Festlegung von Standards zu verbessern, wurde im August 1993 die Workflow Management Coalition (WfMC) gegründet.

Die wesentlichen Ziele der WfMC sind:
- Spezifikationen im Gebiet der Workflowmanagementtechnologie erstellen,
- durch das Etablieren gemeinsamer Standards die Nutzung dieser Technologie intensivieren und auf eine langfristig gesicherte Basis stellen,
- das Verständnis für die Workflowtechnologie am Markt vertiefen.

Zunächst versuchte die Workflow Management Coalition, eine einheitliche *Terminologie* für den Workflowbereich zu schaffen, da bisher aufgrund des schnellen und unkontrollierten Wachstums von Konzepten und Produkten auf diesem Gebiet eine uneinheitliche und unkonsolidierte Begriffswelt vorlag. Eine erste Version des Glossars wurde 1994 veröffentlicht [WfMC_94].

Ein weiteres Tätigkeitsfeld der WfMC innerhalb der „Reference Model Workgroup“ besteht in der Erarbeitung eines *Referenzmodells für Workflow Management Systeme.* Anhand dessen können zum Beispiel existierende Workflow-Systeme unabhängig von der konkreten Realisierung auf konzeptioneller Ebene beschrieben oder verglichen werden. Dieses Referenzmodell stellt einen Rahmen für Workflow-Systeme dar, der von der Vielzahl der am Markt erhältlichen Workflowprodukte mit ihren verschiedenen Implementierungstechniken, Kommunikationsinfrastrukturen und Einsatzumgebungen abstrahiert.

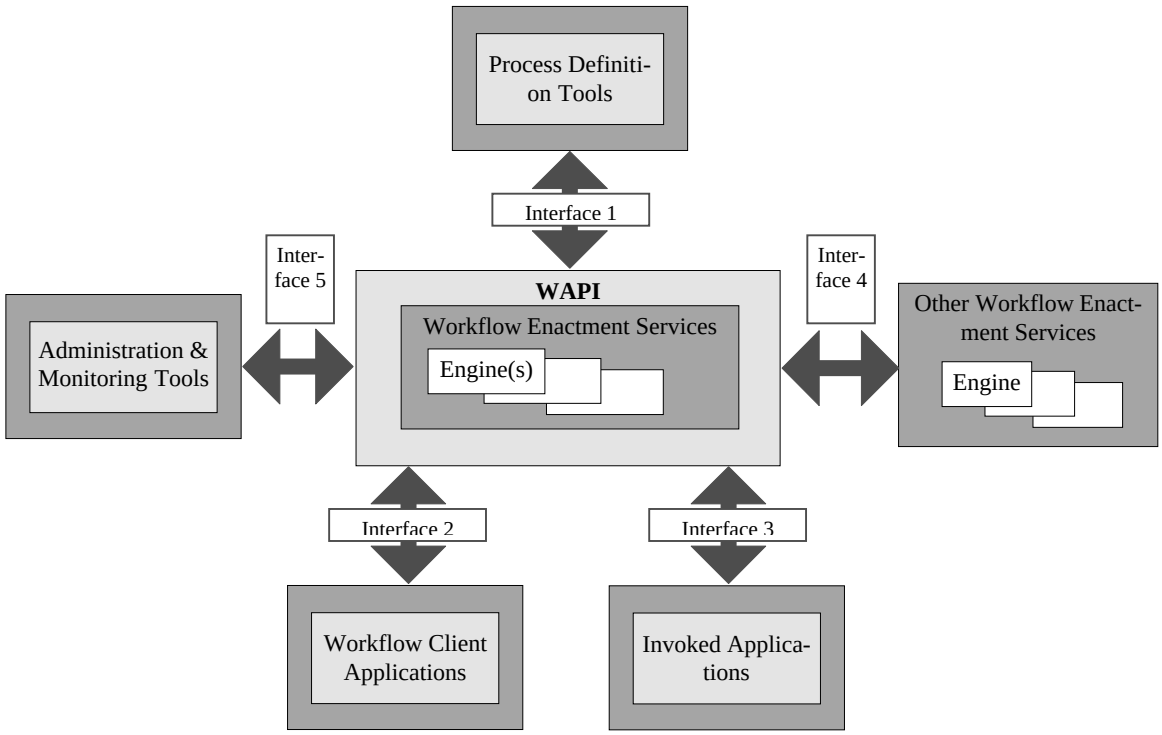


Abb. 2-4: Referenzmodell der WfMC [WfMC_95]

Die fachliche Arbeit der WfMC ist durch spezifische Arbeitsgruppen organisiert. Diese entwickelten auf der Basis des Referenzmodells bislang Standards für die fünf in der Abbildung 2-4 dargestellten Schnittstellen.
So definiert z.B. die Arbeitsgruppe des Interface 1 eine gemeinsame Prozeßdefinitionssprache für Ablaufeditoren und Analysetools als Austauschformat zu Workflow Management Systemen. Die Gruppe 2 konzentriert sich auf den standardisierten Aufruf von Funktionen der WfMS, um die Interaktion mit Bearbeitern zu realisieren. Standards, die den direkten oder über einen sogenannten Tool-Agenten vermittelten Aufruf von externen Anwendungen aus dem Workflow heraus betreffen, werden in den Definitionen zu Interface 3 zusammengefaßt. Unter den Gesichtspunkt Interoperabilität **(**Interface 4**)** fallen Standards, die die Kooperationsfähigkeit von Workflow-Systemen verschiedener Hersteller ermöglichen sollen. Die Arbeitsgruppe 5 beschäftigt sich mit der Festlegung von Monitoring- und Kontrollfunktionen eines Workflow Management Systems sowie der Definition einer diesbezüglichen Schnittstelle (Interface 5).

Es gibt noch weitere Arbeitsgruppen, die sich z.B. konforme Begriffsverwendung in den Arbeitsgruppen und die Konsistenz verwendeter Begriffe mit dem Glossar zum Ziel gesetzt haben oder die anstreben, bestehende Workflow-Produkte auf die Anwendung der definierten WfMC-Standards hin zu überprüfen und Ergebnislisten öffentlich zu machen.
Nach unserem Wissensstand beschäftigt sich die WfMC derzeit in keiner Weise mit Betrachtungen oder Standardisierungsvorschlägen zur Sicherheit von Workflow Management Systemen. Aber gerade in einer Zeit, wo sich Workflow Management Systeme z.B. durch die Entwicklung von WWW-Frontends zu offenen Systemen hin etwickeln (COSAIntraNet [Cosa_1], Action Workflow Metro [Action_1] und viele andere), nimmt die Sicherung der Workflow Management Systeme im Interesse der Anwender essentielle Bedeutung ein.

2.2.2 Identifizierte Rollen

Jedes Unternehmen hat seine besonderen Eigenheiten. Die Aufbauorganisation, die Zuständigkeiten, die Verantwortlichkeiten und die Abläufe machen in ihrer Gesamtheit die Individualität einer Firma aus.
Die in einem Büro existierenden Rollen sind jedoch im wesentlichen bei allen Unternehmen ähnlich. Durch die folgenden drei Rollentypen soll versucht werden, eine allgemeingültige Abstufung zu finden (vgl. Abbildung 2-x):

1. *geschäftsbeziehungsbezogene Rollen:* Rollen, die Menschengruppen einnehmen, wenn sie geschäftlich miteinander in Beziehung stehen. Eine solche Menschengruppe, die z.B. als Firma oder Kunde bezeichnet werden kann, hat dann bezüglich eines Zieles gleiche Interessen.

2. *Organisationseinheiten:* sind Zusammenfassungen von gleichartigen oder/und unterschiedlichen Stellen innerhalb einer Firma zu Abteilungen oder Bereichen. Beispiele sind u.a. DV-Abteilung, Beschaffung, Marketing, Produktionsabteilung.

3. *Stellen:* definieren den Arbeitsbereich einzelner Personen mit ihren Kompetenzen und Zielsetzungen. In Stellenbeschreibungen ist festgeschrieben, welche Art der Tätigkeit eine Person als Inhaber dieser Stelle auszuüben hat und welche Entscheidungsbefugnisse und Verantwortlichkeiten sie besitzt.

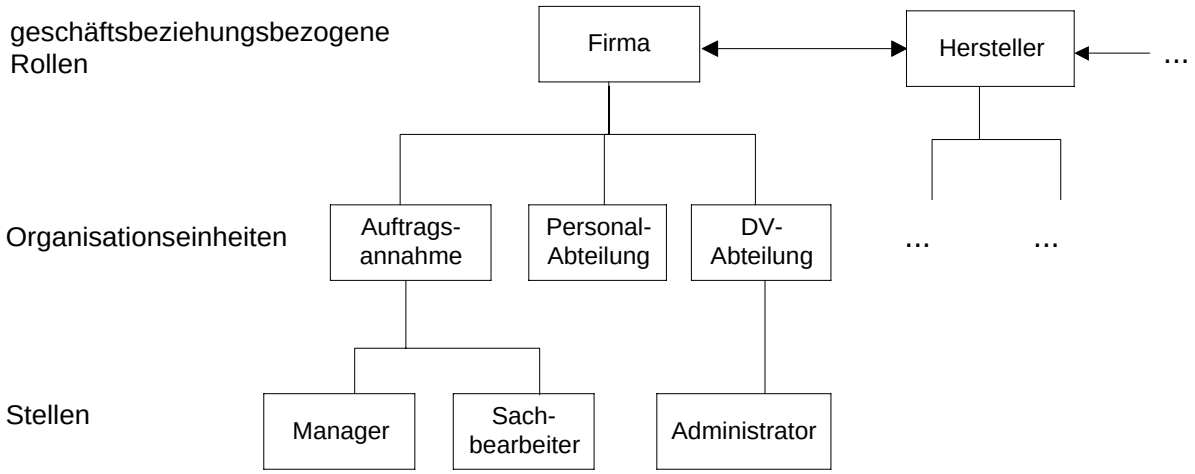


Abb. 2-5: Rollen und Rollenhierarchie in Unternehmen

Geschäftsbeziehungsbezogene Rollen, die im Zusammenhang mit der Anwendung eines WfMS in einem Unternehmen auftreten und die für die Betrachtungen des Anwendungsszenarios Workflow Management bezüglich Sicherheitsanforderungen weiter untersucht werden sollen, sind:
- Hersteller des WfMS,
- Betreiber des WfMS,
- Firma, in der das WfMS eingesetzt wird,
- Kunde der Firma, die das WfMS einsetzt.

Zu beachten ist hierbei, daß die Rollen Hersteller und Betreiber des Workflow Management Systems zusammenfallen können, also durch eine Firma repräsentiert werden.
Um die Interessen beider Rollen untersuchen zu können, werden Hersteller und Betreiber im vorliegenden Bericht getrennt betrachtet. Fallen beide Rollen einer Firma zu, so decken sich auch ihre Interessen.

Organisationseinheiten, die in der vorliegenden Anforderungsanalyse in die Diskussion einbezogen werden, sind:
- DV-Abteilung,
- Revision/Controlling,
- Buchhaltung,
- Betriebsrat.

Auch die *Stellen*, die in Unternehmen durch Personen besetzt werden, werden durch die Anwendung eines WfMS erweitert bzw. spezialisiert. Somit zählen zu den relevanten Stellen:
- Sachbearbeiter(in)
- Sekretär(in)
- Administrator Betriebssystem-Ebene
- Administrator Workflowsystem-Ebene
- Modellierer der Workflows
- Manager/Vorgesetzte(r)
- Sicherheits- bzw. Datenschutzbeauftragte(r)

Analog zu den geschäftsbeziehungsbezogenen Rollen Hersteller und Betreiber des WfMS können auch die Rollen der Administratoren der Betriebssystem- und Workflowsystem-Ebene durch ein und dieselbe Person eingenommen werden. Bezüglich der Interessenfindung werden beide Rollen im weiteren jedoch getrennt betrachtet.
Interessant sind auch die möglichen Einordnungen der Rolle des Workflowmodellierers: Zunächst ist es möglich, daß der Betriebssystem- oder Workflowsystem-Administrator auch der Modellierer der Workflows ist. Weiterhin kann der Modellierer verschiedenen geschäftsbeziehungsbezogenen Rollen angehören. So ist es durchaus praktikabel, daß der Workflow-Modellierer nicht Mitarbeiter der Firma ist, die das WfMS in ihrer Organisation einsetzt, sondern daß die Workflows, die in der Firma ablaufen werden, extern durch einen Mitarbeiter des WfMS-Herstellers oder -Betreibers modelliert werden. Dies birgt natürlich Risiken des WfMS-Anwenders hinsichtlich der Vertraulichkeit ihrer internen Daten.

Werden in einem Büro beziehungsweise Unternehmen Workflow Management Systeme eingesetzt, um Abläufe effizienter bearbeiten zu können, so erfolgt eine Abbildung der in der Büroumgebung real existierenden Rollen in das Workflow Management System (siehe Abbildung 2-6). Die Rollen im WfMS - im folgenden kurz als *WfMS-Rollen* bezeichnet - abstrahieren von der realen Welt und sind somit wertfrei und austauschbar.

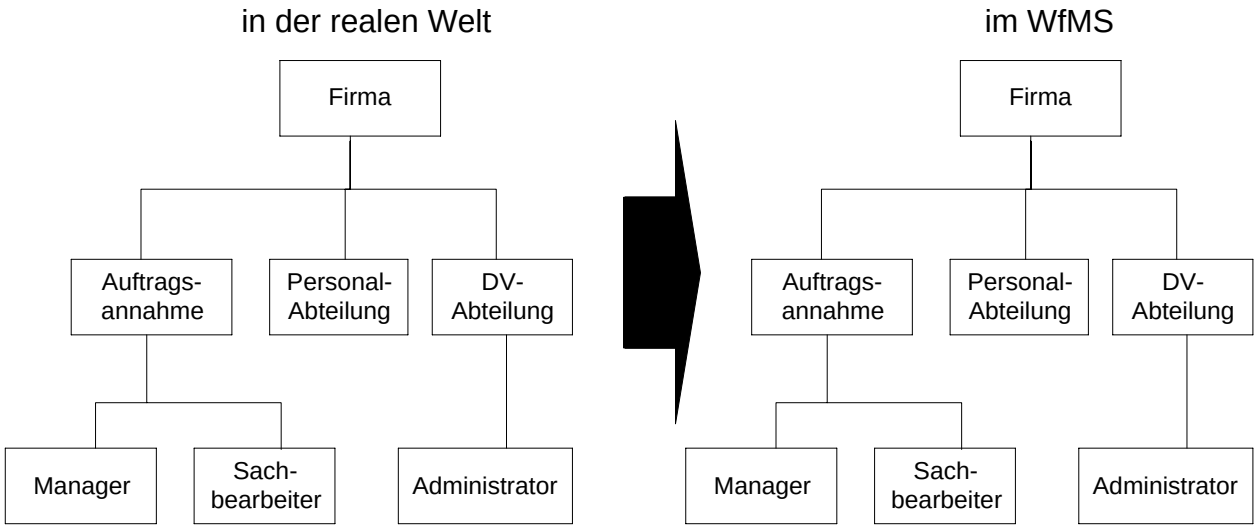


Abb. 2-6: Abbildung der real existierenden Rollen in ein WfMS

Demzufolge finden sich Abstraktionen von den meisten realen Rollen auch innerhalb des Workflow Management Systems wieder. Zusätzlich werden im WfMS Rollen eingeführt, die durch die Arbeit mit Workflow Management Systemen notwendig werden, so z.B. der Initiator eines Vorgangs im WfMS. Betrachtete WfMS-Rollen sind:

- Sachbearbeiter(in),
- Manager/Vorgesetzte(r),
- Sekretär(in),
- Initiator.

2.2.3 Interessen und Sicherheitsanforderungen

Vorüberlegungen

Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen nicht nur einer der beteiligten Parteien. Forderungen nach mehrseitiger Sicherheit können nach [Rann_96] in folgende Teilziele untergliedert werden, die beispielhaft im Umfeld von Workflow Management Systemen erläutert werden:

(1)*Vertraulichkeit* ➔ kein unbefugter Informationsgewinn
In einem Workflow Management System existierende Daten sollen nur den dazu befugten Personen zur Kenntnis gelangen. Dies würde z.B. bedeuten, daß jeder Bearbeiter eines Workflows nur den für seine Arbeit wesentlichen Teil der Daten einsehen darf.

(2)*Integrität* ➔ keine unbefugte Modifikation von Informationen
In einem Workflow Management System existierende Daten sollen nicht unbemerkt geändert werden können. So soll z.B. der Initiator eines Workflows nur wirkliche Instanzen des ursprünglich modellierten Workflowtyps starten können.

(3)*Verfügbarkeit* ➔ keine unbefugte Beeinträchtigung der Funktionalität
Ist ein Workflow Management Sytem ausgefallen, so hängen wesentliche Bearbeitungsvorgänge an den jeweiligen Rechnern der Bearbeiter fest und der allgemeine Arbeitsfortschritt wird beeinträchtigt.

(4)*Zurechenbarkeit* ➔ keine unzulässige Unverbindlichkeit
Es muß klar nachvollziehbar bzw. erkennbar sein, welcher Modellierer welches Workflowmodell erstellt hat, um Administratoren von Workflow Systemen die Möglichkeit zu geben, Unstimmigkeiten bzw. Probleme mit der jeweils verantwortlichen Person zu klären.

Sollen nun die Anforderungen mehrseitiger Sicherheit an Workflow Management Systeme erörtert werden, so muß ihr gesamtes Anwendungsumfeld (siehe Kapitel 2.2.2) in die Betrachtungen einbezogen werden.

Schaut man sich zunächst die geschäftsbeziehungsbezogenen Rollen an, so trifft man auf eine *Kapselung der Organisationsstruktur*: Eine Firma A hat gegenüber einer anderen Firma B lediglich das Interesse, daß ihr Auftrag erfüllt wird. Die Firma B fungiert in ihrer Gesamtheit als Ansprechpartner der Firma A, für die die interne Organisationsstruktur der Firma B verborgen bleibt, wie in Abbildung 2-7 dargestellt.

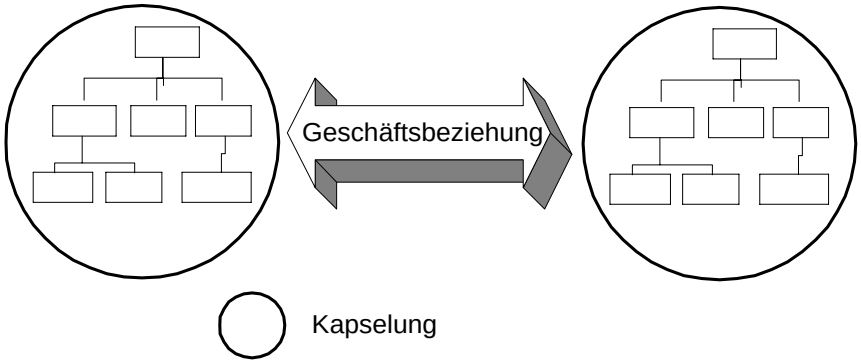


Abb. 2-7: Kapselung in Geschäftsbeziehungen

Untersucht man die Firmeninteressen im Zusammenhang mit der internen Struktur, so findet man eine Interessenvererbung vor. *Interessenvererbung* bedeutet in diesem Zusammenhang, daß die Interessen von Teilbereichen oder Organisationseinheiten einer Firma den Zielen der Firma bzw. Firmenleitung untergeordnet sind und daß sich die meisten Interessen der Mitarbeiter (Stellen) einer Abteilung (Organisationseinheit) aus den Interessen der übergeordneten Organisationseinheit und somit aus den Firmenzielen ergeben (siehe Abbildung 2-8).

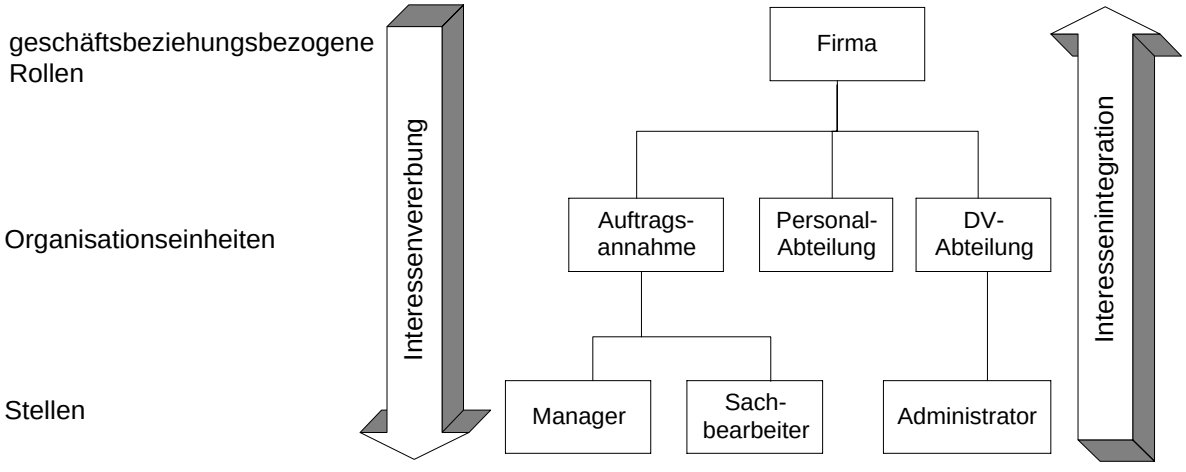


Abb. 2-8: Interessenvererbung und Interessenintegration innerhalb einer Organisation

Aus der gegensätzlichen Perspektive heraus kann man von *Interessenintegration* sprechen, wenn man von den Interessen der Stelleninhaber ausgehend in höhere Ebenen zusammenfaßt. Es wird zugrundegelegt, daß die Inhaber der Stellen individuelle Interessen haben, z.B. Datenschutzinteressen. Unter dieser Voraussetzung können alle nichtwidersprüchlichen Interessen der Stelleninhaber zu den gültigen Interessen der Organisationseinheiten integriert werden. So wird auf der jeweils nächsthöheren Ebene zusammengefaßt, wobei dort natürlich noch weitere vorhandene Interessen hinzugefügt werden, wodurch eine vielfältige Interessenzusammenstellung entsteht, bis die Ebene der Firmenleitung erreicht ist.

In den weiteren Betrachtungen wird davon ausgegangen, daß alle Bereiche, Organisationseinheiten und Mitarbeiter eines Unternehmens ihre Interessen im allgemeinen den Firmenzielen unterordnen, d.h., daß die Individualinteressen nicht widersprüchlich zum Gesamtziel der Organisation sind.

Interessen

Im folgenden Abschnitt werden Sicherheitsinteressen für die im Kapitel 2.2.2 identifizierten Rollen beschrieben. Dabei werden kurz Interessen allgemeinerer Natur angegeben, aus denen sich in den meisten Fällen Sicherheitsinteressen ableiten lassen. In tabellarischer Form werden Sicherheitsinteressen zu den in der oben angeführten Sicherheitsdefinition erläuterten Sicherheitseigenschaften Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit zugeordnet.
Es wird explizit darauf hingewiesen, daß die Sammlung der Interessen keinerlei Anspruch auf Vollständigkeit erhebt. Weitere Interessen ergäben sich zum Beispiel, wenn konkrete Rollengegenüberstellungen (*Wer* will was vor *wem* sichern?) diskutiert würden.

A) geschäftsbeziehungsbezogene Rollen:
Grundlegende Interessen der Beteiligten auf dieser Ebene ergeben sich unmittelbar aus dem Zusammenhang der Geschäftsbeziehungen. So möchte der Hersteller des WfMS natürlich sein Produkt verkaufen. Hersteller und Betreiber wollen den Kunden insoweit zufriedenstellen, daß ihr Image gesichert ist und dadurch auch zukünftig das Workflow Management System verkauft bzw. betrieben werden kann.
Der Kunde möchte in erster Linie, daß sein Auftrag zu seiner Zufriedenheit erfüllt wird. Er hat den Wunsch nach einem Ansprechpartner innerhalb der Firma und will seine Interessen im Extremfall durch einen Mitarbeiter der Firma z.B. (in einer Bank) vertreten wissen.
Die Firma, in der das Workflow Management system eingesetzt wird, hat das Ziel, daß ihre Unternehmensabläufe durch den Einsatz des WfMS effizienter und schneller bearbeitet werden. Sie möchte Zusicherungen über die Funktionalität und die Adäquatheit des WfMS vom Hersteller oder Betreiber des Systems. Der Kunde soll bei Nachfragen zügig Auskunft über den Stand der Bearbeitung seines Auftrages erhalten. Die Firma möchte möglichst viele Informationen über den Kunden zur Erstellung eines Kundenprofiles sammeln, um dessen Wünsche schneller identifizieren und somit schneller darauf reagieren zu können.

Aus der Tabelle, in der die Sicherheitsinteressen der geschäftsbeziehungsbezogenen Rollen eingeordnet sind, ist ersichtlich, daß in der Praxis eine Abgrenzung der Sicherheitsziele Verfügbarkeit und Integrität nur schwer zu vollziehen ist. Diese Unterteilung erscheint sinnvoller, wenn die Interessen nach Primär- und Sekundärinteresse differenziert werden (vgl. Kapitel 2.1.3).

Rollen	Interessen bezüglich			
	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit
Betreiber des WfMS	• Konfiguration des WfMS bezüglich der jeweiligen Kundenfirma	• Workflow Management System		• ordnungsgemäßer Betrieb • WfMS unverfälscht betrieben
Hersteller des WfMS	• verwendete Algorithmen und Realisierungsdetails des WfMS	• Workflow Management System		
Kunde	• Information über gemäß DSG gespeicherte persönliche Daten			• Auftrag und Ergebnisse der Auftragsarbeit
	• persönliche Daten	• Information über Stand der Bearbeitung des Auftrages		
Firma, die WfMS einsetzt	• kein Firmen-Know-How offenbaren • Daten, die innerhalb eines Arbeitsvorganges anfallen bzw. verarbeitet werden • keine internen Daten an Hersteller/ Betreiber/ Modellierer	• Workflow Management System		

Tab. 2-4: Sicherheitsinteressen geschäftsbeziehungsbezogener Rollen

B) Organisationseinheiten:

Einen wesentlichen Aspekt stellt die Ordnungsmäßigkeit und gegebenenfalls Rechtsverbindlichkeit bestimmter Büroaktivitäten dar. Hier muß bei Workflow Management System der gleiche Status erreicht werden, der in der Papierwelt gefordert ist. Zum Beispiel muß für alle vertragsrelevanten Dokumente deren Unversehrtheit, Eindeutigkeit und Unbestreitbarkeit gewährleistet sein.

Rollen	Interessen bezüglich			
	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit
DV-Abteilung		• technische Infrastruktur	• moderne Technik	• Datenzugriffe
Revision/ Controlling		• Historie von Arbeitsabläufen • Angaben zu geleisteter Arbeitszeit		
Buchhaltung		• Abrechnungsdaten		
Betriebsrat	• keine unzulässige Überwachung der Mitarbeiter			

Tab. 2-5: Sicherheitsinteressen von Organisationseinheiten

Für mögliche Betriebs- oder Vorgangsprüfungen müssen alle relevanten Geschäftsdokumente sicher archiviert und die dabei durchlaufenen wesentlichen Arbeitsschritte zu Nachweiszwekken aufgezeichnet sein (Revisionsfähigkeit) [Herd_95].

Werden im Workflow Management System personenbezogene Daten verarbeitet, sind neben den allgemeinen Regelungen des Datenschutzgesetzes des Bundes und der Länder auch Betriebsvereinbarungen oder individuelle Abmachungen mit einzelnen Mitarbeitern zu berücksichtigen. In diesem Zusammenhang ist gegebenenfalls darauf zu achten, daß die Daten externer Personen (zum Beispiel Kunden) ausschließlich gemäß deren expliziter Vorgaben verwendet oder weitergegeben werden.

C) Stellen:
Die Inhaber der Stellen entwickeln bestimmte Interessen bei der Arbeit mit einem Workflow Management System. Das heißt, Inhaber von Stellen haben neben den Interessen, die sich generell aus dem Arbeitsumfeld ergeben, zusätzliche Interessen, die erst durch den Einsatz eines WfMS im Unternehmen entstehen. Deshalb werden die Inhaber der Stellen im wesentlichen ihre konventionellen Interessen besitzen; diese werden aber in vielen Fällen durch die Benutzung eines WfMS erweitert.

Rollen	Interessen bezüglich			
	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit
Sachbearbeiter(in)/ Sekretär(in)	• keine minutiöse Überwachung der Arbeit • Möglichkeit der Korrektur eigener Fehler • persönliche Arbeitszeiteinteilung • benutzte/benötigte Hilfsmittel ⇒ Workflowhistorie	• Arbeitsumgebung • Aufgabenstellung	• benötigte Hilfsmittel	• erledigte Aufgaben • erstellte Dokumente
Administrator Betriebssystem-Ebene	• Arbeitsumgebung	• Zugriffsrechte • Betriebssystem		• Information über Zugriffe (Log-Files)
Administrator Workflowsystem-Ebene	• Arbeitsumgebung • Bearbeiter sehen nur den für ihre Arbeit relevanten Teil des Workflows	• Zugriffsrechte (Rollen) • Workflowsystem		• Information über Rolleneinnahmen (Log-Files) • Zuordnung von Workflows zu Modellierern
Modellierer der Workflows	• Arbeitsumgebung	• modellierte Workflows • Ausgangsdaten für die Workflowmodellierung		• Zuordnung von Workflows zu Modellierern
Manager/ Vorgesetzte(r)	• Arbeitsumgebung	• modellierte Kompetenzen		
Sicherheits- bzw. Datenschutzbeauftragte(r)	• Mitarbeiterdaten • Kundendaten			

Tab. 2-6: Sicherheitsinteressen von Stelleninhabern

An der Ausführung eines Workflows beteiligte Mitarbeiter (z.B. Sachbearbeiter(in) oder Sekretär(in)) wollen eine gerechte Aufgabenverteilung, d.h. keinerlei Übervorteilung einzelner Mitarbeiter und eine Aufgabenzuteilung gemäß der eigenen Fähigkeiten und Stellenbeschreibung. Das bedeutet gleichzeitig, daß die Workflowmodellierung darauf ausgerichtet sein muß, diese Ziele zu erfüllen; sie muß also adäquat sein.
Manager wünschen sich u.a. eine zügige Aufgabenbearbeitung, eine zum Zwecke der Arbeitsverfolgung ausreichende Überwachung des Arbeitsflusses im Unternehmen und eine Aufgabenverteilung gemäß den vorhandenen Ressourcen und Kompetenzen der Mitarbeiter.

Betrachtet man die Schritte, die ausgehend von der Erhebung der im Unternehmen ablaufenden Vorgänge bis hin zur Abarbeitung modellierter Workflows getan werden müssen, so kann man direkt auf Sicherheitsfragen schließen.
Dabei ist es immer wichtig zu betrachten, welche Rollen welche Tätigkeiten übernehmen. Erhebt zum Beispiel die Firma, die plant, ein WfMS einzusetzen, ihre internen Vorgänge nicht selbst, sondern beauftragt eine externe Firma mit der Geschäftsprozeßerhebung, so sollte schon an diesem Punkt die Diskussion von Sicherheitsfragen beginnen. Grund dafür ist die Offenlegung interner Vorgänge an Außenstehende.
Ein extern eingesetzter Workflowmodellierer z.B. als Mitarbeiter der Betreiberfirma hat sogar über die reine Kenntnis der unternehmensinternern Daten hinaus weitere Macht. Er modelliert die Arbeitsabläufe im Workflow Management System, die später von den Mitarbeitern der Firma ausgeführt werden müssen. Somit besteht die Gefahr, daß modellierte Workflows eher den Interessen des Modellierers entsprechen als denen der Firma.

D) WfMS-Rollen
Da WfMS-Rollen im wesentlichen Abbildungen der real existierenden Rollen im Workflow Management System sind, entsprechen die Interessen der Rolleninhaber der WfMS-Rollen denen der Stelleninhaber. Die einzige Rolle, die ein Mitarbeiter lediglich innerhalb des Workflow Management Systems einnehmen kann, ist die Rolle des Initiators eines Workflows. Aus diesem Grund wird für die Interessen der Rollen Sachbearbeiter(in), Sekretär(in), Manager usw. auf die Tabelle 2-6 verwiesen, und es werden in der Tabelle 2-7 lediglich die Interessen des Initiators aufgeführt.

Rollen	Interessen bezüglich			
	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit
alle Rollen und ihre Interessen aus Tabelle 2-6 und zusätzlich:				
Initiator		• Workflowmodell bzw. Workflow-beschreibung		• Workflow • Startzeitpunkt

Tab. 2-7: Sicherheitsinteressen von WfMS-Rollen

2.2.4 Beispiele konkreter Systeme

Im vorliegenden Kapitel werden einige Implementationen von Workflow Management Systemen kurz vorgestellt. Es wird Bezug auf ihre Besonderheiten genommen, die teilweise Ansätzen von Sicherheitslösungen entsprechen oder aus denen Probleme im Sicherheitsbereich entstehen.

WorkParty (SNI)

WorkParty ist ein kommerziell verfügbares Workflow Management System der SNI AG. WorkParty ist ein System, das vielen verschiedenen Anforderungen an die Funktionalität von Workflow Management Systemen gerecht wird.

Ein im Kontext von Sicherheitsfragen besonders hervorzuhebender Aspekt ist der internationale Einsatz des Systems. So werden laut Angaben von SNI bei einem Kunden bereits Workflows zwischen Deutschland, Mexiko und Tschechien gesteuert.
Diese Anwendung des WfMS über Ländergrenzen hinweg bringt aufgrund der unterschiedlichen Gesetzgebungen in den verschiedenen Staaten zunächst rechtliche Probleme mit sich, die noch verschärft werden, wenn die Kommunikation zwischen den Beteiligten verschlüsselt vorgenommen werden soll. Den Autoren sind bisher leider keine Lösungsansätze der Firma SNI für dieses Problem bekannt.

ProMInanD (IABG)

Ein weiteres kommerzielles Workflow Management System ist das System ProMInanD (Process Migration Integration and Dispositions). Besonders herausgestellt werden soll an dieser Stelle das Rollenkonzept dieses Systems.
Zu bearbeitende Workflows oder Schritte werden in ProMInanD einer Rolle zugewiesen. Durch eine entsprechende Auswahl der Rolle durch den Modellierer kann der Kreis von Personen eingeschränkt werden, die einen Arbeitsschritt in einem Workflow bearbeiten dürfen.
In der Organisationsdatenbank von ProMInanD wird neben der Festlegung der einnehmbaren Rollen auch definiert, welche Rollenkombinationen sich ausschließen. Diese verbotenen Rollenkombinationen ergeben sich aus Interessen- und Befugniskonflikten [Herd_93].

BPAFrame (TU Dresden)

BPAFrame (Framework for Business Process Automation) wird innerhalb eines Projektes am Lehrstuhl Rechnernetze der TU Dresden [BPAF_1] entwickelt und ist ein Workflow System, das auf CORBA-Technologie aufsetzt. CORBA ist der Standard der Object Management Group (OMG) [OMG_1] für verteilte objektorientierte Anwendungen.

Ein erster Prototyp von BPAFrame ist bereits fertiggestellt und befindet sich zur Zeit in einer Phase der Umstrukturierung und Erweiterung. Bisher ist außer der Absicherung der Scriptdatenbank (Workflowbeschreibungen) und der Administrationsdatenbank keinerlei explizite Sicherheitsfunktionalität im System integriert.
Nach Meinung der Entwickler wären Sicherheitsfunktionen jedoch nach der Verfügbarkeit von CORBA-Security-Implementationen mit geringerem Aufwand als bei herkömmlicher Programmierung integrierbar. Die Probleme liegen dann eher bei CORBA security services und ihren Unzulänglichkeiten [OMG_95].

CodAlf (TU Dresden)

Ein weiteres an der TU Dresden entwickeltes Steuerungssystem für verteilte Abläufe ist das CodAlf System. Es ist ein traderbasiertes [Gass_95] auf OSF/DCE [OSF_1] aufsetzendes System.

Auch für dieses System hängen die Möglichkeiten der Erfüllung von Sicherheitsanforderungen zunächst von den in der verteilten Softwareplattform OSF/DCE definierten Standard-Sicherheitsmechanismen ab. Diesem Problem wurde hier damit begegnet, daß im Trader einige Sicherheitsmechanismen implementiert wurden.
Ein weiterer interessanter Aspekt besteht in der Realisierung der differenzierten Überwachungsmöglichkeiten der Workflow-Bearbeitungsstati durch verschiedene Rollen. So haben Initiator des Workflows, Administrator des Workflow Management Systems oder Bearbeiter eines Schrittes des Workflows unterschiedliche Möglichkeiten der Einsicht gemäß ihren Kompetenzen.

2.3 Anwendungsbeispiel: Medizin

2.3.1 Einleitung

Im medizinischen Umfeld existieren schon immer besonders hohe Datenschutzanforderungen, die sich in solchen Grundprinzipien wie der Schweigepflicht des Arztes äußern. Diese Anforderungen resultieren aus der hohen Vertraulichkeit der anfallenden medizinischen und persönlichen Daten und werden auch in den seltensten Fällen in Frage gestellt. Andererseits sind die Ärzte nach §11 ihrer Berufsordnung dazu verpflichtet, Dokumentationen zu erstellen [Zila_95], die persönliche und medizinische Daten enthalten. Diese gehen in wesentlichem Maße in die Patientenakte ein, deren elektronische Abbildung eine große Herausforderung an die Informationstechnik darstellt, da sie die weitgehende Standardisierung von Datenformaten, medizinischen Termini und Kommunikationsarten erforderlich macht.
Weiterhin ist die Verfügbarkeit aktueller und korrekter Daten eine wesentliche Voraussetzung für fundierte medizinische Entscheidungen, von denen Leib und Leben des Patienten abhängen können. Dies geht einher mit der Forderung nach gleichzeitiger Realisierung strengster Sicherheitsvorschriften.
Es gibt viele Anwendungen, an die zuzüglich zu ihren Anforderungen im normalen Einsatz verschärfte Anforderungen zu stellen sind, wenn sie im medizinischen Bereich angewendet werden. Das betrifft z.B.:

- Informationssysteme, bei denen Fehler in Datenbeständen zu lebensbedrohlichen Situationen führen können,
- Kommunikationssysteme, die zur Wahrung der Vertraulichkeit in hohem Maße abhörsicher sein sollten,
- rechtsverbindliche Zuordnung von Dokumenten, Echtheitsnachweise und Zeitstempel

Ein Sicherheitsaspekt, der oft durch den Einsatz von Computertechnologie untergraben wird, ist die rechtsverbindliche Zuordnung von Dokumenten zu ihrem Urheber. Dies ist insbesondere bei der Bereitstellung von medizinischen Informationen zu beachten.
Ein technisches Mittel, um diese Zuordnung zu realisieren, sind digitale Signaturen. Diese bieten weiterhin den Vorteil, daß sie auch zur Überprüfung der Integrität erhaltener Daten verwendbar sind. Ein ausgezeichnetes Anwendungsgebiet für solche digitalen Signaturen stellen die schon erwähnten medizinischen Informationssysteme dar, aber auch andere Anwendungen wie die Ausstellung von Rezepten oder Krankschreibungen profitieren vom Einsatz digitaler Signaturen.
Laut [Zila_95] weisen die in der Medizin verwendeten Systeme die charakteristischen Merkmale offener verteilter Anwendungen auf, wie

- die Verteiltheit der Datengenerierung, - verarbeitung, - speicherung und -nutzung,
- Heterogenität der Systemkomponenten,
- Autonomie der Benutzung und
- Offenheit der Kommunikationsbeziehungen.

Gerade die beiden letzten Punkte stellen sich als problematisch dar, da sie den oft vorhandenen Konflikt zwischen Offenheit und Restriktionsfreiheit des Systems und dessen Sicherheit beinhalten.
Momentan gibt es erste Feldversuche zur Wahrung der Vertraulichkeit bei Kommunikation zwischen Ärzten und Abrechnungsstellen (s. [Tenh_96]). Auch hier wurden als wesentlich Anforderungen an medizinische Daten genannt:

- Integrität
- Verfügbarkeit

- Vertraulichkeit
- Authentizität
- Nichtabstreitbarkeit
- Originalität

Diese Kriterien erzwingen den Einsatz solcher Mechanismen wie Datenverschlüsselung und digitaler Signaturen.
Der genannte Versuch ist jedoch nur als ein erster Schritt auf dem Wege zur offenen und sicheren Kommunikation im Medizinbereich zu betrachten.

2.3.2 Identifizierte Rollen

Zur Veranschaulichung der in einem typischen Szenario auftretenden Rollen betrachte man die folgende Abbildung:

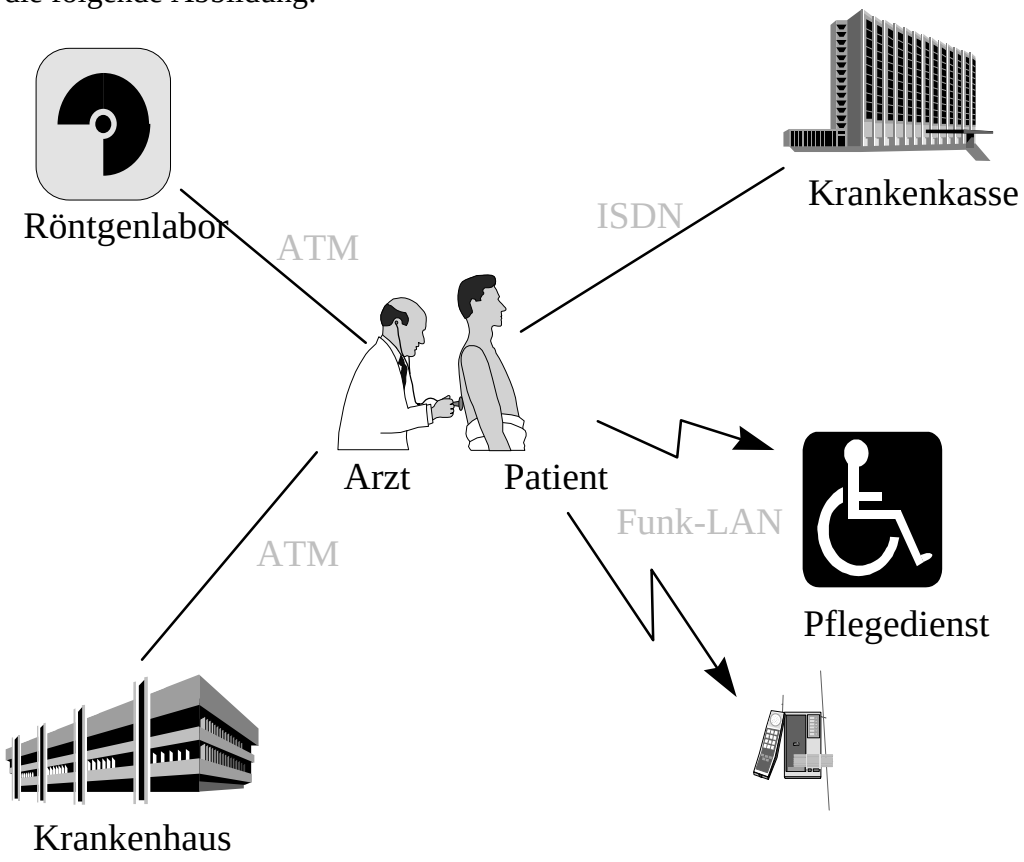


Abb. 2-9: Beispielszenario Medizin

Die Beteiligten kann man den folgenden Rollen zuordnen:
– Patient
– Arzt
– Laborpersonal
– Pflegedienst
– Krankenhaus
– Krankenkasse

2.3.3 Interessen und Sicherheitsanforderungen

Die Interessen der in Abschnitt 2.3.2 aufgeführten Rollen sind in der nachfolgenden Tabelle zusammengestellt und jeweils den Kriterien Vertraulichkeit, Integrität und Verfügbarkeit zugeordnet.
Es stellt immer eine gewisse Schwierigkeit dar, die Kriterien Verfügbarkeit und Integrität voneinander zu trennen, denn:

- ohne Verfügbarkeit kann ein Dienst selbstverständlich keine Integrität garantieren und
- ein verfügbarer Dienst ist wertlos, wenn er keine Integrität bieten kann.

Dies spiegelt sich in der nachfolgenden Tabelle dergestalt wieder, daß die Spalten Integrität und Verfügbarkeit zusammengefaßt wurden.
Die Aufstellung dieser Interessen erhebt keinen Anspruch auf Vollständigkeit, da sich nahezu beliebige weitere Interessen mit bestimmten Szenarien aufstellen und begründen ließen.

Rollen	Interessen bezüglich			
	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit
Patient	• Befunde	• Dokumentation • Technik • Personal		• Dokumentation
Arzt	• Überwachung • Kollegen Informationen vorenthalten	• Patientendaten • Daten für Forschungszwecke		• Informationen von Kollegen
Pflegedienst	• keine Überwachung	• Patientendaten		• Aufträge • Anweisungen
Krankenhaus	• nach Datenschutzgesetz relevante Daten	• Abrechnungsdaten • Dokumentation • Betriebsmittel • Zutrittskontrolle		
Krankenkasse		• Wissen über Diagnosen/Therapien • Abrechnungsdaten • Informationen über potentielle Mitglieder		• Abrechnungsdaten

Tab. 2-8: Interessen im Medizinbereich

Das in dieser Tabelle enthaltene Konfliktpotential beruht vor allem auf den unterschiedlichen Interessen verschiedener Gruppen in bezug auf Vertraulichkeit bestimmter Daten und ihrer Verfügbarkeit für andere.
Ein Beispiel sind die Befunde, die außer den Patienten und den Arzt auch die Krankenkasse interessieren, da sie so die erstellten Diagnosen und verordneten Medikamente nachprüfen könnte. Das Ziel dieser Vorgehensweise ist eine Möglichkeit für die Krankenkassen, Behandlungen als unverhältnismäßig zu deklarieren und so Kosten zu sparen.
Weiterhin muß das Äquivalent der eigenhändigen Unterschrift existieren, um bei eventuellen Rechtsstreitigkeiten vor Gericht verwertbare Beweise zu haben.

2.3.4 Konkrete Problemsituationen

Entfernte Zugriffe auf ein medizinisches Informationssystem

Dieses Szenario befaßt sich mit der Datenhaltung eines solchen Systems und wurde gewählt, da ein Projektvorschlag des Medical Network e.V. in Zusammenarbeit mit dem Universitätsklinikum Dresden existiert, der sich mit dieser Problematik befaßt. Konkret ist das Ziel der Aufbau eines Kompetenzzentrums mit der Funktion eines Informationspools für den Bereich Pharmakologie.
Im Rahmen der Projektdurchführung sind Kontakte zwischen der SSONET-Projektgruppe und dem Universitätsklinikum vorgesehen, so daß sich die Betrachtung eines solchen Szenarios hier anbietet.
Im genannten Projektvorschlag wird von einem zweigleisigen Informationsmodell ausgegangen, das einerseits übliche persönlich Auskunftsdienste wie Telefonservice sowie andererseits einen über Datenverbindungen direkt erreichbaren Datenpool beinhaltet. Die Datensammlung umfaßt umfangreiche Informationen zu den wichtigsten klinisch relevanten Arzneimitteln, die nur für Ärzte bzw. entsprechend ausgebildete Personen zugänglich sein sollten.
Hier wird aus naheliegenden Gründen nur die zweite Informationsvariante betrachtet und als ein mögliches Szenario das folgende vorgeschlagen:
Die Datensammlung besteht aus einer in einer Klinik befindlichen Datenbank, auf die Ärzte durch Datenverbindung (Modem oder ISDN) aus ihrer Praxis Zugriff haben.
Zugriff auf dieses System haben:

- Datenbankbetreiber
- Systemadministrator des Rechnersystems, auf dem die Datenbank läuft
- Datenbankadministrator
- Datentypisten (sofern nicht mit Datenbankadministrator identisch)
- Datenlieferanten (z.B. Pharmaproduzenten)
- abrufende Ärzte

Es wird angenommen, daß die Rechnersysteme sowohl bei den Ärzten als auch beim Datenbankbetreiber vertrauenswürdig sind, also insbesondere nicht durch Dritte hardware- oder softwaretechnisch verändert werden können. Dies kann z.B. durch Zusammenwirken von physischen Zugriffsschutz (in angemessenem Rahmen) und softwareseitige Zugangskontrollen ausreichend gut realisiert werden.
Die Akteure in diesem Szenario haben folgende Interessen:

Akteur	Interessen
Datenbankbetreiber	– Historie – Abrechnungsdaten – korrekte Datenbasis (Image), Integritätskontrolle – aktuelle Daten – hohe Datensicherheit und Verfügbarkeit des Systems – Zugriff nur für autorisierte Personen – Zuordnung von Datenbeständen zu Verursachern bei Konflikten – Einhaltung von Datenschutzrichtlinien
Systemadministrator	– Kontrolle über das System – Verfügbarkeit des Systems – Zugangskontrolle – keine Arbeitsüberwachung
Datenbankadministrator	– keine Arbeitsüberwachung – Zugriffskontrolle auf Datenbank – Verfügbarkeit des Systems – Datenintegrität – Zuordnung von Datenbankaktionen (Historie)
Datentypisten	– keine Arbeitsüberwachung – Zuordnung von Daten (zum Nachweis externer Fehler)
Datenlieferanten	– Nachweis korrekt gelieferter Daten – externer Zugriff mit Korrekturmöglichkeiten – schnellstmögliche Integration neuer Daten in Datenbank
Ärzte	– korrekte Daten – aktuelle Daten – Zuordnung der Daten zum Erzeuger zum Nachweis von Fehlern – Verfügbarkeit des Systems – einfache Bedienung – mit einfacher, ggf. schon existierender Technik zu realisieren – keine Übermittlung von Abfragedaten an andere

Tab. 2-9: Sicherheitsinteressen im medizinischen Informationssystem

Die Konflikte, die sich ergeben, lassen sich wiederum den vier Sicherheitsmerkmalen Verfügbarkeit, Integrität, Vertraulichkeit und Zurechenbarkeit zuordnen.
Die Verfügbarkeitsproblematik stellt sich in allen relevanten Computeranwendungen und wurde auch schon in großem Maße untersucht. Im medizinischen Umfeld bestehen besonders hohe Anforderungen, die zu solchen extremen Maßnahmen wie komplett redundanten Systemen mit jeweils redundanter Stromversorgung führen. Im vorliegenden Fall sollte die Verfügbarkeit hoch sein, es dürften jedoch keine unmittelbar bedrohlichen Situationen bei einem kurzzeitigen Ausfall des Systems auftreten. Eine Wiederanlaufstrategie mit Überprüfung der Daten hinsichtlich Konsistenz und Vollständigkeit erscheint jedoch notwendig.
Die Integrität von Daten soll sicherstellen, daß die Korrektheit der Daten immer auf überprüfbare Weise gewährleistet ist. Genauer gesagt sollen absichtliche und unabsichtliche Modifikationen nach der Dateneingabe erkannt werden. Diese Aufgabenstellung läßt sich dahingehend mit der Zurechenbarkeitsproblematik in Verbindung bringen, daß sich beide mittels digitaler Signaturen realisieren lassen.
Die Zurechenbarkeit erscheint als ein extrem wichtiger Punkt, da sie die Rechtsverbindlichkeit von Daten und ihre eindeutige Zuordnung zu ihrem jeweiligen Erzeuger ermöglicht. Dies ist besonders bei fehlerhaften Informationen von großer Bedeutung.
Vertraulichkeit ist durch Verschlüsselung zu erreichen. Im Sinne eines einfacheren Schlüsselmanagements sind asymmetrische Verfahren vorzuziehen. Die Vertraulichkeit von Infor-

mationen besteht vor allem seitens des Arztes gegenüber anderen Beteiligten, da dabei eventuell direkt oder indirekt seine Patienten betroffen sein können.
Zusammenfassend kann man folgende Kriterien aufstellen:

1. Es ist ein Datenbanksystem mit ausgefeilten Transaktionsmechanismen einzusetzen.
2. Es sollten sowohl Verschlüsselung als auch digitale Signaturen unterstützt werden.
3. Die Technik sollte auf Anwenderseite einfach anzuwenden und nicht mit hohen Kosten verbunden sein.

Ein Ansatz zur Lösung der gesamten Aufgabenstellung unter diesen Voraussetzungen besteht darin, die Techniken des World Wide Web mit denen von herkömmlicher Datenbanksysteme und dem Programm PGP zur Verschlüsselung und Signatur [Stall_95] zu verbinden.
Das Szenario ist folgendes:
Der Datenbankbetreiber setzt ein kommerzielles Datanbanksystem mit SQL-Schnittstelle ein. Weiterhin besitzt er einen WWW-Server, der über diese SQL-Schnittstelle Informationen mit der Datenbank austauschen kann.
In die Datenbank werden die Daten komplett mit der zugehörigen digitalen Signatur eingetragen, die mit PGP erzeugt wird.
Auf Anwenderseite wird ein Internetzugang und ein WWW-Browser benötigt (und natürlich PGP). Die für die Überprüfung der Signaturen nötigen öffentlichen Schlüssel werden über die WWW-Verbindung zum Anwender übertragen, dieser muß im Gegenzug seinen öffentlichen Schlüssel dem Datenbankbetreiber bekanntmachen und sich dabei authentisieren. Die Authentikation erfolgt dabei außerhalb des hier beschriebenen Systems, z.B. über persönliches Erscheinen oder eine dritte Instanz, der sowohl Anbieter als auch Anwender vertrauen.
Alle Anfragen durch den Arzt werden mit dem öffentlichen Schlüssel des Anbieters verschlüsselt und vom Anwender signiert. Auf diese Weise kann nur der Anbieter die Anfrage lesen und gleichzeitig eine Zulässigkeitsprüfung für die Anfrage vornehmen.
Die Anfrage wird dann durch die Datenbank bearbeitet, das Ergebnis signiert und mit dem öffentlichen Schlüssel des Anwenders verschlüsselt zurücktransportiert.
Beim Anwender wird die Entschlüsselung und Signaturprüfung durch PGP vorgenommen (das dazu vom WWW-Browser aus automatisch aufgerufen wird).
Die eben skizzierte Lösung bietet den Vorteil, relativ preiswert und verfügbar zu sein und dennoch anerkannt sichere Mechanismen wie die von PGP zu benutzen.
Das Hauptproblem stellt vermutlich der sorgsame Umgang mit dem geheimen Schlüssel. Es wäre zu überlegen, diese in einen an das System anschließbaren Kartenleser zu integrieren, aber das sind schon weiterführende Überlegungen, die erst nach einem Test der einfacheren Lösung sinnvoll erscheinen.

3 Grob-Sicherheitsarchitektur

3.1 Einführung

Der Architekturbegriff umfaßt allgemein die Beschreibung des Zwecks und die Beschreibung einer dem Zweck angepaßten Form einer Struktur. Speziell für die Kommunikation in Netzen versteht man unter Architektur die logische Struktur des Netzes (im Gegensatz zur topologischen Struktur), die also das zweckorientierte funktionelle Wirkprinzip des Netzes beschreibt, vgl. [Wern_95]. Der Zweck der Sicherheitsarchitektur wird jetzt näher untersucht.
Die hier betrachtete Welt sieht Systeme vor, an denen mehrere Nutzer beteiligt sind. Die Nutzer werden als mit berechtigtem Interesse am System teilnehmend betrachtet. Üblicherweise verfolgt jeder Nutzer in Abhängigkeit von seiner Rolle, die er im System einnimmt, unterschiedliche Ziele. Vorausgesetzt wird, daß die Nutzer diese Ziele mit dem System verfolgen wollen. Sie sollten daher *im eigenen Interesse* handeln können, ohne daß sie von vornherein durch das System daran gehindert werden. Falls letzteres geschieht, wäre dem Teilnehmer die Nutzungsgrundlage praktisch entzogen. Im eigenen Interesse zu handeln, bedeutet auch, daß das System jedem Nutzer ermöglichen soll, für die eigene Sicherheit zu sorgen. Damit wird erreicht, daß das Sicherheitsbedürfnis einer einzelnen Instanz berücksichtigt wird, und zwar so, daß es nur von ihrem eigenen Tun und Lassen abhängt. Damit wäre ein wesentliches Prinzip (das der Verantwortlichkeit) durch das System unterstützt.
Nachdem das System dem Nutzer die Freiheit läßt, seine Ziele zu verfolgen (Standardfall), ist zu untersuchen, wie sich das auf die Sicherheit der anderen Systemteilnehmer auswirkt. Klar ist, daß damit zu rechnen ist, daß Nutzer in einem System ihre eigenen Interessen verfolgen, ohne die der anderen Teilnehmer mehr als nötig zu berücksichtigen. Insbesondere trifft das auch auf Sicherheitsinteressen zu. Aus Sicht eines einzelnen Teilnehmers würde es genügen, daß das System zuerst die eigenen Sicherheitsbedürfnisse voll unterstützt und die der anderen Teilnehmer nur soweit wie für das Zustandekommen einer tragfähigen Beziehung aus eigener Sicht nötig. Ein so gestaltetes System gewährleistet *einseitige Sicherheit*. Einem Teilnehmer wird mehr Freiheit in der Ausübung seiner Sicherheitsinteressen eingeräumt als anderen.
Mit der Unterstützung nur einseitiger Sicherheit in einem System gibt es jedoch immer Nutzer, deren Sicherheit nicht nur von eigenem Handeln abhängt, sondern auch von dem anderer. Das oben genannte Verantwortlichkeitsprinzip wird so nicht unterstützt.
Es erscheint durchaus legitim zu verlangen, daß Nutzer in der Wahrung ihrer Sicherheitsinteressen durch das System gleichberechtigt zu unterstützen sind. Wenn man allen Nutzern zubilligt, daß ihre Sicherheit nicht von der Gutwilligkeit anderer abhängt, sondern nur auf eigenem Verhalten aufbaut, kann man ein System, daß dieses Konzept verwirklicht, *mehrseitig sicher* nennen.

Die spezielle Sicherheitsarchitektur verfolgt also den Zweck, einen Rahmen für mehrseitige Sicherheit für Menschen bzw. Organisationen, die das System nutzen oder davon betroffen sind, zu geben. Teilnehmern soll es möglich sein, bei Nutzung z.B. verteilter Anwendungssysteme Sicherheitsinteressen und- bedürfnisse zu formulieren, den Bedarf auszuhandeln und durchzusetzen.

3.2 Grob-Sicherheitsarchitektur-Varianten

3.2.1 Variante mit SW-Schirmungsschicht

Zunächst sei auf folgendes Szenario hingewiesen: Das Betriebssystem bindet Fremdmodule ein, die Sicherheitsfunktionalität anbieten und stellt sie Applikationen zur Verfügung, vgl. [Wiew_96]. Die Schnittstellen sind dabei genau beschrieben, so daß Applikationen in der Lage sind, einzelne angebotene Bibliotheksfunktionen aufzurufen, ohne die Implementation in den Modulen zu kennen. Es ist vorgesehen, für ein- und dieselbe Sicherheitsfunktionalität (beispielsweise für digitale Signaturen) eine Auswahl unter Modulen verschiedener Anbieter treffen zu können, von denen dann eines eingebunden wird. Module können dabei auch Hardwarekomponenten beinhalten.
Im folgenden wird das Betriebssystem um einen Sicherheitsmanager erweitert, der eine neue Ebene zwischen den Modulen, Applikationen und dem Betriebssystem bildet. Applikationen greifen so nicht mehr direkt auf das Betriebssystem zu, wenn sie Sicherheitsmechanismen nutzen.

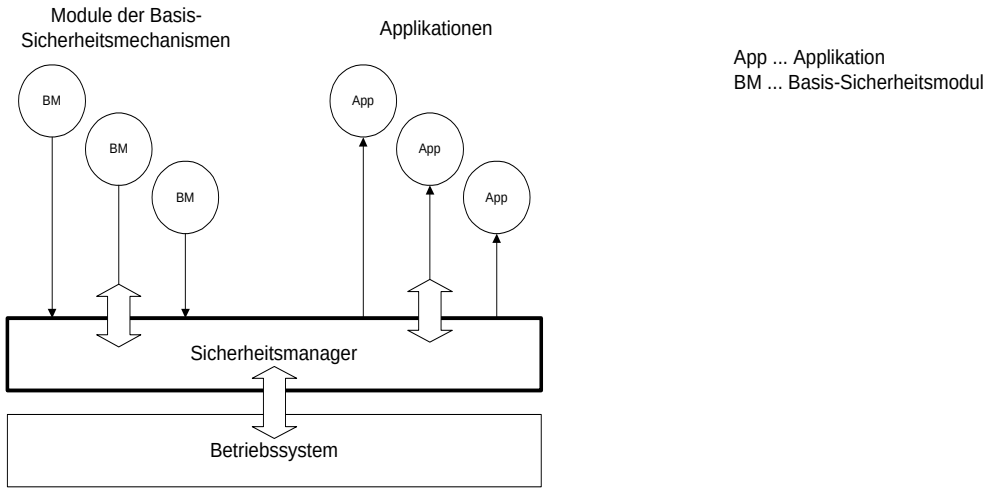


Abb. 3-1: Architektur mit SW-Schirmungsschicht

Architektur:
Die vertrauenswürdige Schicht „Sicherheitsmanager“ schirmt das Betriebssystem ab. Sie ist konfigurierbar (evtl. weitere Schnittstelle nach oben). Applikationen können nur über den Sicherheitsmanager Sicherheitsmechanismen der zur Verfügung stehenden Module nutzen und Betriebssystemaufrufe vornehmen. Applikationen sind gezwungen, auf die vom Sicherheitsmanager gefiltert und konfiguriert bereitgestellten Ressourcen zurückzugreifen. Er überprüft alle betriebssystemexternen Aufrufe, modifiziert sie gegebenenfalls oder weist sie zurück.

Vorteile:
- für unsicheres Betriebssystem nutzbar (unter der Einschränkung vorausgesetzten Wohlverhaltens des Betriebssystems)
- Betriebssystem vor Manipulationen geschützt

Nachteile:
- Performance: Leistungsfähigkeit des Gesamtsystems sinkt, Sicherheitsmanager ist „Flaschenhals“
- Hoher Implementierungsaufwand bei Sicherheitsmanager durch Anpassungsaufwand an Betriebssystem
- Abhängigkeit von Betriebssystemverhalten

Kritik:
- Idealzustand der vollständigen Schirmung vor unerwünschten Einflüssen / „Ausflüssen“ kaum erreichbar
- Das Abfangen aller Betriebssystemaufrufe behindert den Lauf von Applikationen innerhalb einer vernünftigen Zeitspanne, was die Verfügbarkeit aus Nutzersicht einschränkt

3.2.2 Variante mit sich selbst schützendem Betriebssystemkern

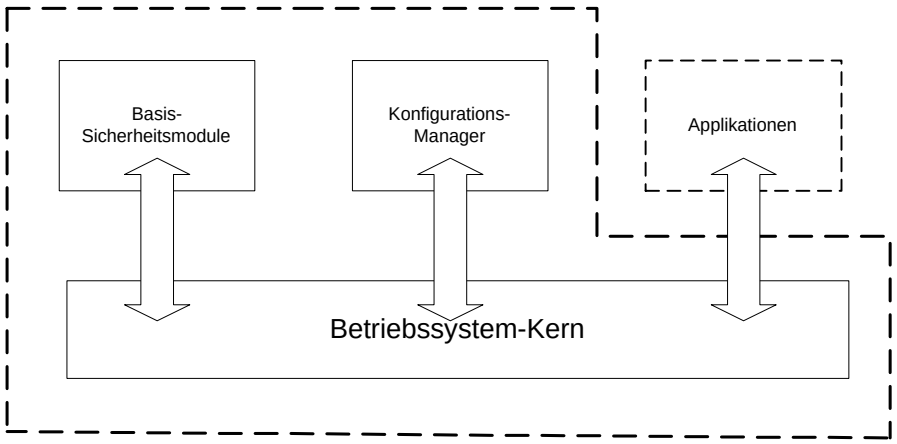


Abb. 3-2: sicherer Betriebssystemkern

Architektur:
Der Konfigurationsmanager ist wie die Basis-Sicherheitsmodule Komponente des Betriebssystems und tritt für Anwendungen nicht in Erscheinung. Es gibt eine begrenzte Anzahl von Schnittstellen zum Betriebssystemkern. Er ist der zentrale Teil der Sicherheitsarchitektur. Er ist in der Lage, sich selbst mit vorhandenen Mechanismen zu schützen. Es wird vorausgesetzt, daß ihm bezüglich Sicherheit zu trauen ist. Der Konfigurationsmanager kann auf alle (Schutz-)Mechanismen des Betriebssystems zugreifen und die Einbindung der Basis-Sicherheitsmodule regeln, jedoch weder auf diese noch auf Applikationen direkt einwirken (Brandmauerprinzip). Vgl. zu dieser Architektur [HäKK_92].

Die Betrachtung der begrenzten Anzahl der Schnittstellen zum Betriebssystemkern führt zu Überlegungen über einen minimalen Satz von Operatoren, die Zugriffe ermöglichen. Sie sind zu identifizieren und Schutzeigenschaften zuzuordnen. Für ihre Festlegung ist die Kenntnis des Betriebssystemkerns und seiner Sicherheitsmechanismen nötig. Dazu gehören beispielsweise auch solche Konzepte wie **Domain** (Menge von Objekt-Rechte-Paaren), **Access Control List** (ACL) und **Capability List** bzw. **Subject Restriction List** (SRL), vgl. [HäKK_92] und [Tane_95].

Ein konkreter Anwendungsfall besteht darin, daß mit einer ACL für eine Datei gewisse Zugriffsrechte vergeben werden. Zugriffe, die ein in die Architektur eingebettetes Workflow-Managementsystem vornimmt, werden vom Betriebssystemkern anhand dieser ACL geprüft.

Vorteile:
- Performance: Durch direktes Zusammenwirken von Anwendung und Betriebssystemkern entfällt der „Flaschenhals“ einer zwischengelagerten Schicht
- Komplexität: Gegenüber der Architektur unter 1.1 reduziert, da der Konfigurationsmanager keine Betriebssystemaufrufe filtern muß wie es der Sicherheitsmanager dort vornimmt

Nachteile:
- Vorausgesetztes Vertrauen in Betriebssystemkern auf Gutwilligkeit und Abwesenheit trojanischer Pferde
- Konfiguration muß mit evtl. nicht modifizierbarem Betriebssystemkern zurechtkommen, keine puffernde Schale vorhanden

Kritik:
- Kontrolle des Betriebssystems wünschenswert, um der „Übermacht“ des Betriebssystems aus Sicht des Anwenders zu begegnen (sonst droht „Ausgeliefertsein“)
- Voraussetzung, daß Betriebssystemkern ausreichend Sicherheitsmechanismen beinhaltet und diese auch einsetzt, ist nicht in jedem Fall erfüllt

3.2.3 Gegenüberstellung

Die Applikation richtet ihre Befehle immer an ein- und dieselbe Adresse, unabhängig davon, welche Architektur betrachtet wird.
Zwei verschiedene Ansätze für eine Sicherheitsarchitektur wurden bisher identifiziert (3.2.1 und 3.2.2):
- Der Sicherheitsmanager als zentraler Teil der Architektur nutzt ein unsicheres Betriebssystem und schirmt es ab.
- Der Betriebssystemkern ist der zentrale Teil der Architektur. Der Konfigurationsmanager ist selbst Komponente des Betriebssystems und tritt gegenüber der Anwendung nicht explizit in Erscheinung. Er kann alle Sicherheitsmechanismen des Betriebssystemkerns nutzen und setzt dabei deren Sicherheit voraus.

Die Architektur aus 3.2.1 wird (vorläufig) nicht betrachtet, da abzusehen ist, daß der erwartete Nutzen in einem ungünstigen Verhältnis zum eingesetzen Aufwand steht. Vielmehr wird der unter 3.2.2 vorgestellte Vorschlag zu einer verteilten Architektur erweitert.

3.2.4 Verteilte Architektur

Architektur:
In dieser herrscht bei jedem Teilnehmer lokal die gleiche Struktur, insbesondere sind Schnittstellen äquivalent. In diese Struktur können jedoch durchaus lokal verschiedene Betriebssystemkerne und Basis-Sicherheitsmodule eingebettet sein. Der Konfigurationsmanager dient zur Repräsentation der lokalen Sicherheitsinteressen und sollte für alle Nutzer die gleiche

Funktionalität zur Verfügung stellen. Die dafür notwendigen Sicherheitsmechanismen werden neben dem Betriebssystemkern vor allem durch lokale Basis-Sicherheitsmodule bereitgestellt.

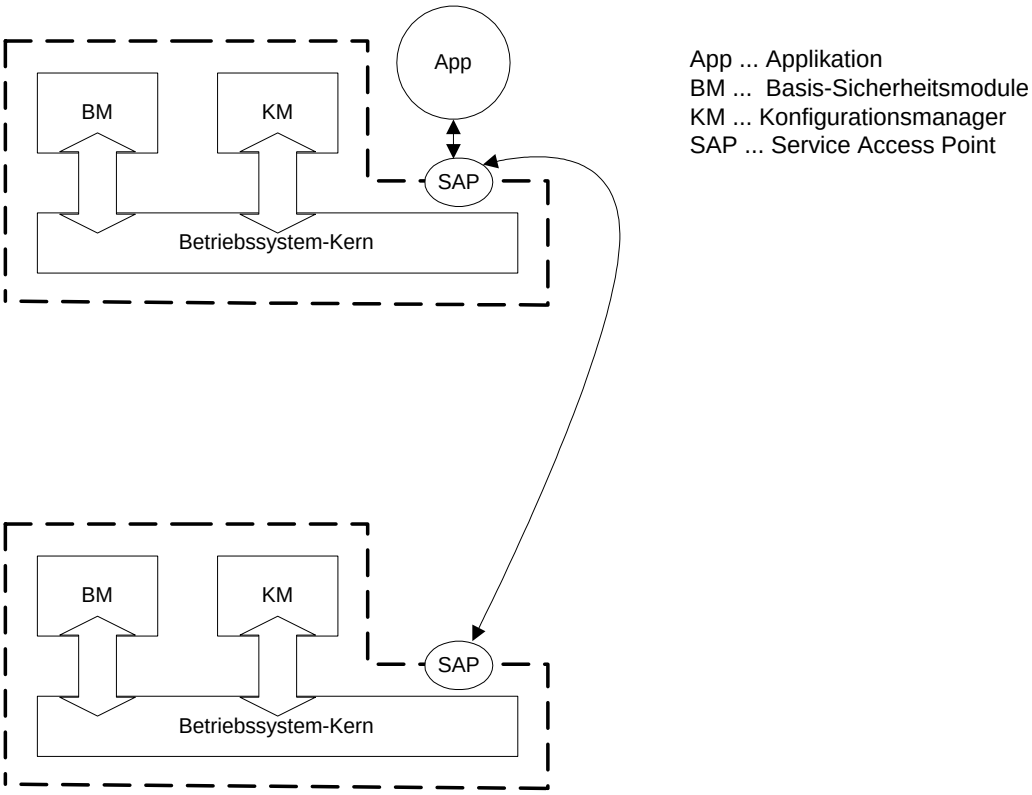


Abb. 3-3: verteilte Architektur

Außerdem gibt es im System verteilte Applikationen und Sicherheitsmodule, die nicht überall lokal vorhanden sind. Stellt der Betriebssystemkern fest, daß bei einem Aufruf durch eine Applikation lokal vorhandene Ressourcen nicht ausreichen, um eine spezielle Sicherheitsfunktionalität zu bieten, sollen entfernte Sicherheitsmodule genutzt werden können.

Am jeweiligen Service Access Point (SAP) greifen nicht nur lokale Applikationen zu, sondern auch entfernte. Für entfernte Applikationen ist keine weitere zu sichernde Schnittstelle nötig, sie lassen sich wie lokale behandeln. Voraussetzung ist die Verwendung interaktiver Protokolle, die eine Zugriffskontrolle ermöglichen und die Integrität sicherstellen.

Wichtig für die Konfigurierung von Diensten ist, daß die Schnittstellen, insbesondere die der Basis-Sicherheitsmodule, einheitlich sind.

Vorteile:
- die üblichen verteilter Systeme, insbesondere ökonomische Ressourcennutzung

Nachteile:
- Auftreten evtl. entgegengesetzter Interessen der Teilnehmer kann für die Verfügbarkeit von Ressourcen negative Folgen haben

Damit in der verteilten Architektur mehrseitige Sicherheit sinnvoll verwirklicht werden kann, müssen zwei Ebenen (entsprechend Gesamtsystem / Teilsystem) berücksichtigt werden:

- *Sicherheit auf lokaler Ebene:* Zu identifizieren ist die für jedes Teilsystem (bestehend aus den lokalen Komponenten) notwendige minimale Sicherheitsfunktionalität, die der Betriebssystemkern haben muß, damit Applikationen und damit dem Teilnehmer in einer bestimmten Rolle kein Schaden zugefügt werden kann (beispielsweise im Zahlungssystem die Verhinderung von Betrug durch Ausgeben „gestohlenener" Zahlungsmittel).
- *Sicherheit auf globaler Ebene:* Zu identifizieren ist die für das Gesamtsystem (bestehend aus den miteinander im offenen Netz verbundenen lokalen Teilsystemen) notwendige minimale Sicherheitsfunktionalität, die das lokale Teilsystem erbringen muß, damit das Gesamtsystem keinen Schaden erleidet und zielgerichtet funktioniert, d.h. der ausgehandelte „Vertrag" zwischen den Teilnehmern in ihren Rollen erfüllt werden kann (beispielsweise im Zahlungssystem die Ausführung eines Geldtransfers).

4 Ausblick

Bei der Gestaltung einer verteilten Sicherheitsarchitektur sind folgende Fragestellungen weiter zu vertiefen:

- Wie weit ist Vertrauen in andere Instanzen Voraussetzung für die Erreichung lokaler Sicherheit bzw. der Sicherheit des Gesamtsystems? Wie stark haben gegensätzliche Interessen der Teilnehmer Einfluß auf ihre jeweilige Sicherheit?
- Kann man die Betrachtung der Sicherheit im verteilten System (Bsp.: Problem entfernter Applikationen) auf die Betrachtung der Sicherheit eines Teilsystems reduzieren (lokale Applikationen)?
- Welches Verhältnis zwischen sicherheitsbezogenen Einschränkungen und Freiheiten herrscht für die lokalen Applikationen? Stellt der Konfigurationsmanager Gebote auf, an die sich die Applikation halten kann oder wird sie durch Verbote zu bestimmtem Verhalten gezwungen? Es entsteht für eine entfernte Station kein Schaden, wenn sie Aufrufe toleriert, die nur die Sicherheit der aufrufenden Applikation gefährden. Wo liegt jedoch die Grenze, ab der die Sicherheit entfernter Stationen bzw. die des Gesamtsystems leidet? Jede Applikation sollte zusätzliche, eigene Sicherheitsmechanismen nutzen können, solange sie nicht die durch das lokale System vorgeschriebene Sicherheit umgeht.
- Wie kann die Verfügbarkeit von Betriebsmitteln im verteilten System garantiert werden, ohne zu sehr in die Autonomie einzelner einzugreifen? Anders formuliert: Welche Funktionalität ist zwingend auf der lokalen Station notwendig, um die eigenen Sicherheitsinteressen wahren zu können, ohne auf die Kooperation anderer Instanzen angewiesen zu sein? Unter Betriebsmitteln können hier auch Daten verstanden werden, die von einem Teilnehmer verwaltet und von einem anderen benötigt werden. Es kann dabei notwendig werden, Regulativa einzusetzen, die außerhalb des eigentlichen IT-Systems liegen.

Die Schwierigkeit wird nicht die Einbettung und Anwendung kryptographischer Verfahren in die Architektur sein, denn diese sind verbreitet, relativ gut erforscht und anerkannt. Vielmehr ist ein Rahmenwerk für verschiedenste Architekturausprägungen abzustecken, die jeweils die Interessen aller Beteiligten unterstützen und Möglichkeiten zur Aushandlung von Sicherheitszielen bieten. Dies ist bei konventionellen Ansätzen, die auf einer zentralistischen Sicherheitsdefinition aufbauen, in keiner akzeptablen Weise realisiert.

Ein solches verteiltes System kann eine wie eben genannt zentrale oder eine dezentrale Struktur haben. Wie bereits bemerkt wurde, hat die dezentrale Definition von Sicherheitszielen für viele Anwender Vorteile bezüglich ihrer Sicherheit und Privatheit, wobei natürlich eine sichere Ende-zu-Ende-Kommunikation Voraussetzung zur Erreichung dieser Ziele ist. Auch steigert die notwendige Replikation von Sicherheitsfunktionalität die Ausfallsicherheit des Gesamtsystems.

Dennoch darf ein solches System nicht anarchistisch werden; es gibt bestimmte Gesamtinteressen (z.B. die der Firma bei Angestellten), die die Kooperation von vielen Instanzen notwendig machen. Der Widerstand Einzelner kann dann hinderlich für Viele werden. Hier erscheint eine zentrale Autorität als die einzig mögliche Lösung. Wie kann diese auf einem dezentralen System emuliert werden?

Als Analogie bietet sich hier die demokratische Gesellschaft an: Jeder, der ihr angehört, hat Rechte, aber auch Verpflichtungen, die er dadurch anerkennt, daß er Mitglied der Gemeinschaft ist. Wenn er diesen nicht nachkommt, gibt es Instanzen, durch die er zu Rechenschaft gezogen werden kann. Eine ähnliche Vorgehensweise erscheint auch in verteilten Systemen als praktikabel und gerecht.

5 Literatur

[Action_1] http://www.actiontech.com/products/

[BaFo_95] D. Bartmann, C. Fotschki:
„Elektronische Geldbörse - nützliche Innovation oder technischer Gag?“ in:
Die Bank (1995) 11, 644-649

[Baue_96] K. Bauer:
„Girokonto für alle? Schön wär's gewesen!“ in:
Datenschutz Nachrichten (DANA), 19 (1996) 1, 11

[BCMM_95] A. Bosselaers, R. Cramer, R. Michelsen u.a.:
„Deliverable Functionality of the Basic Protocols“
ESPRIT 7023 CAFE Document IHS8341, CAFE Public Report - Preprint 1995.

[BGHH_95] M. Bellare, J.A. Garay, R. Hauser u.a.:
„iKP - A Family of Secure Electronic Payment Protocols“
Mai 1995.
http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/

[BPAF_1] http://mephisto.inf.tu-dresden.de/RESEARCH/bpaframe/bpaframe_eng.html

[ChPe_93a] D. Chaum, T.P. Pedersen:
„Transferred Cash Grows in Size“ in:
R.A. Rueppel (Hrsg.): Advances in Cryptology - EUROCRYPT '92,
Lecture Notes of Computer Science (LNCS) 658, Berlin 1993, 390-407

[Cosa_1] http://www.cosa.de/

[Dier_94] M. Dier, S. Lautenbacher:
„Groupware-Technologien für die lernende Organisation: Rahmen - Konzepte, Fallstudien“
Computerwoche Verlag GmbH, 1994

[Ellis_91] C. A. Ellis, S. J. Gibbs, G. L. Rein:
„Groupware - Some issues and experiences“ in:
Communications of the ACM; Vol. 34, No. 1, 1991

[Gass_95] G. Gassauer:
„Traderinterworking am Beispiel des X*Traders“;
Großer Beleg, TU Dresden, 1995

[HäKK_92] H. Härtig, O. Kowalski, W. Kühnhauser:
„The BirliX Security Architecture“
Journal of Computer Security, 2(1). 5-21, 1993
http://os.inf.tu-dresden.de/~haertig/bsa.ps

[Ham_94] M. Hammer, J. Champy:
„Business Reengineering“;
Campus Verlag, 1994

[Hase_94] U. Hasenkamp, S. Kirn, M. Syring:
„CSCW - Computer Supported Cooperative Work“;
Addison Wesley, 1994

[Herd_95] S. Herda, S. Mund, A. Steinacker:
„Szenarien zur Sicherheit informationstechnischer Systeme“;
REMO-Arbeitsberichte, Oldenbourg, 1993

[Jabl_95] S. Jablonski:
„Workflow-Management-Systeme: Modellierung und Architektur“;
Thomson´s Aktuelle Tutorien, International Thomson Publishing, 1995

[JaWa_95] P. Janson, M. Waidner:
„Electronic Payment over Open Networks - A Technology Overview“
Aug. 1995. IBM Zurich Research Lab,
http://www.zurich.ibm.com/Technology/Security/publication/1995/JaWa.dir/JaWa95

[OMG_1] http://www.omg.org/

[OSF_1] http://www.osf.org/dce/

[Pern_1] http://132.252.52.7/ifs/forsch14.html

[PfWP_90] B. Pfitzmann, M. Waidner, A. Pfitzmann:
„Rechtssicherheit trotz Anonymität in offenen digitalen Systemen“ in:
Datenschutz und Datensicherung (DuD) (1990) 5, 243-253 und DuD (1990) 6, 305-315

[Rann_96] K. Rannenberg, A. Pfitzmann, G. Müller:
„Sicherheit, insbesondere mehrseitige Sicherheit“ in:
it+ti, Heft 4, 1996

[Stall_95] W. Stallings
Protect your Privacy - A guide for PGP users
Prentice Hall
Englewood Cliffs 1995

[Tane_95] A.S. Tanenbaum:
„Moderne Betriebssysteme“
2. Aufl. München 1995

[Tenh_96] B. Tenhagen:
„Feldversuch Marburg“ in:
Praxis Computer, Ausgabe 4/96, S. 4 ff
Deutscher Ärzte-Verlag GmbH, Köln, 1996

[Weic_96] T. Weichert:
„Die elektronische Geldbörse“ in:
Datenschutz Nachrichten (DANA), 19 (1996) 1, 8-10

[Wern_95] D. Werner (Hrsg.):
„Taschenbuch der Informatik“
2. Aufl., Leipzig 1995

[WfMC_94] Workflow Management Coalition:
„Glossary“;
WfMC, Document Number TC00-0011, 1994

[WfMC_95] Workflow Management Coalition:
„Overview: Introduction to the Workflow Management Coalition“;
WfMC, 1995

[Wiew_96] E. Wiewall:
„Secure Your Applications with the Microsoft CryptoAPI“ in:
Microsoft Developer Network News, 5 (1996) 3/4, 1

[WiMö_96] A. Wilfert, T. Mörsdorf:
„Elektronische Geldbörsen als Bargeldersatz“ (Teil 1) in:
Finanzierung Leasing Factoring (FLF), (1996) 1, 17-22

[Zila_95] M. G. Zilahi-Szabó (Hrsg.):
„Kleines Lexikon der Informatik und Wirtschaftsinformatik“
Oldenbourg, 1995