LEHRSTUHL FÜR
ALLG. BWL UND WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. HERBERT KARGL

Harper, David; Schwickert, Axel C.

Sicherheit von eBusiness-Anwendungen – Eine Fallstudie

ARBEITSPAPIERE WI
Nr. 10/1999

Schriftleitung:
Dr. rer. pol. Axel C. Schwickert

Information

Reihe: Arbeitspapiere WI

Herausgeber: Univ.-Prof. Dr. Axel C. Schwickert
Professur für BWL und Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Bis Ende des Jahres 2000 lag die Herausgeberschaft bei:

Lehrstuhl für Allg. BWL und Wirtschaftsinformatik
Johannes Gutenberg-Universität Mainz
Fachbereich Rechts- und Wirtschaftswissenschaften
Welderweg 9
D - 55099 Mainz

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IuK-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstanden aus Forschungsarbeiten, Diplom-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen des Lehrstuhls für Allg. Betriebswirtschaftslehre und Wirtschaftsinformatik Univ. Prof. Dr. Herbert Kargl an der Johannes Gutenberg-Universität Mainz.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.
Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber (Gießen) unter obiger Adresse Kontakt auf.
Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe und deren Bezug erhalten Sie auf dem Schlußblatt eines jeden Arbeitspapiers und auf der Web Site des Lehrstuhls unter der Adresse http://wi.uni-giessen.de

Alle Arbeitspapiere der Reihe „Arbeitspapiere WI“ sind einschließlich aller Abbildungen urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Herausgebers unzulässig. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung, Be- und Verarbeitung in elektronischen Systemen. Layout by ACS Publications Copyright 1996 - 2001

Arbeitspapiere WI Nr. 10/1999

Autoren: Harper, David; Schwickert Axel C.

Titel: Sicherheit von eBusiness-Anwendungen – Eine Fallstudie

Zitation: Harper, David; Schwickert, Axel C.: Sicherheit von eBusiness-Anwendungen – Eine Fallstudie, in: Arbeitspapiere WI, Nr. 10/1999, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1999.

Kurzfassung: Kunden, die online Bestellungen aufgeben, Bankgeschäfte tätigen oder Verträge unterzeichnen, setzen ein vertrauenswürdiges Medium voraus. Das in vielerlei Hinsicht auf völlige Offenheit ausgelegte Internet vermag dies ohne spezielle Sicherheitsmaßnahmen nicht zu leisten. Die Sicherheitsproblematik des Internet betrifft die folgenden drei Bereiche: Schutz und Sicherheit technischer Systeme (z. B. Hard-/Software von Web Sites), vertrauenswürdige Verfahren zur Abwicklung von elektronischen Geschäftsaktivitäten sowie Schutz und Sicherheit nicht-öffentlicher Daten. Das vorliegende Arbeitspapier legt seinen Schwerpunkt auf die Analyse der Sicherheitsproblematik bzgl. der Verfahren und Daten. Ziel ist es, Sicherheitssysteme zu erörtern, die Verfahren zum sicheren Transport vertraulicher Daten über das unsichere Medium Internet realisieren. Die Wissenschaft der Kryptographie bietet hierfür ein praktikables Instrumentarium an. Im Zentrum der Ausführungen stehen somit die verfügbaren technischen Kryptographie-Verfahren, die zum Verständnis erforderliche kryptographische Theorie, die relevanten Standards und technischen Verfahren. Reales Bezugsobjekt für die Ausführungen ist dabei das Kundenkonteninformationssystem (KKIS) der Bausparkasse Mainz AG (BKM). Die BKM prüft derzeit, inwiefern es ihren Kunden ermöglicht werden kann, über die BKM-Web-Site auf vertrauliche, personenbezogene Daten des KKIS wie z. B. Kontostände zuzugreifen.

Schlüsselwörter: Sicherheit, Web Site Security, Electronic Business, Kryptographie, Verschlüsselung, S-HTTP, SSL, HBCI

Inhaltsverzeichnis

1 Problemstellung, Ziel und Aufbau

Im Rahmen des immer weiter verbreiteten Einsatzes von Web Sites zum eBusiness und der stetig steigenden Bedeutung von kommerziellen Transaktionen im globalen Internet kommt der Sicherheit von Daten und Transaktionen sowie der dazu eingesetzten Verfahren eine entscheidende Bedeutung zu.[1] Die Sicherheitsrisiken der ausschließlichen Online-Präsentation eines Produkt-/Leistungsangebotes sind relativ begrenzt. Die Web Site eines Unternehmens übernimmt hier die Aufgabe, den traditionellen gedruckten Leistungskatalog in digitaler Form öffentlich zur Verfügung zu stellen. Obwohl sensible Firmendaten hierbei unzugänglich bleiben, kann durch eine unbefugte Manipulation einer Web Site,[2] Schaden verursacht werden. Ein daraus resultierender Image-Verlust, kann beträchtlich sein.

Will ein Unternehmen mehr als einen Online-Katalog zu Informationszwecken anbieten, steigen die Sicherheitsrisiken durch die notwendige Öffnung der Web Site zum Internet. Dies gilt für alle Formen des eBusiness. Ob Online-Shopping in der virtuellen Mall mit Kreditkartenzahlung, Online-Buchung der Privat- oder Geschäftsreise, Online-Banking und -Aktienhandel, allen gemeinsam ist die Verquickung öffentlicher Internet-Anwendungen mit internen Firmendaten. Je mehr sich ein Unternehmen dem Internet öffnet, desto größer wird das Risiko und der mögliche Schaden.[3]

Kunden, die online Bestellungen aufgeben, Bankgeschäfte tätigen oder Verträge unterzeichnen, setzen ein vertrauenswürdiges Medium voraus. Das in vielerlei Hinsicht auf völlige Offenheit ausgelegte Internet vermag dies ohne spezielle Sicherheitsmaßnahmen nicht zu leisten. Für den Verbraucher korreliert Vertrauen eng mit Sicherheit. Folglich scheint die Sicherheitsproblematik einer der wichtigsten Hürden zu sein, die es auf dem Weg zur kommerziellen Erschießung des Internet zu überwinden gilt.

Die Sicherheitsproblematik des Internet betrifft die folgenden drei Bereiche:

- Schutz und Sicherheit technischer Systeme (z. B. Hard-/Software von Web Sites),
- Sichere, vertrauenswürdige Verfahren zur Abwicklung von elektronischen Geschäftsaktivitäten,
- Schutz und Sicherheit nicht-öffentlicher Daten.

Die vorliegende Arbeit legt ihren Schwerpunkt hierbei auf Analyse der Sicherheitsproblematik bzgl. der Verfahren und Daten. Ziel ist es, Sicherheitssysteme zu erörtern, die Verfahren zum sicheren Transport vertraulicher Daten über das unsichere Medium Internet realisieren.[4] Die Wissenschaft der Kryptographie bietet hierfür ein praktikables Instrumentarium an.

---

1 Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, Berlin et al.: Springer 1998, S. 1.

2 Vgl. o. V.: Homepage 2600, Online im Internet: http://www.2600.com/hacked_pages, 21.05.1999, und vgl. Luckhardt, Norbert: Weitere Web-Hacks in Deutschland, Online im Internet: http://www.heise.de/newsticker/data/nl-08.10.98-000/, 08.10.1998.

3 Vgl. Gehlen, Susanne; Nobis, Thomas: Web der offenen Tür, Die größten Sicherheitslöcher im Internet, in: Computerwoche Spezial, 4/1998, S. 12-13.

4 Vgl. Weck, Gerhard: Key Recovery - Möglichkeiten und Risiken, in: Informatik-Spektrum, 21/1998, S. 147-158.

Im Zentrum der nachfolgenden Ausführungen stehen somit die verfügbaren technischen Kryptographie-Verfahren, die relevanten Standards und die zum Verständnis erforderliche kryptographische Theorie. Reales Bezugsobjekt für die Ausführungen ist dabei das Kundenkonteninformationssystem (KKIS) der Bausparkasse Mainz AG (BKM). Die BKM prüft derzeit, inwiefern es ihren Kunden ermöglicht werden kann, über die BKM-Web-Site auf vertrauliche, personenbezogene Daten des KKIS wie z. B. Kontostände zuzugreifen.

In Kapitel 2 wird zunächst das Unternehmen Bausparkasse Mainz AG mit den involvierten Unternehmensbereichen, der „neuen Kernanwendung“ sowie dem projektierten Kundenkonteninformationssystem vorgestellt. Kapitel 3 schildert die kryptographischen Grundlagen, soweit diese zur Überwindung der Sicherheitsproblematik von Bedeutung sind.

Im bezogenen Business-to-Consumer-Bereich der BKM stellen die beteiligten Akteure unterschiedliche Anforderungen an ein Sicherheitssystem. Kapitel 4 arbeitet die unterschiedlichen Anforderungen und Ziele heraus. In Kapitel 5 werden die relevanten Standards und technischen Verfahren skizziert und anhand der in Kapitel 6 ermittelten Anforderungen bewertet.

Kapitel 7 skizziert, wie adäquate Sicherheitsmaßnahmen in das Kundenkonteninformationssystem der BKM integriert werden können. Ein Fazit und ein Ausblick auf Tendenzen im Bereich der Internet-Kryptographie schließen die Arbeit ab.

2 Die Bausparkasse Mainz AG

2.1 Allgemeine Informationen

Die Bausparkasse Mainz AG ist ein in der gesamten Bundesrepublik tätiger Anbieter des Bauspar- und Finanzierungsgeschäftes mit einer Bilanzsumme in 1998 von 3,8 Mrd. DM[5]. 1998 wurden insgesamt 42.066 neue Verträge mit der BKM geschlossen, die eine Bausparsumme von 1,810 Mrd. DM einlösten. Insgesamt betrug der Bestand an Verträgen zum Jahreswechsel 345.344 Stück mit einer Bausparsumme von 13,265 Mrd. DM. Die BKM liegt damit deutlich über dem Durchschnitt der Privaten Bausparkassen.[6] Sitz des Unternehmens ist seit 1930 Mainz am Rhein.

Bausparkassen sind zweckorientierte Spezialkreditinstitute, „die nur Darlehens- und Kreditgeschäfte betreiben dürfen, die der Vor- und Zwischenfinanzierung von Bauvorhaben u. a. wohnungswirtschaftlichen Zwecken dienen“.[7] Als Hauptaufgabe der Bausparkassen gilt die Finanzierung von privatem Wohnraum durch spezielle Finanzierungsformen, die im Vergleich zum Marktzins günstigere und weniger volatile Zinskonditionen bieten.[8]

5 Vgl. Bausparkasse Mainz AG (Hrsg.): Bericht über das Geschäftsjahr 1998, Mainz 1999, S. 26.

6 Vgl. Bausparkasse Mainz AG (Hrsg.): Bericht über das Geschäftsjahr 1998, a. a. O., S. 21.

7 Vgl. Woll, A.: Wirtschaftslexikon, 7., überarbeitete Aufl., München et al..: Oldenbourg 1993, S. 67.

8 Vgl. o. V.: Bankbetriebslehre, Bank-Enzyklopädie Bd. 2, Wiesbaden Dr. Gabler-Verlag 1975, S. 504.

Die Bausparkasse Mainz ist Spezialistin in allen Fragen rund um das bessere Wohnen. Zu dem Produktangebot gehören innovative Bauspar- und Finanzierungsangebote, das Hausprogramm „Mainzer Haus“ sowie eine bundesweite Immobilienvermittlung. Die Produkte werden durch zwei eigene Vertriebsschienen und durch den Versicherungsaußendienst des Mehrheitsanteileigners „INTER-Versicherungen“, Mannheim vertrieben.[9]

2.2 JoKer und KKIS

Zentraler Fokus der Hauptabteilung Organisation und Informatik ist zur Zeit das neue **J**ava basierte, **o**bjektorientierte **Ker**nsystem (**JoKer)**. Ziel ist es, die operativen DV-Systeme und Anwendungen auf eine neue technische Basis zu überführen, die zukunftsorientiert ist und die Gewähr dafür bietet, daß die Investitionen in die neuen Anwendungen mindestens für die nächsten 10 Jahre geschützt sind. Die komplette Ablösung des bisherigen Mainframesystems geht damit einher. Diese Ziele können nur mit modernen, innovativen Technologien verwirklicht werden. Daher soll die Entwicklung der neuen Anwendung objektorientiert erfolgen und die Grundprinzipien einer modernen Softwarearchitektur berücksichtigen.

Die organisatorischen Zielsetzungen sind mit der Erneuerung der DV-Landschaft eng verzahnt. So soll die Ablauf- und Aufbauorganisation des Hauses ebenfalls komplett neu gestaltet werden. Verbesserung der Servicequalität und Ausschöpfung von Rationalisierungspotential stehen hierbei im Vordergrund. Die neuen Qualitätsstandards, die im System verankert werden, sollen den Kundenservice der BKM nachhaltig verbessern.[10]

Rationalisierungen als Mittel zur Kostensenkung sind auf ein bestimmtes Rationalisierungspotential und damit auf eine bestimmte Wettbewerbswirkung begrenzt. Zur Steigerung ihrer Wettbewerbsfähigkeit heben sich die erfolgreichen Unternehmen der Zukunft daher durch ihre Kommunikation mit Kunden und Lieferanten von ihren Konkurrenten ab.[11] Aus dieser Sicht eines verbesserten Kundenservices und der damit verbundenen Schaffung eines Mehrwertes durch Kundenzufriedenheit sowie der möglichen Einsparungspotentiale beim Telefon- bzw. Brief-basierten Kundenservice plant die BKM die Bereitstellung von Internet-Services für ihre Kunden. Funktionalitäten wie die Abfrage des Kontostandes etc. sind bereits bei ähnlichen Institutionen[12] im Einsatz, so daß auch aus marktpolitischen Gründen ein Handlungsbedarf erkennbar ist.

Ein Ziel des geplanten Kundenkonteninformationssystems (KKIS) ist es, Kunden der BKM den Zugriff auf bestimmte Informationen via Internet zu ermöglichen. Zum Informationsangebot via Internet sollen u. a. gehören:

9 Vgl. Bausparkasse Mainz AG (Hrsg.): Die Bausparkasse Mainz AG, Online im Internet: http://www.bkm-dv.de/Framesets/230.htm, 12.06.1999.

10 Vgl. Bausparkasse Mainz AG (Hrsg.): Das Projekt, Online im Internet: http://www.bkm-dv.de/Framesets/229.htm, 12.06.1999.

11 Vgl. o. V.: Kommunikation im Internet bestimmt Erfolg, in: Frankfurter Allgemeine Zeitung, 05.03.1998, S. 27.

12 Vgl. IDUNA Bausparkasse AG (Hrsg.): IDUNA Bausparkasse interaktiv, Online im Internet: http://www.iduna-bausparkasse.de/service/index.html, 03.08.1999.

- allgemeine Marketinginformationen,
- neue Angebote der BKM,
- Daten zum Vertragsverhältnis zwischen der BKM und dem Kunden,
- Abfrage persönlicher Kontostände.

Das bedeutet, daß auch hochsensible, personenbezogene Daten übermittelt werden und folglich an die betroffenen Verfahren besonders hohe Sicherheitsanforderungen zu stellen sind. Die kunden- bzw. vertragsspezifischen Daten befinden sich derzeit in Datenbanken, die auf BS2000-Hosts verwaltet werden. Im Rahmen des JoKer-Projektes wird die Migration zu einer Client/Server-basierten IT-Landschaft betrieben, wobei auf IBM AIX als Server-Plattform gesetzt wird. Das KKIS soll sowohl die Services der neuen Kernanwendung „JoKer“ als auch die Services der Mainframe-Anwendungen nutzen können. Ein wesentliches Ziel des KKIS-Projektes ist es, die höchstmögliche Akzeptanz auf Seiten der BKM-Kunden zu erzielen.

Zur Beobachtung der Akzeptanz der angebotenen Online-Dienste durch die BKM-Kunden ist es sinnvoll, statistische Auswertungen der Frequenz und Art von Benutzeraktionen zur Verfügung zu stellen und so aufzubereiten, daß diese Informationen von autorisierten BKM-Mitarbeitern über das Intranet abgerufen werden können. Zu beachten ist dabei, daß keine personenbezogenen Daten (wie persönliche Kontostände) für Dritte einsehbar protokolliert werden.

2.2 eBusiness der BKM

Aufgeräumt, übersichtlich und sachlich präsentiert sich die derzeitige Startseite der BKM-Web Site (siehe Abb. 1). Der anklickbare Newsticker sowie Rollover-Buttons links und rechts vom Bild der Firmenzentrale sorgen für Abwechslung. Die dargestellten Hauptbereiche

- Firmenportrait,
- Presse,
- Karriere,
- Leistungen,
- Aktuelles und
- Kundenservice

finden sich später in der Menüleiste wieder, die jeweils links in einem Frame angeordnet ist (siehe Abb. 2).

Abb. 1: Homepage der BKM

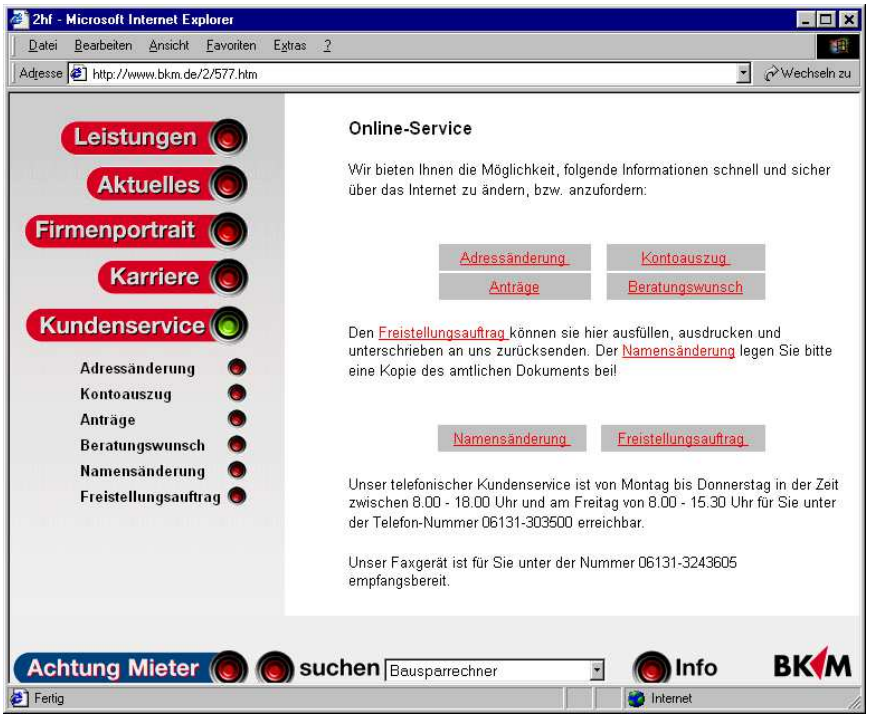

Abb. 2: Serviceseiten der BKM

Die Hauptbereiche sind alle identisch aufgebaut, so daß die Benutzerführung intuitiv zu erfassen ist. Am unteren Bildschirmrand ist auf allen Seiten ein weiterer Frame positioniert in dem sich ein Link zur Infoseite, ein Drop-down-Menue zu ausgewählten Inhalten der Web Site sowie eine Suchfunktion befinden.

Im ganzen merkt man der BKM-Web Site jedoch insbesondere bei den grafischen Elementen an, daß sie nahezu unverändert seit über 2 Jahren online ist. Ganz besonders deutlich wird dies beim Betrachten von Web-Auftritten branchengleicher Unternehmen. Im Hauptbereich Kundenservice (siehe Abb. 2) bietet die BKM-Web Site dem Benutzer die Möglichkeit, z. B. Adress- und Namensänderungen in einem Formular einzugeben und per Mail zu verschicken (siehe Abb. 3). Diese Mail wird von einem Servicemitarbeiter der BKM entgegengenommen; nach einer Plausibilitätsprüfung werden die neuen Daten per Hand in den Datenbestand übernommen. Darüber hinaus gibt es nichts Interaktives, das als „Kunden-Service“ bezeichnet werden könnte.

Abb. 3: Adressänderungsformular[13]

Ziel des KKIS-basierten eBusiness der BKM ist es, eine Anbindung der BKM-internen (JoKer)-Anwendungen mit dem Service-Bereich der BKM-Web Site zu realisieren. Die o. g. Adreßänderung führt der Kunde bspw. dann über ein Web-Formular und dessen Anbindung an den BKM-internen Datenbestand aus, ohne daß ein BKM-Mitarbeiter in diesen Änderungsvorgang involviert ist. Der Informationsfluß vom Kunden zur BKM und umgekehrt soll ohne Medienbruch erfolgen. Nicht nur der Informationsfluß vom Kunden zur BKM, sondern auch aus dem Datenbestand zum Kunden soll ermöglicht werden. Beispiele für Informationen, die via Web Site direkt zum Kunden gelangen können, sind Kontobewegungen und persönliche Kontostände.

13 Vgl. Bausparkasse Mainz AG (Hrsg.): Adressänderung, Online im Internet: http://www.bkm.de/2/998.htm, 12.06.1999.

3 Kryptographie in der Theorie

3.1 Terminologie

Die Kryptographie zählt zu den grundlegenden Verfahren in vielen Sicherheitstechnologien. Allgemein wird darunter die Ver- und Entschlüsselung von Daten verstanden. Es werden vertrauliche Informationen (Klartext) unter Bemühung der Erkenntnisse moderner Mathematik und mit Computerunterstützung auf komplexe, genau definierte Weise so transformiert, daß sie anschließend in einer unkenntlichen Form vorliegen (Chiffretext).[14] In eine Verschlüsselung geht stets ein Paßwort (Schlüssel) mit ein, ohne das eine Entschlüsselung nicht möglich ist. Während der Schlüssel nur denjenigen bekannt sein darf, die die Befugnis zur Dechiffrierung haben, ist eine Geheimhaltung des Verschlüsselungsverfahrens an sich bei einer solchen Praxis nicht notwendig.[15]

Die Begriffe *chiffrieren* und *verschlüsseln* sowie *dechiffrieren* und *entschlüsseln* werden gleichbedeutend verwendet. Ansätze, die chiffrierte Information ohne Kenntnis des geheimen Schlüssels wieder in Klartext zu wandeln, nennt man Kryptoanalyse.[16] Kryptographie und -analyse werden unter dem Oberbegriff Kryptologie zusammengefaßt.

Neben der *Vertraulichkeit*, dem Schutz vor unberechtigten Einblicken Dritter, soll die Kryptographie auch die *Integrität*, die Sicherung gegen beabsichtigte oder zufällige Manipulationen, die *Authentizität*, die zweifelsfreie Identifizierung des Absenders, und die *Verbindlichkeit*, die Nichtabstreitbarkeit oder Rechtsverbindlichkeit einer Nachricht, sicherstellen. Nachfolgend werden diese Anforderungen näher betrachte.

3.2 Vertraulichkeit der Daten

3.2.1 Symmetrische Verschlüsselung

Symmetrische Verschlüsselung bedeutet die Anwendung einer bestimmten Verschlüsselungsfunktion sowohl auf den Klartext als auch auf den Chiffretext. Sender und Empfänger verwenden also zur Ver- und Entschlüsselung den gleichen Schlüssel. Wenn der Schlüssel zur Verschlüsselung bekannt ist, ist damit auch der Schlüssel zur Entschlüsselung bekannt. Wenn Sender und Empfänger zwar über unterschiedliche Schlüssel verfügen, diese aber in einer einfachen funktionalen Beziehung zueinander stehen, spricht man ebenfalls von einer symmetrischen Verschlüsselung.[17] Einfache Verfahren für symmetrische Verschlüsselung sind u. a.:

14 Vgl. Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, Heidelberg: dpunkt-Verlag 1998, S. 12.

15 Ein Grundsatz der auf Kerckhoffs von Nieuwenhof zurückgeht. Vgl. dazu Kerckhoffs, A.: La Cryptographie Militaire. Librairie Militaire de L. Baudon & Cie. 1883.

16 Vgl. Oppliger, Rolf: IT-Sicherheit: Grundlagen und Umsetzung in der Praxis, Braunschweig, Wiesbaden: Verlag Vieweg 1997, S. 52 f.

17 Vgl. Oppliger, Rolf: IT-Sicherheit: Grundlagen und Umsetzung in der Praxis, a. a. O., S. 70.

- die logische Bitnegation,
- die XOR-Verknüpfung von Text und Schlüssel, wobei der Schlüssel länger als der Text sein muß,
- die Rotation im Alphabet um z. B. 3 Buchstaben (monoalphabetische Substitutionsmethode).[18]

Komplexere und aktuelle Verfahren zur symmetrischen Verschlüsselung sind z. B.:

- DES[19] (Data Encryption Standard) mit 56-Bit-Schlüsseln,
- Triple-DES (dreifache, kaskadische Anwendung von DES) mit effektiver Schlüssellänge von 112 Bit,[20]
- Rivest Cipher Nr. 4 (RC4) mit bis zu 128-Bit-Schlüsseln,
- Rivest Cipher Nr. 5 (RC5) mit variabler Schlüssellänge bis zu maximal 2048 Bit,
- IDEA[21] (International Data Encryption Algorithm) mit 128-Bit-Schlüsseln.

Bei den guten Verfahren zur symmetrischen Verschlüsselung ist nach heutigem Wissensstand der Versuch, einen Schlüssel zu knacken, nur durch Brute-Force-Angriff möglich. Dabei werden alle möglichen Schlüssel solange durchprobiert, bis ein Wort, von dem man weiß, daß es im Originaltext enthalten sein muß, entschlüsselt werden kann. Um z. B. einen 56-Bit-Schlüssel zu knacken, benötigt man im Durchschnitt 2^{55} ($2^{56}/2$) Versuche.

Anwendungen, die die Verschlüsselungsverfahren DES, RC4 und RC5 nutzen, kommen vorwiegend – wie viele andere auch – aus den USA und unterliegen einer strengen Exportbeschränkung, nach der sie nur für geheime Schlüssel(teile) von maximal 40 Bit Länge ausgeführt werden dürfen. Für alle diese guten Verfahren gilt, daß

- sie bei gleicher Schlüssellänge in etwa gleich sicher und gleich schnell sind,
- höhere Sicherheit nur durch größere Schlüssellängen (aktuell 128 Bit) erreicht werden kann.

In diesem Kontext ist die maximale Dauer eines Brut-Force-Angriffs von Interesse (siehe Tab. 1). Diese Werte der Tabelle 1 sind jedoch nur als Orientierungshilfe zu sehen, da die Dauer von der eingesetzten Rechenleistung und diese wiederum von dem zur Verfügung stehenden finanziellen Mitteln abhängig ist. Erfahrungsgemäß verdoppelt sich die Anzahl der Transistoren und somit die Rechenleistung eines Chip etwa alle 18 Monate. Im Laufe der Zeit sinkt somit die Dauer eines Brut-Force-Angriffs in Relation zu den Kosten rapide.

18 Auch als Ceasar Cipher, nach Gaius Julius Cäsar (100 - 44 v.Chr.), bekannt.

19 Amerikanischer Verschlüsselungsstandard, der seit 1976 als Regierungsstandard für nichtklassifizierte Kommunikation dient und ursprünglich von IBM entwickelt wurde. Wird auch im Finanzdienstleistungsbereich beim Verschlüsseln der Daten auf der EC-Karte verwendet.

20 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, 1., korrigierter Nachdruck, Bonn et al.: Addison-Wesley 1996, S. 413.

21 IDEA wurde an der Eidgenössischen Technischen Hochschule (ETH) Zürich in Zusammenarbeit mit der Ascom Tech AG entwickelt.

Alle symmetrischen Verschlüsselungsverfahren sind schnell, vergrößern nicht das Datenvolumen und lassen sich durch mehrfache Iteration mit sogenannten Subschlüsseln (z. B. Triple-DES) skalieren.

Schlüssellänge	Verschlüsselungsverfahren	
	DES	RC4
40 Bit	0,2 Sekunden	7,5 Tage
56 Bit	3,5 Stunden	1.350 Jahre
64 Bit	37 Tage	350.000 Jahre
128 Bit	7000 Jahre	>1024 Jahre

Tab. 1: Mittlere Zeitschätzung für einen Brut-Force-Angriff[22]

Bei symmetrischen Verschlüsselungsverfahren muß zwischen jeweils zwei Kommunikationspartnern ein eigener Schlüssel vereinbart werden, so daß für 1.000 Teilnehmer rund 500.000 (1000 * 1000 / 2) Schlüssel erforderlich sind. Jeder dieser Schlüssel muß zwischen den Kommunikationspartnern auf sicherem Wege ausgetauscht werden. Zum einen ist dies aufwendig, zum anderen stellt der sichere Transport der Schlüssel ein schwieriges Problem dar. Die Vielzahl benötigter Schlüssel und der erforderliche Austausch von Schlüsseln sind die wesentlichen Nachteile symmetrischer Verschlüsselungsverfahren.

3.2.2 Asymmetrische Verschlüsselung

Eine Lösung für die vorgenannten Probleme bietet die asymmetrische Verschlüsselung, die auch als Public-Key-Verfahren bezeichnet wird. Bei den Public-Key-Verfahren wird der geheime Schlüsselaustausch durch einen Mechanismus ersetzt, der keinerlei Geheimhaltung erfordert.

Asymmetrische Verschlüsselung bedeutet die Anwendung einer komplexen Verschlüsselungsfunktion auf den Klartext und einer von der Verschlüsselungsfunktion abweichenden, komplexen Entschlüsselungsfunktion auf den Chiffretext. Public-Key-Verfahren kombinieren zwei komplementäre, mathematisch miteinander in Bezug stehende Schlüssel, den öffentlichen und den privaten Schlüssel, zu einem Schlüsselpaar.[23] Jeder Teilnehmer einer asymmetrisch gesicherten Kommunikation benötigt ein solches Schlüsselpaar.

Der Sender verschlüsselt eine Nachricht mit dem öffentlichen Schlüssel (engl. public key) des Empfängers (siehe Abb. 4). Öffentliche Schlüssel werden zentral verteilt und verwaltet und sind wie Telefonnummern in einem Telefonbuch allgemein zugänglich.

22 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, a. a. O., S. 178 und vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 54 f. und vgl. Stark, T.: Encryption for a small Planet, in: Byte, April/97.

23 Vgl. Smith, Richard E.: Internet-Kryptographie, Bonn: Addison-Wesley-Longman 1998, S. 211 ff.

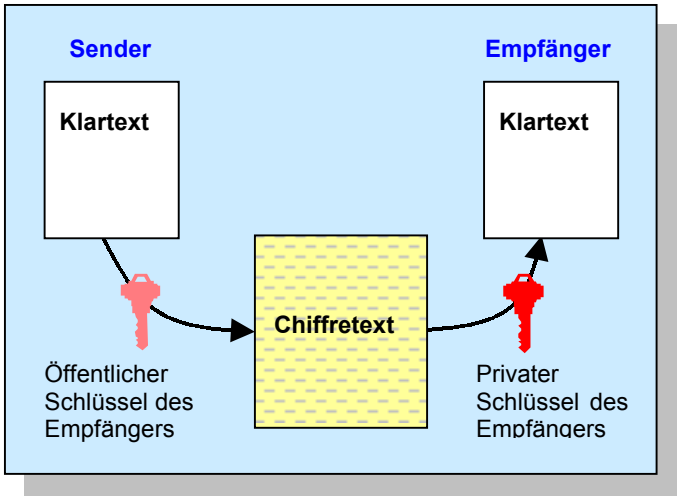

Abb. 4: Public-Key-Verfahren

Der Empfänger entschlüsselt diese Nachricht mit seinem privaten Schlüssel (engl. private key). Ein privater Schlüssel ist im Idealfall auf einer Chipkarte, im Normalfall auf der Festplatte abgelegt und durch ein Paßwort, die *Passphrase* geschützt.[24] Die Schlüssel sind so gewählt, daß eine mit dem öffentlichen Schlüssel chiffrierte Nachricht nur mit dem passenden privaten Schlüssel dechiffriert werden kann et vice versa. Allerdings ist es dadurch für den Sender nicht möglich, eine einmal mit dem public key des Empfängers verschlüsselte Nachricht wieder zu dechiffrieren.

Zu den bekanntesten Vertretern asymmetrischer Verschlüsselungsverfahren gehört der Quasi-Standard RSA (Rivest, Shamir, Adleman) mit variabler Schlüssellänge bis zu derzeit maximal 4096 Bit.[25] RSA spielt unter den asymmetrischen Verschlüsselungsverfahren eine dominierende Rolle, ähnlich wie DES unter den symmetrischen. Für RSA und alle Programme, die RSA nutzen, gilt die Exportbeschränkung der USA auf Schlüssel von maximal 512 Bit Länge. 512-Bit-Schlüssel sollten heute bereits nicht mehr verwendet werden, da schon 768-Bit-Schlüssel nur noch bis ins Jahr 2004 als sicher gelten.[26] Für die nächsten zehn Jahre werden Schlüssel von 1024 Bit Länge als hinreichend sicher erachtet und 2048-Bit-Schlüssel nur für sehr hohe Sicherheitsanforderungen empfohlen.

Asymmetrische Verschlüsselungsverfahren sind langsamer als symmetrische, weil sie komplexe mathematische Funktionen aus der Zahlentheorie ausführen (RSA braucht z. B. 1000-mal so lange wie DES)[27]. Außerdem können asymmetrische Verschlüsselungen das Datenvolumen von Nachrichten vergrößern. Asymmetrische Verschlüsselungsverfahren vermeiden jedoch den Austausch von Schlüsseln und benötigen deshalb pro Teilnehmer nur genau 1 Schlüsselpaar (1.000 Schlüsselpaare für 1.000 Teilnehmer).

24 Vgl. Luckhardt, Norbert: Qnf jne rvasnpu, tryy?, Kryptologische Begriffe und Verfahren, in: c´t Magazin für Computertechnik, 12/96 S. 110.

25 Die bekannteste RSA-Implementierung ist PGP (Pretty Good Privacy) zur Ver- und Entschlüsselung von eMails.

26 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, a. a. O. , S. 185-193.

27 Vgl. Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O., S. 96

3.2.3 Hybride Verschlüsselungsverfahren

In der Praxis stellen Public-Key-Verfahren keinen Ersatz für symmetrische Verschlüsselungsverfahren dar. Sie werden aufgrund der Tatsache, daß sie das Nachrichtenvolumen vergrößern und mehr Rechenleistung benötigen als symmetrische Verschlüsselungsverfahren fast nie zum Verschlüsseln von Nachrichten verwendet. Statt dessen wird per Public-Key-Verfahren ein sogenannter Sitzungsschlüssel (engl. session key) versendet, um damit den Rest der Nachrichtenübermittlung symmetrisch zu verschlüsseln.[28] Diese Kombination der beiden Verfahren bezeichnet man als hybrides Verschlüsselungsverfahren (siehe Abb. 5).

Der symmetrische Sitzungsschlüssel, der meist nur für die aktuelle Kommunikationsbeziehung (Sitzung) oder für einen bestimmten Zeitraum Gültigkeit hat, wird vom Sender nach dem Zufallsprinzip erzeugt.[29] Dieser Sitzungsschlüssel wird nun mit dem public key des Empfängers verschlüsselt, nachdem zuvor mit ihm der Klartext chiffriert wurde.

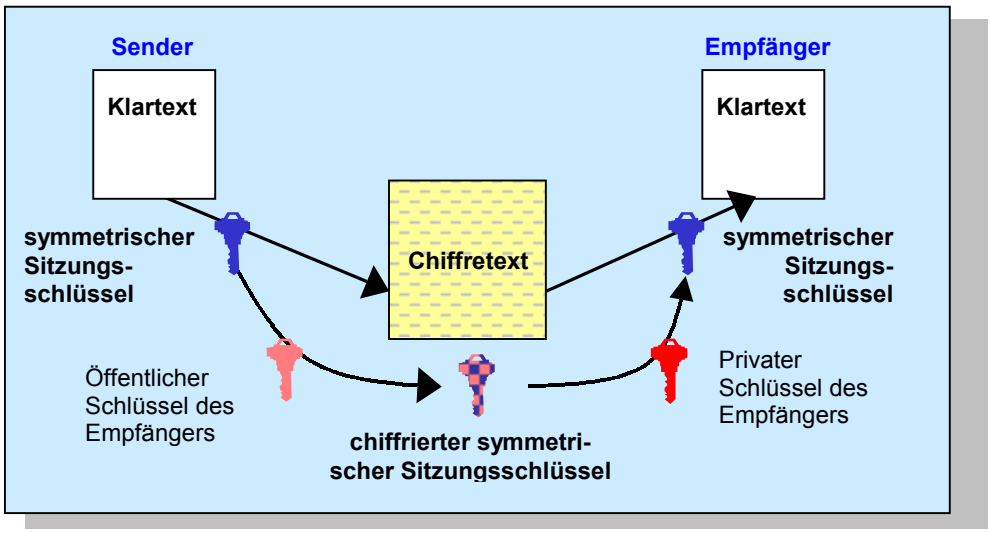

Abb. 5: Hybride Verschlüsselung

Sowohl Chiffretext als auch chiffrierter symmetrischer Sitzungsschlüssel werden dem Empfänger übermittelt. Mithilfe seines privaten Schlüssels dechiffriert dieser den Sitzungsschlüssel und damit nachfolgend den Nachrichtentext selbst.

3.3 Integrität der Daten

Verschlüsselung sichert die Vertraulichkeit von übermittelten Daten. Um den Originaltext einer Nachricht reproduzieren zu können, muß eine ganz bestimmte Entschlüsselungsfunktion bekannt sein und auf den verschlüsselten Text angewendet werden. Ver-

28 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg: dpunkt-Verlag 1998, S. 109.

29 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, a. a. O. , S. 203 ff.

schlüsselung allein sichert aber nicht die Integrität der übermittelten Daten. Eine Nachricht kann durchaus verändert und verfälscht werden, ohne daß sie zuvor entschlüsselt werden muß, z. B. durch Übertragungsfehler.

Um die Unverfälschtheit von Daten überprüfen zu können, bedarf es eines Vergleichskriteriums, das vom Sender generiert wird und vom Empfänger zwecks Abgleich reproduziert werden kann. Hierzu wird aus dem Klartext einer Nachricht eine Zeichenkette mit fester Länge erzeugt, die als Hashwert bezeichnet wird. Dieser Wert sollte möglichst eindeutig sein. Jede Veränderung am Originaltext[30] führt zu einem anderen Hashwert. Natürlich wird es bei der Abbildung von beliebig langen Texten in einen endlich großen Hashwert gleiche Funktionswerte für verschiedene Dokumente geben. Dokumente mit gleichem Hashwert herauszufinden oder aus einem bekannten Hashwert ein zweites Dokument zu erzeugen, ist aber gemessen an dem „Erfolg", ein einziges Dokument fälschen zu können, unverhältnismäßig aufwendig.

Der generierte Hashwert wird an den Originaltext angehängt. Der Empfänger wendet auf das übermittelte Dokument dieselbe Hashfunktion an, vergleicht sein Ergebnis mit dem gesendeten Hashwert und überprüft so die Unversehrtheit der übermittelten Daten. Einen Hashwert zu bilden ohne Verschlüsselung des selbigen, schützt nicht davor, daß ein unbefugter Dritter die übertragenen Daten abfängt, verändert, mit einem neu generierten Hashwert versieht und so weitergibt. Um die Integrität des Hashwertes und damit der – möglicherweise unverschlüsselten – Nachricht zu sichern, kommt das Public-Key-Verfahren in entgegengesetzter Richtung zum Einsatz. Der Hashwert wird zunächst mit dem privaten Schlüssel des Senders verschlüsselt. Jeder Empfänger, der im Besitz des zugehörigen öffentlichen Schlüssels ist, kann den Original-Hashwert reproduzieren und damit die Integrität der Nachricht verifizieren. Ein solches Vorgehen bezeichnet man dann als digitales Signieren (vgl. Kapitel 3.4.3) und ist Bestandteil eines Zertifikates.[31]

Zu den heute gängigsten Hash-Verfahren im Internet zählen die von Ron Rivest entwic??kelten MD4[32] und MD5[33] sowie der vom amerikanischen National Institute of Standards and Technology (NIST) entworfene „Secure Hash Algorithm" (SHA 1[34]).

3.4 Authentifikation der Benutzer

3.4.1 Client-Authentifikation via Kennung und Paßwort

Die Übermittlung einer Benutzer-Kennung und des zugehörigen Paßworts an den Server ist das einfachste Verfahren zur Authentifizierung eines Benutzers. Ein Beispiel für die Implementierung eines solchen Verfahrens ist die sogenannte „Basic Authentication" von Web-Servern.

30 Bspw. das Hinzufügen oder Entfernen eines Leerzeichens.

31 Man beachte, daß bei einer „digitalen Signatur" im Sinne des Signaturgesetztes, digitales Signieren in Verbindung mit einem Zertifikat gemeint ist.

32 Vgl. Rivest, R. L.: The MD4 Message Digest Algorithm, RFC 1320, April 1992.

33 Vgl. Rivest, R. L.: The MD5 Message Digest Algorithm, RFC 1321, April 1992.

34 Eine verbesserte Variante des SHA mit 160 Bit langem Hashwert.

Die Kennung und das Paßwort dürfen keinesfalls unverschlüsselt übermittelt werden, wie das bei der „Basic Authentication“ standardmäßig der Fall ist. Andernfalls können sie von Dritten im Internet abgehört und für den Zugriff auf sensible Daten ausgenutzt werden.

Bei einer Verschlüsselung von Kennung und Paßwort darf auch nicht immer derselbe Schlüssel verwendet werden, da sonst mit den verschlüsselten Anmeldedaten ein neuer Anmeldeversuch (Replay-Angriff) gestartet werden kann. Außerdem können Dritte im Internet die verschlüsselten Anmeldedaten abhören, über einen längeren Zeitraum sammeln und das Paßwort über einen sogenannten Klartextangriff ermitteln – insbesondere dann, wenn die Kennung von Benutzern bekannt ist (z. B. der Name).[35]

Ein Verfahren für eine vergleichsweise sichere Authentifizierung mit Hilfe von Kennung und Paßwort wird im Zusammenhang mit der Beschreibung der SSL-Technik in Kapitel 5.3 angegeben. Die meisten auf Kennung und Paßwort basierenden Authentifizierungsverfahren, z. B. der Login über Telnet, sind aufgrund fehlender oder mangelhafter Verschlüsselung als unsicher zu verwerfen.

3.4.2 Client-Authentifikation via PIN und TAN

Ein alternatives Anmeldeverfahren stellt die Authentifikation via PIN (Persönliche Identifikationsnummer) und Transaktionsnummer (TAN) dar. Die PIN erfüllt die Funktion der Kennung, die TAN ist ein Einmal-Paßwort. Jeder Benutzer erhält eine Liste von Transaktionsnummern, die er der Reihe nach je einmal verwenden kann. Gegenüber einer Authentifikation mit einem Paßwort mit unbegrenzter Gültigkeit hat ein TAN-Verfahren den Vorteil, daß Dritte durch ein Abhören des Anmeldevorgangs keine ausreichende Information gewinnen, um selbst eine Verbindung zum Server unter der abgehörten Kennung aufnehmen zu können. Die Authentifikation mit Transaktionsnummern hat jedoch auch gravierende Nachteile:

- Für eine Web-Abfrage sind im allgemeinen mehrere TCP-Verbindungen in Folge erforderlich. Damit nicht für jede angeforderte WWW-Seite ggfs. mehrere TAN durch den Benutzer eingegeben werden müssen, wird normalerweise ein und dieselbe TAN für mehrere aufeinanderfolgende Transaktionen Gültigkeit besitzen. Ein Dritter, der die Verbindung abhört, kann dies ausnuzen und weitere Transaktionen mit derselben TAN ausführen.
- Es besteht das Problem, dem Benutzer die TAN auf sichere Weise mitzuteilen, wie auch die Übermittlung des Paßworts bei der Authentifikation mit Kennung und Paßwort problematisch ist (siehe Kapitel 3.4.1).
- Die Aufbewahrung der TAN durch den Kunden ist ein großes Problem, da kein Benutzer sich sämtliche TAN merken kann (im Gegensatz zu einem einzigen Paßwort). Auf keinen Fall darf die TAN-Liste in elektronischer Form auf dem PC des Kunden gespeichert werden, da sie sonst von potentiellen Angreifern mit Hilfe von soge-

35 Vgl. Smith, Richard E.: Internet-Kryptographie, a. a. o., S. 86 f.

nannten „trojanischen Pferden“ gestohlen werden kann. Eine Übermittlung der TAN-Liste auf elektronischem Wege scheidet somit aus.

- Aus den genannten Gründen, implementiert kein aktueller Web-Server eine Authentifizierung mittels PIN und TAN.

Ein TAN-Verfahren macht die Verschlüsselung des gesamten Datentransfers inklusive der Anmeldedaten nicht überflüssig. Inwieweit eine TAN-Authentifizierung mit vollständiger Verschlüsselung einer ebenfalls voll verschlüsselten Authentifizierung mit Kennung und Paßwort überlegen ist, muß unter Berücksichtigung der genannten Punkte von Fall zu Fall entschieden werden.

3.4.3 Client-Authentifikation durch digitales Signieren

Mit Signaturen kann man Daten vor Manipulation schützen. Um auch die Authentizität und Vertraulichkeit der Information zu gewährleisten, wird wie folgt verfahren.[36]

Der Absender signiert mittels Hashfunktion und seinem privaten Schlüssel den Klartext wie in Kapitel 3.3 beschrieben. Anschließend wird der Klartext mit dem öffentlichen Schlüssel des Empfängers chiffriert (siehe Abb. 6).

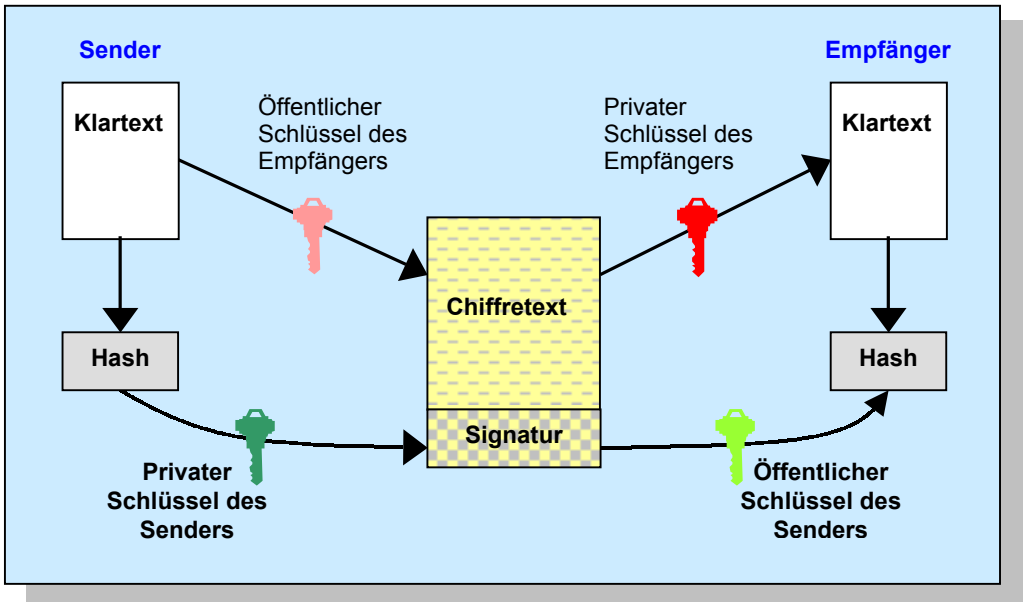

Abb. 6: Verschlüsselung und digitale Signatur

Der Empfänger dechiffriert den Chiffretext mit seinem eigenen privaten Schlüssel und berechnet den Hashwert des Klartextes mit der gleichen Hashfunktion wie der Sender. Anschließend dechiffriert er die Signatur des Senders mit dessen öffentlichem Schlüssel und erhält damit den gesendeten Hashwert. Eine Übereinstimmung der beiden Hashwerte garantiert, daß die Daten sowohl unverfälscht und korrekt, also integer, als auch

36 Vgl. Smith, Richard E.: Internet-Kryptographie, a. a. o., S. 21.

authentisch sind, also von dem Sender kommen, dem der öffentliche Schlüssel für die Entschlüsselung der Signatur gehört. Durch die Verschlüsselung des Originaltextes ist zudem gewährleistet, daß die Daten auf dem Übertragungsweg nicht von Dritten eingesehen wurden, da sie nur mit dem privaten Schlüssel des Empfängers zu entschlüsseln sind.

3.5 Autorisierung der Benutzer

Die Gewährleistung der Integrität und Vertraulichkeit der übertragenen Informationen sowie die Authentifizierung der Benutzer bilden die Grundlage für deren Autorisierung. Sie erfordert folglich ein Zusammenwirken dieser einzelnen Komponenten in einer Sicherheitsarchitektur.[37]

Autorisierung regelt die Zuteilung, Verwaltung und Überprüfung von Zugangs- und Zugriffsrechten auf Rechner, Programme und Daten innerhalb eines unternehmensinternen Netzes. Jeder, der einen Service des BKM-internen Netzes anfordert, muß dazu von der BKM autorisiert sein. Zugangs- und Zugriffsrechte sind an die Identität des Benutzers gebunden, so daß eine Autorisierung immer die Authentifizierung (siehe Kapitel 3.4) voraussetzt. Die zuvor beschriebenen Mechanismen zur Authentifizierung von Benutzern und Diensten existieren erst seit kurzem. Damit und mit der abgesicherten Datenübertragung (siehe Kapitel 3.2 und Kapitel 3.3) wird erstmals eine wirkungsvolle Autorisierung auch für Internet-Protokolle möglich.[38]

Fordert ein Kunde einen Internet-Service an, prüft die Firewall anhand der externen IP-Adresse und der internen Portnummer die Zugangsberechtigung der Anfrage zum BKM-internen Netz und zum gewünschten Service. Kommt die Verbindung zustande, prüft der Web-Server anhand der Identifikation des Anfragers (Kunde) die Berechtigung des Zugriffs durch diesen auf die zur Übertragung angeforderten Daten.

Für die Übermittlung statischer Internet-Seiten genügt eine Zugriffssicherung durch den Web-Server auf URL-Ebene. In diesem Fall sind der Kennung eines Benutzers bestimmte Internet-Seiten fest zugeordnet. Dieses Verfahren trägt natürlich nicht für das KKIS der BKM, weil z. B. der Kontostand eines Benutzers jeweils aktuell ermittelt und dynamisch erzeugt werden muß.

Zur Erstellung dynamischer Internet-Seiten dienen u. a. CGI-Programme und Java-Servlets. Hier kann die Zugriffssicherung durch den Web-Server nicht auf URL-Ebene eingegrenzt werden, da unterschiedliche Benutzer dieselben CGI-Programme oder Java-Servlets verwenden. In diesem Fall muß der Web-Service (das CGI-Programm resp. Java-Servlet) die Zugriffskontrolle durchführen und für den Aufbau einer dynamischen Internet-Seite nur erlaubte Datenzugriffe durchführen.

Die Beziehungen zwischen Anwender-Identifikation und Zugriffsrechten (Benutzerprofilen) werden zumeist in Datenbanken gespeichert und sind von jedem Web-Service ab-

37 Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 131.

38 Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 131.

zufragen, um die Autorisierung eines Benutzers für diesen Service zu gewährleisten. Mit der Öffnung des BKM-internen Netzes nach außen wächst die Anzahl der zuzulassenden Benutzer und die Menge der Daten, die über jeden Benutzer zu speichern sind. Neben den Benutzerprofilen werden IP-Adressen, eMail-Adressen, Netzwerk-Adressen für Server, URLs, öffentliche Schlüssel u. a. m. benötigt, um über die Zulässigkeit einer Anforderung aus dem Internet zu entscheiden.

Für die Ablage dieser verschiedenartigen Informationen sind inzwischen standardisierte Datenmodelle mit Zugriffsoperationen auf diese Datenmodelle, sogenannte Verzeichnisdienste (engl. directory services), verfügbar[39]:

- X.500[40] für Adreßinformationen
- X.509[41] für Zertifkate (siehe Kapitel 3.6)

Ein Directory Server ist ein zentrales Repository mit Paaren aus teilqualifizierendem Attribut und Wert, aus dem ein Client mit Hilfe von strukturierten Abfragen Einträge ermitteln kann. Ein eindeutiger Pfad zu einer Identität wird als Distinguished Name (dn) bezeichnet.

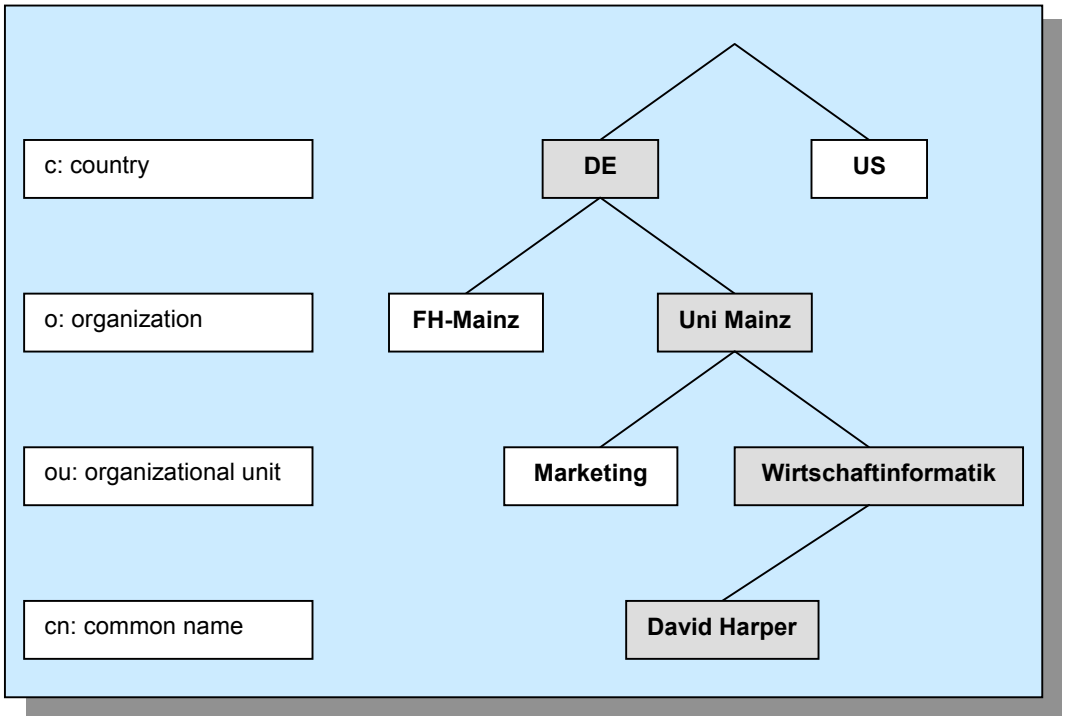

Abb. 7: Globaler Namensraum nach X.500

Ein Verzeichnisdienst repräsentiert das Telefonbuch des Netzwerks.[42] Internet-Clients steht z. B. für Anfragen an einen Directory-Server das ebenfalls standardisierte Proto-

39 Vgl. Smith, Richard E.: Internet-Kryptographie, a. a. o., S. 316 f.

40 Ein in Zusammenarbeit der ISO und der ITU-T entstandener Verzeichnisdienst.

41 Vgl. CCITT, Recommendation X.509, The Directory-Authentication Framework, Consultation Committee Iternational Telephone and Telegraph, International Telecommunications Union, Genf 1989.

koll LDAP (Lightweight Directory Access Protocol) zur Verfügung.[43] Bekannte Implementierungen sind der frei verfügbare LDAP-Server der University of Michigan und der Netscape Directory Server.

LDAP benutzt als zugrundeliegenden Transportmechanismus die Internet-Protokolle, baut auf TCP auf und zeichnet sich durch folgende Punkte aus:

- relativ einfache Handhabung von Benutzerkonten,
- zentrale Verwaltung und Bereitstellung von Adresslisten,
- zentrale Vergabe und Verwaltung von Benutzerrechten (unabhängig vom Betriebssystem),
- Konzentration aller relevanten Daten (auch Bilder, PGP-Schlüssel o. ä.) über Personen, Rechner usw.

Als Zugriffsoperationen auf LDAP-Verzeichnisse sind search, compare, add, delete, modify und modRDN (relative distinguished name) definiert.[44] Aufgrund des offenen Standards existieren bereits Gateways zwischen LDAP und X.500 sowie von HTTP, WHOIS++, Finger, eMail und SSL jeweils auf LDAP.

Microsoft versucht, durch AD (Active Directories) einen neuen, eigenen Ansatz für diese Systemdienste zu etablieren und die verschiedenen bereits vorhandenen Standards unter Windows NT zu vereinheitlichen. AD sollen im angekündigten Windows 2000 enthalten sein[45] und basiert auf X.500 und LDAP.

3.6 Verbindlichkeit der Kommunikation

Zur Verbindlichkeit der Kommunikation gehört neben der Vertraulichkeit, Integrität und Authentizität der ausgetauschten Daten auch der zweifelsfreie Nachweis, welche Partner an der Kommunikation beteiligt sind. Dies ist weniger ein kryptographisches Problem als eine Frage des Vertrauens zur Quelle eines öffentlichen Schlüssels. Praktisch gelöst wird die Zuordnung eines Schlüssels daher von einer vertrauenswürdigen Organisation. Eine Certifying Authority (CA)[46] gibt sogenannte Zertifikate heraus, die bestätigen, daß ein Schlüssel einer bestimmten Person oder Institution gehört. Demnach wird durch ein Zertifikat die Identität durch eine unabhängige, vertrauenswürdige Organisation festgestellt und geprüft. Eine Identität kann eine Person, ein Server, ein Unternehmen, ein Software-Anbieter o. ä. sein.

42 Vgl. Graefen, Rainer; Reuß, Annette: Verzeichnisdienste: Hoffnung für gestreßte Administratoren, in: Information Week, 3/1999, S. 38 f.

43 Die Standardisierung des LDAP-Protokolls erfolgt durch die Access and Searching of Internet Directories-Arbeitsgruppe (ASID) der Internet Engineering Task Force (IETF). LDAP ist sehr gut in Form von Internet-RFCs dokumentiert: RFC-1823, RFC-1777-1779, RFC-1558. Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 113.

44 Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 114.

45 Vgl. Graefen, Rainer; Reuß, Annette: Verzeichnisdienste: Hoffnung für gestreßte Administratoren, a. a. O., S. 38 f.

46 Im deutschsprachigen Raum auch oft als Trust Center oder Zertifizierungsstelle bezeichnet.

Die von den CA als Nachweis der Identität erbrachte Zertifizierung geschieht bspw. nach X.509[47], einem von der International Telecommunication Union (ITU) Standardisierten Zertifikateformat. Dieses Format ist Grundlage für den Austausch von Zertifikaten zwischen Anwendungen unterschiedlicher Hersteller. Zertifikate nach X.509 speichern und verwalten die dazugehörigen Daten in hierarchischen Verzeichnisstrukturen gemäß X.500-Standard und sind von den verwendeten asymmetrischen Verschlüsselungsverfahren (siehe Kapitel 3.2.2). unabhängig.

Für die Richtigkeit und Gültigkeit eines Zertifikats bzw. eines „digitalen Ausweises" bürgende Certifying Authoritys sind z. B.

- American Express Global CA,
- VeriSign Inc. in den USA,
- Thawte Consulting in Kapstadt, Südafrika,
- TC TrustCenter for Security in Data Networks GmbH in Hamburg[48],
- TeleSec Trust Center Deutsche Telekom AG.

Zertifikate enthalten

- den Namen des Schlüsselinhabers oder dessen Pseudonym,
- die laufende Nummer der Zertifikats,
- den öffentlichen Schlüssel,
- die angewendeten Algorithmen der Schlüsselerzeugung und -verifikation,
- den Gültigkeitszeitraum des Zertifikats,
- Informationen, ob die Anwendung des Schlüssels auf bestimmte Anwendungen eingeschränkt ist,
- die Signatur und den Namen der Certifying Authority.

Für eine Person, ein Unternehmen, einen Server oder andere wird bei der CA ein Zertifikat beantragt. Die CA prüft die Identität des Antragstellers und bescheinigt diese Identität, indem sie seinen öffentlichen Schlüssel zusammen mit den oben genannten Informationen digital signiert.[49] Jeder beliebige Kommunikationspartner kann die Signatur der CA mit dem öffentlichen Schlüssel der CA[50] verifizieren und damit die Identität seines Gegenübers überprüfen.[51]

47 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, a. a. O. , S. 652.

48 Netscape 4.5 liegen erstmals Zertifikate einer deutschen CA bei. Vgl. Luckhardt, Norbert: Deutsche Zertifikate in Netscape 4.5, Online im Internet: http://www.heise.de/newsticker/data/nl-27.10.98-000/, 07.07.1999.

49 Vgl. Jörn, Fritz: Trotz aller Verschlüsselung muß man Vertrauen haben: Das asymmetrische Chiffrieren und die Rolle des Trust Center, in: Frankfurter Allgemeine Zeitung, 17.02.1998, S. T5.

50 Zertifikate der oben genannten CA sind im Netscape Navigator 4.6 standardmäßig enthalten.

51 Internationale Großbanken darunter die Bank of Amerika, die Deutsche Bank und die Hypovereinsbank testen in einem Pilotprojekt die Interoperabilität unterschiedlicher Signaturen. Sie haben dazu ein gemeinsames Trust Center (TC) aufgebaut, das als internationale Zertifizierungsinstanz für Business-to-Business-Transaktionen auftreten soll. Vgl. Afif, Noelani Maria: Digitale Signatur im Test, in: Information Week, 16/1999, S. 10.

Der Antragsteller braucht natürlich noch den zu seinem public key gehörenden private key. Es gibt grundsätzlich zwei Möglichkeiten wie er diesen bekommt. Entweder hat er das Schlüsselpaar selbst erzeugt und den public key der CA übergeben oder die CA hat für ihn das Schlüsselpaar generiert und er bekommt sowohl das Zertifikat als auch den private key ausgehändigt. Grundsätzlich ist die zweite Methode für den Antragsteller mit weniger Aufwand verbunden, jedoch besteht im Transport des private key von der CA zum Antragsteller ein Sicherheitsproblem. Die Vertrauenswürdigkeit einer CA und der von ihr ausgestellten Zertifikate ist nur zu erreichen, wenn die ausstellende CA keine geheimen Teilnhmerschlüssel kennt. Als Ausweg aus leichter Handhabbarkeit und optimaler Sicherheit zeichnet sich die Schlüsselgenerierung auf einer Chipkarte ab. Das Generieren des Schlüssel läuft vollständig auf der Chipkarte ab. Wenn diese dann später auch mit Hilfe eines Kartenlesegerätes zum entschlüsseln verwendet wird, muß der private key die Chipkarte nicht verlassen.[52]

4 IT-Sicherheitsziele

4.1 Kundenanforderungen

Viele Internet-Nutzer scheuen aus Angst vor Manipulationen das Einkaufen und Bezahlen im Internet. Die eCommerce-Anbieter sind daher gehalten bestimmte Strategien und Maßnahmen zur Vertrauensbildung zu ergreifen.[53]

Bei Kunden ist die Sicherheit mehr ein Problem der Wahrnehmung als der Technologie. Sie Nutzen die Angebote nicht, wenn ihnen das Vertrauen in die für sie vielleicht undurchsichtigen Abläufe und Verfahren fehlt. Die Kreditkartenzahlungen mit SET (Secure Electronic Transactions), einem von Visa und Mastercard entwickelten Standard zur sicheren Abwicklung von Kreditkartentransaktionen über die Internet-Protokolle, sind hierfür ein gutes Beispiel. Trotz Lösung der Sicherheitsproblematik wird die Kreditkartenzahlung mit SET von vielen Internet-Nutzern nicht angenommen. Die Mehrzahl der Nutzer hat keine Vorstellung von den potentiellen Risiken. Es werden deshalb einfache und transparente Schutzmechanismen benötigt, die den sicheren Umgang auch ohne tiefgehendes Verständnis der Technik garantieren.

Ausgehend von der Prämisse, daß das zur Verfügung gestellte Informationsangebot grundsätzlich für den BKM-Kunden interessant ist, läßt sich eine hohe Kundenakzeptanz besonders bei Berücksichtigung der folgenden Aspekte erzielen:

Geringer Installationsaufwand beim Kunden

Der Zugang zum KKIS sollte soweit wie möglich mit Hilfe von Standard-Software erfolgen können und im Idealfall ohne spezielle Konfiguration bzw. Installation zusätzlicher Client-Software beim Kunden möglich sein.

52 Vgl. Nehl, Roland: Schlüsselgenerierung in Trust Centern?: Vertrauen durch Trust Center, in: DuD Datenschutz und Datensicherheit, 2/1997, S. 101.

53 Krempel, Stefan: Alles auf eine Karte, in: Computerwoche Spezial, 4/1998, S. 54

Intuitive Benutzerschnittstelle
Die dem Benutzer präsentierte Oberfläche sollte sich an einschlägigen Standards orientieren und intuitiv zu bedienen sein.

Akzeptable Performanz
Die Antwortzeiten des KKIS sollten auch bei weniger schnellen Internet-Verbindungen (z. B. analoge Modemverbindung) annehmbar sein.

Geringe Hardware-Anforderungen
Die Zugangssoftware auf Kunden-Seite sollte auf einem möglichst großen Anteil der heute installierten PCs lauffähig und performant sein.

Absolute Sicherheit und Vertraulichkeit
Dem Kunden muß eine Sicherheitsinfrastruktur geboten werden, die ein Überwinden der Sicherheitsvorkehrungen und Manipulationen zu seinem Nachteil verhindert.

4.2 Unternehmensanforderungen und -ziele

Services über das Web anzubieten, in interne Bearbeitungsstrukturen zu übernehmen und mit einem adäquaten Sicherheitssystem auszustatten, sind eine komplexe Vorgänge, vor denen sich viele im Internet präsente Firmen scheuen.[54] Dabei erschließt erst die Integration unterschiedlicher unternehmensinterner Prozesse das Potential dieser Vertriebs-/Serviceschiene. Um die Potentiale des KKIS zu beurteilen und sie angemessen umzusetzen, sollten folgenden Aspekte Beachtung finden:

Kostensenkung
BKM-intern wird die Effizienz im Kundenservice steigen, da der Kunde direkt, ohne Mitarbeiter zu involvieren, die im KKIS gebotenen Dienstleistungen nutzen kann.

Beschleunigung des Workflows
Durch Vermeidung der beim Telefon- bzw. Brief-basierten Kundenservice auftretenden Medienbrüche und Wartezeiten wird via eService (KKIS) die Abwicklung der Kundenwünsche beschleunigt.

Absatz Steigerung
Größere Kundenzufriedenheit bewirkt eine Stärkung der Kundenbindung und hat damit indirekt Einfluß auf den Absatz.

Sicherheit
Adäquate Sicherheitsverfahren müssen auch aus dem eigenen Sicherheitsbedürfnis heraus angestrebt werden.

Akzeptanz beim Kunden
Durch Erfüllung der in Kapitel 4.1 dargelegten Kundenanforderungen wird die Basis für die erforderliche Akzeptanz beim Kunden geschaffen.

54 Scholvin-Wulff, Barbara: E-Commerce-Berater haben für Mittelständler wenig übrig, in Computerzeitung, 06.08.1998, S. 18.

Standardisierte nicht proprietäre Techniken
Um auf künftige Entwicklungen der Sicherheitstechniken flexibel reagieren zu können und um die zu tätigenden Investitionen zu schützen, sollten bewährte herstellerunabhängige Standards und Verfahren zum Einsatz kommen.

Systemintegration und IT-Homogenisierung
Die bestehende IT-Infrastruktur muß berücksichtigt werden. Das KKIS und das zugehörige Sicherheitskonzept müssen in die Systemlandschaft integrierbar sein.

Image und Marketing
Letztendlich ist das Anbieten von Internet-Services heute auch eine Image-/Marketing-Angelegenheit und muß auch aus marktpolitischer Sicht betrachtet werden.

4.3 Gesetzliche Anforderungen

Die IT-Sicherheit wird hauptsächlich aus dem eigenen Sicherheitsbedürfnis angestrebt, auch wenn sich ihre Notwendigkeit aus vielen gesetzlichen Anforderungen ableiten läßt. Diese beziehen sich allerdings meist nur auf den Umgang mit Informationen und Daten.

Diese gesetzlichen Anforderungen sind im Bundesdatenschutzgesetz (BDSG) geregelt. Datenschutz ist der gesetzliche Schutz des Persönlichkeitsrechts und zielt damit ausschließlich auf Informationen, die sich unmittelbar oder mittelbar auf natürliche Personen beziehen. Dabei stehen vor allem die Zulässigkeit der Erhebung, Verarbeitung und Nutzung sowie die Vertraulichkeit der personenbezogenen Daten im Vordergrund. Da das KKIS direkt auf JoKer aufsetzen wird und diese Aspekte von JoKer bereits berücksichtigt werden, besteht für das KKIS hier kein Handlungsbedarf.

Zu den gesetzlichen Anforderungen gehört auch die Ordnungsmäßigkeit der betrieblichen Aufgabenerfüllung. Dazu zählen beispielsweise die Einhaltung der und GoB[55] bei finanzwirksamen Daten sowie die Revisionsfähigkeit. Auch diese Aspekte sind bereits durch JoKer berücksichtigt und bedürfen für das KKIS hier keiner weiteren Beachtung.

Größere Bedeutung kommt der Rechtsverbindlichkeit der über das Internet im Rahmen des KKIS stattfindenden Handlungen, Willenserklärungen und Verträgen zu. Ein konkretes *Netlaw* existiert noch nicht. Es finden grundsätzlich die geltenden Vorschriften in einer Vielzahl von Rechtsbereichen zum Teil mit noch nicht gelösten Internet-spezifischen Problemen Anwendung. Mit dem Erlaß von Sondergesetzen zum Internet muß zukünftig gerechnet werden.. Die vorhandenen Gesetze bieten aber einen ausreichenden Regelungsspielraum. Der Abschluß nicht formgebundener Kauf- und anderer Verträge ist daher im Internet möglich. Im konkreten Fall des KKIS ist der entscheidende Punkt die rechtliche Verbindlichkeit der digitalen Signatur. Sie ist durch das *Informations- und Kommunikations Dienstegesetz* geregelt.[56] Der juristische Komplex muß vor Realisierung des KKIS durch auf diesem Teilgebiet fachkundigen Juristen eingehender beleuchtet werden.

55 Grundsätze ordnungsmäßiger Buchführung und Bilanzierung. Vgl. Schierenbeck, Henner: Grundzüge der Betriebswirtschaftslehre, 12., überarb. Aufl., München et al.: Oldenbourg 1995, S. 528 ff.

56 Es ist davon auszugehen, daß die EU mit einer ähnlichen Regelung nachziehen wird, da im Vorfeld Beratungen und Abstimmungsgespräche mit den EU-Mitgliedsstaaten durchgeführt wurden.

5 Relevante Standards und technische Verfahren

5.1 Überblick

In Kapitel 5 werden die für die BKM in Frage kommenden Sicherheits-Verfahren zusammengetragen und erläutert. Im einzelnen sind dies:

- Secure-Hypertext Transfer Protocol (S-HTTP; siehe Kapitel 5.2)
- Secure Sockets Layer (SSL; siehe Kapitel 5.3)
- Homebanking Computer Interface (HBCI; siehe Kapitel 5.4).

Mit PCT, TLS und DSig existieren zwar noch andere Verfahren, die jedoch die in Kapitel 4 dargelegten Ziel-Anforderungen nicht oder nur zum Teil erfüllen können. Z. B. ist das Verfahren PCT[57] (Private Communication Technology) von Microsoft ein SSL-Gegenstück, das die gleiche Funktionalität wie SSL bietet, aber zu SSL z. B. nicht kompatibel ist. Das PCT-Protokoll wird nur vom Microsoft Internet Explorer unterstützt und ist als Reaktion Microsofts auf Netscapes SSL im Kampf um Marktanteile im Internet-Geschäft zusehen. PCT besitzt keine heute praktische Relevanz mehr.

TLS (Transport Layer Security) hingegen ist noch nicht etabliert und wird gerade von der Internet Engineering Task Force (IETF) standardisiert. Ziel dabei ist es, einen industrieweiten und herstellerunabhängigen Standard zu schaffen, der auf der aktuellen SSL-Version 3.0 aufbaut. Um die beiden Konkurrenten Netscape und Microsoft zu einer Kooperation zu bewegen, hat man auf den ursprünglichen Namen SSL 3.1 verzichtet. TLS stellt im Prinzip lediglich die nächste Versionsstufe von SSL dar, das in Kapitel 5.3 näher erläutert wird.

DSig ist ein Standardisierungsvorhaben des World-Wide-Web-Konsortium (W3C)[58], das digitale Signaturen im Internet etablieren soll.[59] Es soll zum Signieren von ausführbarem Code (z. B. ActiveX, Plug-ins, Java Applets) und verbindlichen Dokumenten (z. B. Preislisten, Börsenkurse, politische Publikationen) eingesetzt werden. Zum Signieren von Benutzereingaben wird DSig nicht eingesetzt werden können und kommt deshalb für das KKIS nicht in Betracht.

5.2 Secure-Hypertext Transfer Protocol (S-HTTP)

Secure-HTTP ist der Versuch, alle kryptographischen Defizite von HTTP auf einen Schlag zu lösen und umfangreicher als das nachfolgend beschriebene SSL (siehe Kapitel 5.3). In der Praxis ist jedoch S-HTTP kein Erfolg und gilt als gescheitert.[60] Einer der

57 Benloh, J.; Lampson, B.; Simon, D.;Spies, T.; Yee, B.: The Private Communications Technology Protocol, Online im Internet: http://www.lne.com/ericm/pct.html, 13.06.1999.

58 Neben dem IETF entwickelt auch das W3C Standards für das Internet. Das W3C ist im Gegensatz zum IETF ein Industrieverband und nur für Vertreter der Mitgliedsfirmen zugänglich.

59 Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O., S. 232.

60 Vgl. Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O, S. 231 und Smith, Richard E.: Internet-Kryptographie, a. a. O. S. 251.

Hauptgründe ist die komplizierte Konfiguration der zahllosen kryptographischen Operationsmodi in Konfigurationsdateien, die dem Anwender unter S-HTTP geboten werden. Ein SSL-Server läßt sich in der Regel mit nur wenigen Handgriffen einstellen.[61]

Mosaic, der einzige kommerzielle Browser der S-HTTP implementiert hatte, wird nicht mehr weiterentwickelt und auch IBM hat die S-HTTP Unterstützung mit dem Versionswechsel von 4.1 zu 4.2 des Internet Connection Secure Server eingestellt. Daneben bieten nur noch der Transact Server von Open Market und Secure das Web Toolkit von Terisa Systems S-HTTP an (die Autoren der S-HTTP Drafts sind über ein Beratungsunternehmen mit Terisa Systems verbunden).

5.3 Secure Sockets Layer (SSL)

Das Übertragungsprotokoll Secure Socket Layer (SSL) wurde von Netscape Communications Corporation entwickelt, um den Anwendern einen einfachen, weitestgehend transparenten Mechanismus zur Verschlüsselung von vertraulichen Nachrichten zwischen Web-Client (Browser) und -Server über das Internet zu ermöglichen.[62] Das SSL-Protokoll beinhaltet sowohl die Definition der Protokollstrukturen zur Übertragung der verschlüsselten Daten als auch ein Verfahren für den Austausch der notwendigen Schlüssel, die sogenannte Schlüssel-Akquisition.[63]

SSL wurde Ende 1994 von Netscape im Rahmen eines Sicherheitspakets für das World Wide Web vorgestellt und in Verbindung mit dem schon damals weit verbreiteten Netscape Navigator kostenlos angeboten. Aufgrund der starken Marktposition Netscapes und der frühzeitigen Veröffentlichung fand SSL schnell Verbreitung und wurde in viele Produkte anderer Hersteller integriert.[64]

SSL implementiert die bisher diskutierten Verfahren hybride Verschlüsselung, digitale Signatur und Zertifikate. Es verwendet ein symmetrische Verfahren (z. B. DES oder RC 4) zur Verschlüsselung des Klartextes und RSA für das Management des Sitzungsschlüssels.[65] Das Protokoll läßt sich in Anwendungssoftware für Web-Clients und -Server integrieren. Es handelt sich dabei um eine zusätzliche Schicht (Layer) zwischen TCP/IP und dem Verbindungsprotokoll (HTTP, FTP, SMTP etc.). SSL setzt auf TCP/IP auf und ersetzt die Standard-Socket-Kommunikation durch sichere Sockets.[66]

SSL ist gegenwärtig das wichtigste kryptografische Protokoll im Internet und zeichnet sich besonders durch die Vielzahl der unterstützten Verschlüsselungsalgorithmen aus.

61 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 140.

62 Netscape Communications (Hrsg.): SSL 3.0 Specification, Online im Internet: http://home.netscape.com/eng/ssl3/ssl-toc.html, 12.07.1999.

63 Vgl. Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 124.

64 Vgl. Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O, S. 296.

65 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 134.

66 Alle Anwendungen, die über Sockets kommunizieren, können relativ einfach auf Secure Sockets umgestellt werden, so die Applikation im Source-Code vorliegt.

Der Datenaustausch über SSL zwischen Client und Server erfordert auf mindestens einer Seite ein Zertifikat. Das ist sinnvollerweise die Server-Seite, da nicht von jedem Web-Client die Zertifizierung verlangt werden kann. Bis SSL Version 3 war auf der Client-Seite keine Zertifizierung vorgesehen. Im Zentrum des SSL-Protokolls steht das digitale Schlüsselpaar aus öffentlichem und privatem Schlüssel des Servers sowie der Distinguished Name (siehe Kapitel 3.5) der Zertifizierungsstelle. Es wird für jeden (virtuellen) Web-Server ein eigenes Schlüsselpaar benötigt, weil bei dem Distinguished Name unter anderem der Host-Name als Common Name (cn) einfließt.

SSL garantiert

- Vertraulichkeit der Daten durch Verschlüsselung,
- Integrität der Daten durch wirkungsvolle Überprüfungsalgorithmen,
- Authentizität des Servers und optional auch des Web-Clients.[67]

Um normalen von SSL-geschütztem Datenverkehr zu unterscheiden, benutzt SSL-fähige Web-Software eine spezielle Portnummer. SSL-geschützter Web-Verkehr läuft i. a. über eine Verbindung zum Port 443 des Web-Servers, im Gegensatz zum standardmäßig für HTTP genutzten Port 80. Das SSL-Protokoll wird auf der Client-Seite dadurch aktiviert, daß dem bekannten HTTP ein S angehängt wird (z. B. in *https://www.bkm.de*).[68] Dadurch kann gesteuert werden, welche Art von Verkehr verschlüsselt und welcher ohne kryptographischen Schutz (und damit schneller) abgehandelt wird.

Das SSL-Protokoll zeichnet sich dadurch aus, daß Browser und Web-Server die zu verwendenden kryptographischen Verfahren selbst aushandeln (siehe Abb. 8). Der Web-Client (Browser) fordert eine Verbindung zum Server an und teilt in Form einer Liste dabei mit, welche Verschlüsselungs- (siehe Kapitel 3.2) und Hash-Algorithmen (siehe Kapitel 3.3) sowie Schlüssellängen er unterstützt (Schritt 1 in Abb. 8). Der Server entfernt aus dieser Liste die von ihm nicht unterstützten Verfahren und schickt die angepaßte Liste zurück zum Client (Schritt 2 in Abb. 8). Dieser trifft nun die Auswahl der Verschlüsselung.[69] Für die aktuelle Sitzung ist ab jetzt das beidseitig anzuwendende Verschlüsselungsverfahren vereinbart.

Danach erhält der Web-Client vom Server ein Zertifikat (siehe Kapitel 3.5) mit dem öffentlichen Schlüssel des Servers (Schritt 3 in Abb. 8). Dieses Zertifikat reicht aber noch nicht zur Authentifizierung des Servers (siehe Kapitel 3.4) aus, weil es bspw. aus einer anderen Verbindung kopiert sein kann. Der Server muß noch „beweisen“, daß es das eigene Zertifikat ist, d. h., daß er im Besitz des zugehörigen privaten Schlüssels ist.

Dafür erzeugt der Web-Client einen zufälligen Sitzungsschlüssel (Schritt 4 in Abb. 8) für ein symmetrisches Verschlüsselungsverfahren (siehe Kapitel 3.2.1). Der Sitzungs-

67 Vgl. Smith, Richard E.: Internet-Kryptographie, a. a. o., S. 258.

68 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 134.

69 Es ist zu bemerken, daß in der Literatur sich teilweise widersprechende Ausführungen zum Ablauf dieses Handshakes gemacht werden. Vgl. Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O, S. 267, Nusser, Stefan: Sicherheitskonzepte im WWW, a. a. O., S. 126 und Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 134.

schlüssel wird mit dem öffentlichen Schlüssel des Servers asymmetrisch chiffriert (Schritt 5 in Abb. 8) und zusammen mit einer Reihe mit dem symmetrischen Sitzungsschlüssel verschlüsselter Testnachrichten zum Server übertragen (Schritt 6 in Abb. 8). Nur der Server, der in Besitz des zum öffentlichen Schlüssel passenden privaten Schlüssels ist, kann zunächst den Sitzungsschlüssel wieder entschlüsseln (Schritt 7 in Abb. 8), um dann damit wiederum den empfangenen Nachrichtentext zu entschlüsseln (Schritt 8 in Abb. 8). Er bestätigt die Nachrichten mit eindeutigen Antworten, verschlüsselt diese Antworten mit dem Sitzungsschlüssel (Schritt 9 in Abb. 8) und überträgt sie an den Web-Client (Schritt 10 in Abb. 8). Dieser Schritt ist die eigentliche Server-Authentifizierung, denn nur der Besitzer des privaten Server-Schlüssels ist überhaupt in der Lage, den Sitzungsschlüssel und damit die Testnachrichten zu lesen, um diese dann eindeutig beantworten zu können.

SSL verwendet asymmetrische Verschlüsselungsverfahren demnach nur zum Austausch von Sitzungsschlüsseln und zur Authentifizierung. Für die Verschlüsselung der auszutauschenden Klartexte, die beliebig groß sein können, benutzt SSL die wesentlich schnelleren symmetrischen Verschlüsselungsverfahren.

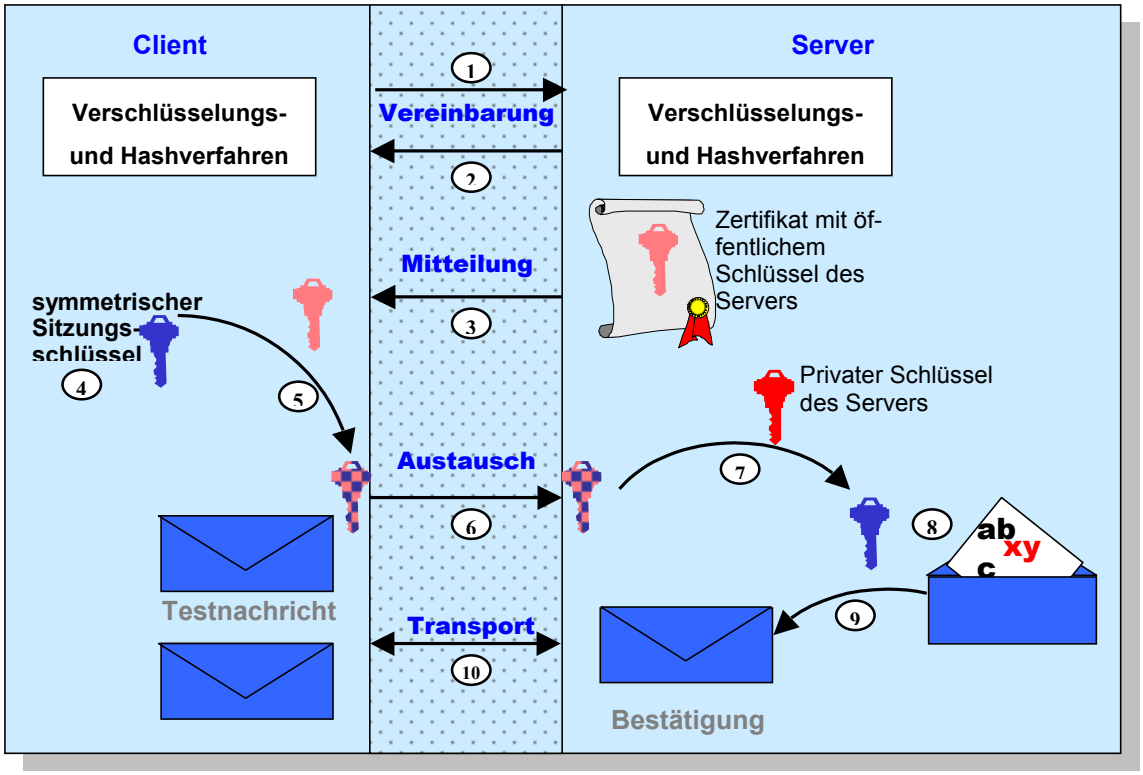

Abb. 8: Funktionsweise des SSL-Protokolls

Mit SSL authentifiziert sich immer der Server ggü. dem Client. Die optionale Client-Authentifizierung läuft ähnlich wie die Server-Authentifizierung ab, setzt aber natürlich voraus, daß der Client (Browser) über einen offiziell zertifizierten Schlüssel verfügt.

US-Produkte wie der Netscape Enterprise Server und Navigator sowie Microsoft Internet Information Server (MS-IIS) und Internet Explorer sind für den Export auf eine

Schlüssellänge von maximal 40 Bit beschränkt (siehe Kapitel 3.2.1). Bei symmetrischen Verschlüsselungsverfahren gelten aber als aktueller „sicherer“ Standard 128-Bit-Schlüssel. Ausschließlich für den Netscape Navigator Web-Client gibt es ein australisches Freeware Zusatzprogramm („Fortify for Netscape“[70]), mit dem die verwendeten Schlüssel von 40 auf 128 Bit erweitert werden können. Der so veränderte Web-Client ist dann in der Lage, starke 128-Bit-Verschlüsselung zum Web-Server aufzubauen, wenn auch dieser dies unterstützt. (Laut Netscape USA verletzt der Einsatz von Fortify die Endbenutzer-Lizenzvereinbarung![71]) Für Web-Server mit Export-Beschränkung sind nichtamerikanische Krypto-Routinen wie die australische SSLeay-Lösung für C-Implementierungen oder die schweizerische Cryptix-Bibliothek für Java-Implementierungen zu empfehlen. Folgende SSL-Software ist derzeit auf dem Markt verfügbar:

Web-Server	
	Netscape Enterprise Server
	Microsoft Internet Information Server (mit Exportbeschränkung)
	Apache-SSL (Apache Version die sich der SSLeay-Bibliothek bedient)
	Stronghold Webserver (Kommerzielles Paket aus Apache-SSL mit einigen Erweiterungen und Wartungsvertrag)
Web-Clients	
	Netscape Navigator (mit Exportbeschränkung)
	Microsoft Internet Explorer (mit Exportbeschränkung)
SSL Entwicklungs-Bibliotheken	
	SSLeay (frei verfügbarer C-Quellcode für nahezu alle Funktionen im Zusammenhang mit Zertifikaten, CAs und Verbindungsaufbau. Unterliegt als australisches Produkt keiner Exportbeschränkung)
	Java-Security-Library von Cryptix (Untermenge der SSLeay-Funktionen als Java-Klassen)
	SSLava von Phaos (Java SSL-Bibliothek die der Exportbeschränkung unterliegt)

Tab. 2: SSL-Produkte

5.4 Homebanking Computer Interface (HBCI)

HBCI ist ein nationaler Branchenstandard, der aktuell in der Version 2.01 zum Einsatz kommt. Entwickelt wurde er als Homebanking-Schnittstelle im Auftrag des Zentralen Kreditausschusses (ZKA).[72] HBCI unterstützt insbesondere die Eigenheiten des deutschen Zahlungsverkehrs. Ziel ist es, HBCI als mindestens nationalen Industriestandard zu etablieren und darüber hinaus zur Standardisierung in internationale, speziell euro-

70 Vgl. Fortify for Netscape (Hrsg.): Homepage, Online im Internet: http://www.fortify.net, 22.07.1999. In Deutschland übernimmt Thierschmidt Datenschutz (http://www.thierschmidt.com/) den kommerziellen Vertrieb des Australischen Netscape-Patches Fortify.

71 Luckhardt, Norbert: Deutscher Support für Krypto-Patch, Online im Internet: http://www.heise.de/newsticker/data/nl-13.01.99-000/, 13.06.1999.

72 Ein HBCI-Referenzsystem wurde im Auftrag des Informatikzentrums der Sparkassenorganisation GmbH (SIZ) durch Pape + Partner Informationssysteme GmbH, Hamburg entwickelt.

päische Gremien einzubringen. Im Rahmen des Homebanking-Abkommens, initiiert durch den ZKA, haben sich bundesweit alle Banken und Sparkassen über ihre Dachverbände verpflichtet, HBCI bis Anfang Oktober 1998 einzuführen.

Mittelfristig wird HBCI die ursprünglich BTX[73]-basierten Homebanking-Lösungen ersetzen und soll im Internet Banking eine zentrale Rolle spielen. Deshalb ist damit zu rechnen, daß die auf dem deutschen Markt angebotenen Homebanking-Produkte wie Intuit Quicken oder Microsoft Money in naher Zukunft HBCI unterstützen werden, obgleich sich diese Hersteller auf das gemeinsame Protokoll OFX[74] geeinigt haben.

Bei der aktuellen HBCI-Version 2.01 stehen neben Kontostandsabfragen und Kontenübersichten, wie sie für das KKIS der BKM benötigt werden, auch die Geschäftsvorfälle Einzelüberweisungen, Daueraufträge, Lastschriften, Festgeldanlagen, Depotaufstellungen, Terminvereinbarungen und Formularbestellungen, wie z. B. Schecks und andere Zahlungsverkehrvordrucke, zur Verfügung.[75]

Grundlegend werden bei HBCI zwei kryptographische Verfahren eingesetzt. Zum einen eine auf einer ZKA-Chipkarte (wie sie auch als ec-Chipkarte Verwendung findet) implementierte symmetrische Verschlüsselung mit Triple-DES (siehe Kapitel 3.2.1), zum anderen eine Softwarelösung mit Diskette, die nach dem asymmetrischen RSA-Verfahren (siehe Kapitel 3.2.2) arbeitet.

Die zur Verschlüsselung eingesetzten Schlüssel bzw. Schlüsselpaare müssen zwischen Kunde und Bank ausgetauscht werden. Beim Chipkarten-Verfahren ist der Schlüsselaustausch unproblematisch. Die Schlüssel werden bei der Bank generiert, auf der Chipkarte abgelegt und dem Kunden in Form dieser Chipkarte ausgehändigt. Beim Softwarebasierten-Verfahren entstehen die Schlüsselpaare beim Kunden. Der Kunde selbst erzeugt und verwaltet per PC-Software seine persönlichen Schlüsselpaare aus privaten und öffentlichen Schlüsseln. Es müssen daher nur die öffentlichen Schlüssel des Kunden an das Banksystem übermittelt werden. Die notwendige Funktionalität ist immer Bestandteil des HBCI-Kundensystems, gleichgültig, ob es sich dabei um ein Endprodukt oder eine Eigenentwicklung handelt.

Vorteil des Chipkarten-Verfahrens ist, daß alle sensitiven Prozesse auf dem Chip ablaufen und folglich nicht von außen zugänglich sind. Außerdem ist die Lösung in Form einer Chipkarte portabel, d. h., in einer unbekannten Umgebung (z. B. öffentliche HBCI-Kundensysteme) problemlos einsetzbar. Demgegenüber hat das Software-basierte-Verfahren den Vorteil, daß keine zusätzlichen Hardware-Kosten für Chipkartenleser am Endgerät entstehen. Die Mobilität kann innerhalb einer sicheren Umgebung durch Diskettentransfer erreicht werden. Während die deutschen Sparkassen auf die Chipkarten-Lösung setzen, präferieren die deutschen Privatbanken die Software-Lösung. Allgemein anerkanntes Ziel ist die Integration beider Ansätze in einer vom ZKA zertifizierten RSA-Chipkarte.

73 In Datex-J, dann T-Online umbennant.

74 OFX (Open Financial Exchange) ist der von Microsoft eingeführte und in Nordamerika etablierte Standard und wird derzeit für den Einsatz bei europäischen Banken definiert.

75 Zwißler, Sonja: Homebanking Computer Interface (HBCI), in: DuD Datenschutz und Datensicherheit, 1/1999, S. 45.

Die Kunden-Authentifikation gegenüber der Bank findet durch Eingabe eines Paßwortes statt. Das Paßwort wird lokal geprüft, verläßt also nicht das Kundensystem. Die Prüfung findet in der Chipkarte oder im Kunden-PC statt. Die Authentifikation eines HBCI-Servers findet nicht statt, was für eine sichere Verbindung zwischen beiden Partnern absolut unzureichend ist. Ein Angreifer kann Kundenaufträge zwar nicht ohne weiteres entschlüsseln und einsehen, aber auf dem Übertragungsweg zur Bank abfangen.

Zertifikate sind in HBCI bis heute noch nicht spezifiziert. Eine entsprechende Erweiterung der HBCI-Spezifikation ist aber zu erwarten und wird sich voraussichtlich am X.509-Standard orientieren. Zur Eigenentwicklung von HBCI-Client-Systemen steht eine HBCI-API für C, C++ und Java zur Verfügung.[76] Der Markt bietet inzwischen einige PC-Produkte an, die HBCI auf Windows-Plattformen ab Version 3.1 unterstützen (StarMoney, ZV-Light u. a.). Die meisten dieser Kundensysteme kommunizieren über T-Online. Für das sog. Browser-Banking sind Java-Applets bzw. ActiveX-Controls für die einzelnen Geschäftsvorfälle und ein Java-API für den HBCI-Kernel verfügbar.

Für die Entwicklung von HBCI-Server-Systemen ist die ebenfalls kostenlose Funktionsbibliothek HBCI-Kernel[77] verfügbar. Der HBCI-Kernel wird von der Sparkassenorganisation entwickelt und unterstützt die Protokolle T-Online und TCP/IP (HBCI-Port = 3000). Eine Firewall, die zwischen HBCI-Kunden- und HBCI-Banksystem plaziert ist, muß für den Zugang über Port 3000 durchlässig sein. Weil Schnittstellen zu Internet-Protokollen wie HTTP, MIME, SSL oder HTTPS in der aktuellen HBCI-Version 2.01 nicht spezifiziert sind, ist eine Web-Integration von HBCI noch nicht ohne weiteres möglich. Bereits produktive HBCI-Serversysteme laufen unter IBM-MVS, IBM-AIX und HP-UX mit den Datenbanken Oracle und Informix. HBCI-Server mit einer Anbindung an DB2 sind bis heute noch nicht realisiert.

Als Internet-Banking-Lösung mit Unterstützung des HBCI-V2.01-Standards wird X·HBCI Banking[78] von Brokat am Markt angeboten. X·HBCI basiert auf BROKAT Twister, einer CORBA/IIOP-basierten Software zur Bereitstellung sicherer, kundenspezifischer Electronic Services Delivery Lösungen. X·HBCI besteht aus den Komponenten

- Twister-Gateway,
- Twister HBCI Administration Tool (HTML-basiert),
- Twister-Accessoren,
- Twister-Services.

Das Twister HBCI-Gateway wandelt den Inhalt der HBCI-Nachrichten in CORBA/ IIOP-Nachrichten um, die anschließend über verschiedene Twister-Accessoren an beliebige Back-End-Systeme weitergereicht werden. Die Twister-Accessoren eröffnen via SQL einen einfachen Datenbankzugriff. Die Twister-Services bieten spezielle Funktionalitäten wie Naming, Logging, Load Balancing, Licensing und Reporting. Die Kommunikation zwischen den einzelnen Twister-Komponenten erfolgt CORBA/IIOP-konform und kann optional mit 128-Bit-SSL verschlüsselt werden. X·HBCI läuft auf allen gängigen Betriebssystem-Plattformen (u. a. Windows-NT, IBM-AIX, HP-UX).

76 http://www.bankverlag.de

77 Im Internet: http://www.hbci-kernel.de, 20.07.1999.

78 Vgl. BROKAT Informationssysteme GmbH (Hrsg.): X.HBCI Banking, Stuttgart: BROKAT 1998.

5.5 Bewertung der Sicherheitstechniken

Die Notwendigkeit, sensitive Daten beim Transport via Internet zu verschlüsseln, ist unbestritten. Dem wird auch von allen hier vorgestellten Sicherheits-Verfahren Rechnung getragen. Allerdings scheidet S-HTTP direkt aus, da das Verfahren inzwischen obsolet ist (siehe Kapitel 5.2).

Das Maß an Integrität und Vertraulichkeit der Daten wird bei der Verschlüsselung durch die verwendeten Schlüssellängen bestimmt; hierin unterscheiden sich die beschriebenen Sicherheitstechniken. SSL benutzt in der US-Exportversion 40-Bit-Schlüssel, also nur sog. schwache Verschlüsselung. Die größte Hürde, um mit SSL starke Verschlüsselung (128-Bit) zu realisieren, stellt die Kundenseite dar, denn die am stärksten verbreiteten Web-Browser Microsoft Internet Explorer und Netscape Navigator/Communicator sind amerikanische Produkte und beherrschen nur schwache Verschlüsselung. Mit „Fortify for Netscape“ kann man jedoch starke Verschlüsselung realisieren. HBCI dagegen arbeitet beim Chipkarten-Verfahren mit 128-Bit-Schlüsseln und beim Software-basierten-Verfahren mit 768-Bit-Schlüsseln, also prinzipiell mit starker Verschlüsselung.

Für die Sicherheit bezgl. *Authentizität und Verbindlichkeit* der Kommunikation sorgen die Verfahren zur Authentifizierung der Partner, in denen sich die beschriebenen Sicherheitstechniken ebenfalls unterschiedlich verhalten. Während sich bei SSL der Web-Server grundsätzlich gegenüber dem Client authentifiziert, tut dies der HBCI-Server nicht.

Die Informationsdienste der neuen Kernanwendung sind für einen HBCI-Server nicht nutzbar. Es müssen die HBCI-Services verwendet werden, die allerdings DB2 als BKM-Datenbank nicht unterstützen.

Sowohl SSL also auch HBCI sind auf Home-PCs lauffähig, die HBCI-Lösung ist jedoch (noch) nicht ausreichend auf Home-PCs portiert und ihr fehlt die Web-Integration. Es bleibt zu bedenken, daß sicherlich einige Bankengruppen neue HBCI-Client-Produkte unterstützen und fördern werden, um HBCI gerade im Marketing- und Servicebereich stärker für ihre Belange nutzen zu können. Eine kostenfreie Verteilung solcher Endbenutzer-Software an die BKM-Kunden könnte dem Problem der fehlenden Web-Integration begegnen. Bis heute gibt es solch ein umfassendes Client-Produkt jedoch nicht.

Der Sicherheitsgewinn durch bestehende Firewall-Lösungen (siehe Kapitel 6) bleibt bei Anwendung von SSL gewahrt. Die Firewall verweigert weiterhin allen externen IP-Adressen den Zugang zum BKM-Netz, die nicht ausdrücklich dazu autorisiert sind. Bei gültiger IP-Adresse reicht die Firewall die vom Client angeforderte Portnummer unbesehen an den Port 443 des SSL-Servers durch. Der SSL-Server kann die übertragenen Anmeldedaten entschlüsseln und schließlich dem Client den Zugang zum angeforderten Web-Service erlauben bzw. verweigern.

Das höchste Maß an Sicherheit bezüglich Authentizität und Verbindlichkeit der Kommunikation wird durch die Client- und Server-Authentifizierung mit Zertifikaten erreicht. Ein zertifizierter Server kann beispielsweise Client-Zertifikate einer bestimmten Certifying Authority oder Clients mit bestimmten Namen oder Zertifikate mit einer bestimmten Gültigkeitsdauer zulassen bzw. ablehnen. Client-Zertifikate erfordern allerdings auch den größten Aufwand bei der Integration und Administration. Die Erstaus-

gabe von Client-Zertifikaten kann über personalisierte Chipkarten oder per Diskette mit entsprechender Software erfolgen. Die Chipkarten-Lösungen sind noch nicht ausgereift. Software-Lösungen, die Zertifikate auf Disketten bereitstellen, sind zahlreich auf dem Markt vorhanden. Die Verwaltung der Zertifikate übernimmt primär die Certifying Authority, an deren Infrastruktur man sich zur Nutzung dieses Services anbinden kann. Innerhalb großer Unternehmen empfiehlt sich der zusätzliche Aufbau einer eigenen CA-Infrastruktur, um die Zertifikate z. B. mit Zugangs- und Zugriffsrechten für interne Dienste und Daten zu verknüpfen.

Ein Kunde kann sich bei SSL entweder mit X.509-Zertifikat oder auch nur mit Basic Authentication durch Kennung und Paßwort authentifizieren. Solange das Paßwort geheim bleibt, gilt die einfachere Variante per Basic Authentication bei Übertragung via SSL als hinreichend sicher. Zertifikate sind technisch neue Verfahren, die mitunter zurückhaltend angenommen werden, noch zurückhaltender aber verwendet werden.[79] Die Anwendung von SSL ohne Client-Zertifikate erfordert keine spezielle Konfiguration des Clients. SSL ist umfassend, arbeitet stabil und sicher und erfüllt die Ziel-Anforderungen aus Kapitel 4. Zudem breitet sich SSL schnell als internationaler Standard aus und wird demzufolge zukunftssicher sein.

Für die BKM kann daher an dieser Stelle die Empfehlung ausgesprochen werden, SSL-basierte Verfahren zur Anbindung und Absicherung des KKIS einzusetzen.

6 Anbindung und Absicherung des KKIS

6.1 Anbindung des aktuellen Web-Auftritts

Der Web-Server der BKM befindet sich in einem durch die Firewall abgetrennten Teilnetz, der sogenannten Demilitarisierten Zone (DMZ). Die Firewall schützt auch das BKM-interne-Netz (trusted Network) vor Bedrohungen aus dem Internet. Abb. 9 zeigt den Ist-Zustand vor der KKIS-Implementation.

6.2 Anbindung des KKIS an die neue Kernanwendung

Basierend auf der Entscheidung das KKIS mit SSL über das Internet zu realisieren, muß zunächst ein SSL-fähiger Web-Server eingerichtet werden. Damit ist dann der sichere Austausch von Nachrichten zwischen Web-Client und Web-Server möglich.

Mit dem ersten Aufruf von Informationen über das KKIS muß sich der Kunde als nutzungsberechtigte Person identifizieren. Als adäquates Mittel kommen hier Kennung und Paßwort zum Einsatz (siehe Kapitel 3.4.1). Dazu muß der Kunde in den Besitz dieser Informationen gelangen. Beispielsweise könnte die BKM jedem Kunden auf Anfrage via Post oder per Call-Center, Kennung und Paßwort zukommen lassen. Nach erfolgter Authentifikation und Autorisierung hat der Kunde nun Zugriff auf die vom KKIS zur

79 Runge, Alexander: Elektronische Unterschriften. Version 1.1 in: Arbeitsbericht / Bericht IM HSG/CCEM 43, 07/97, Hrsg.: Institut für Wirtschaftsinformatik: St. Gallen 1997, Online im Internet: http://www.businessmedia.org/netacademy/publications.nsf/all_pk/208, 27.07.1999.

Verfügung gestellten Services (siehe Kapitel 3.5). Die Zugriffsrechte sind an die Kunden-Identität gebunden und das KKIS gibt die zur Übertragung angeforderten Daten in Abhängigkeit dieser Zugriffsrechte weiter.

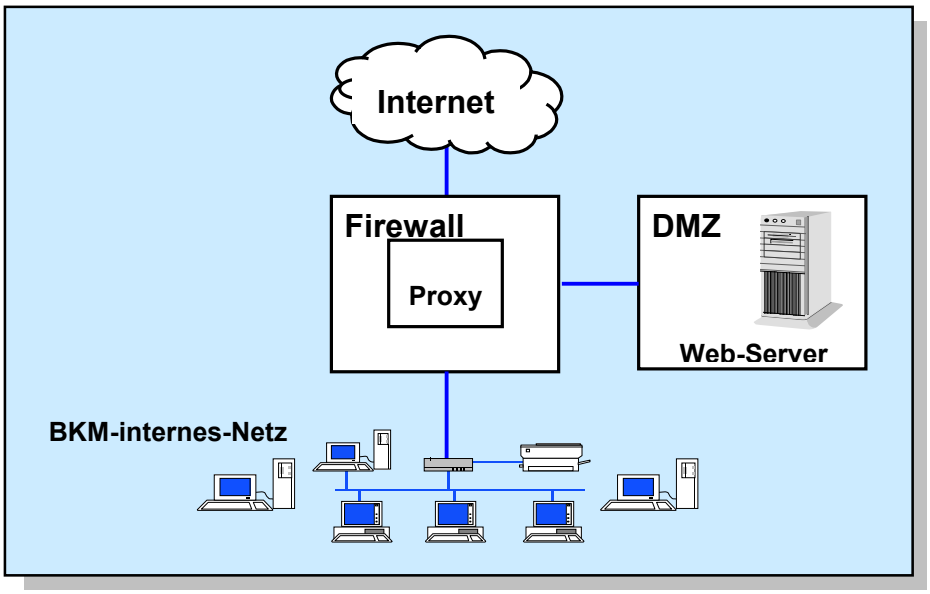

Abb. 9: DMZ-Architektur

Die neue Kernanwendung wird unter anderem Geschäftsprozesse für bestimmte Informationsdienste bereitstellen wie bspw. eine Vertragshistorie oder Kontoübersicht. Diese BKM-internen Anwendungen werden im Rahmen des KKIS über einen Web-Server unter Windows NT für den Zugriff durch Kunden über das Internet bereitgestellt. Der Web-Server spielt dabei im BKM-internen Netz die Rolle eines „normalen“ NT-Clients.

Die variablen Daten in einer vom Kunden ausgefüllten HTML-Anfrage-Seite werden vom Web-Server mit Hilfe eines Schnittstellenprogramms (z. B. ein Java Servlet) an einen Informationsdienst der neuen Kernanwendung weitergereicht. Der damit angesprochene Geschäftsprozeß fordert die relevanten Business-Objects an und gibt sie an das Schnittstellenprogramm zur Aufbereitung in HTML-Antwort-Seiten für den Kunden zurück (siehe Abb. 10).

6.3 Monitoring der Kundenzugriffe

Die Basis eines Online-Monitorings sind Nutzungsdaten, die aus einer Präsenz im Internet resultieren. Durch die Identifikation von Nutzungsvorgängen lassen sich Aussagen über das Verhalten und das Navigieren innerhalb einer Web Site machen. Grundsätzlich ist die Verwendung der Monitoring-Ergebnisse in unterschiedlichen Unternehmensbereichen möglich. Das Sammeln und Auswerten solcher Informationen ermöglicht beispielsweise einen effizienteren Einsatz zielgruppengerichteter Werbung, gezielte Maßnahmen zur Steigerung der Kundenzufriedenheit sowie die Entwicklung

nachfrageorientierter Produkte und Serviceleistungen.[80] Vor allem zur Optimierung des KKIS lassen sich die aus dem Monitoring gewonnen Erkenntnisse nutzen.

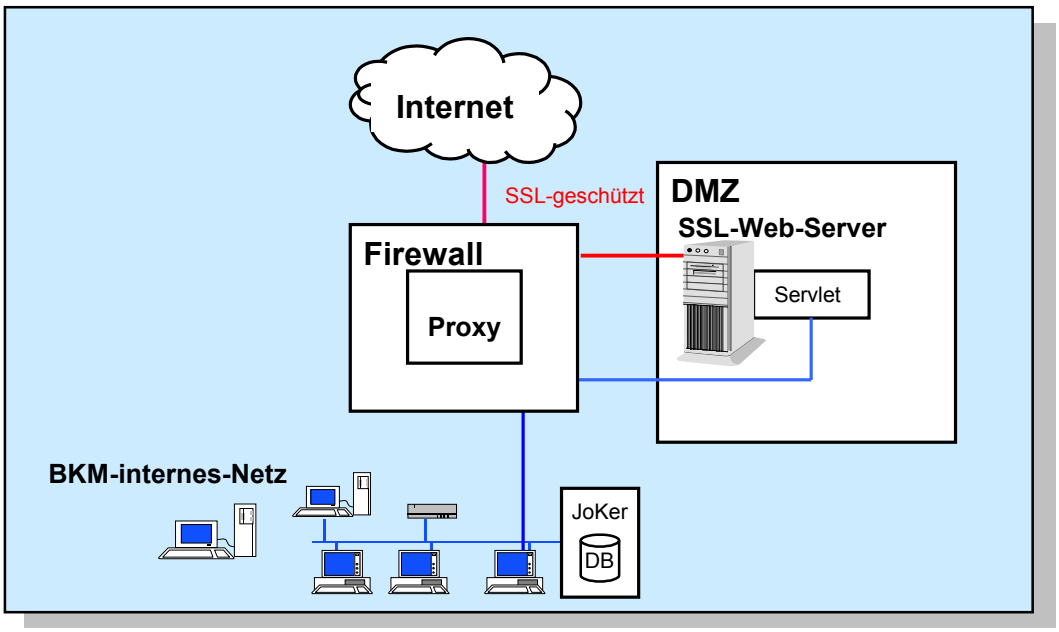

Abb. 10: Datenzugriff über SSL-geschützten Web-Server

Die mit dem Monitoring gesammelten Nutzungsdaten einer statischen Web Site werden üblicherweise in Logfiles gesammelt. Durch die Analyse dieser Logfiles besteht jedoch keine Möglichkeit, den einzelnen Besucher einer Web Site zu identifizieren und wiederzuerkennen. Lösungsansatz für dieses Problem sind die Browserregistrierung durch sogenannte „Cookies“ und die bewußte Registrierung des Kunden. Letzteres wird durch die geschilderte SSL-Lösung möglich, womit die tragfähige Grundlage für ein Online-Monitoring des BKM-Service-Bereichs gegeben ist.

Um die Frequenz und Art von Benutzeranfragen aus dem Internet beobachten und aus diesen Beobachtungen bestimmte Maßnahmen ableiten zu können, ist es sinnvoll, Zugriffe von außen auf das BKM-interne Netz zu protokollieren und statistisch auszuwerten. Zu diesem Zweck ist der KKIS-Server mit zusätzlicher Software auszustatten, deren Funktionalität im einzelnen von der BKM vorzugeben ist. In jedem Fall muß diese Software gewährleisten, daß keine personenbezogenen Nutzdaten wie Kontostände o. ä. in die Protokollierung mit einfließen und dadurch für Unbefugte einsehbar werden.

Bei einem Web-Server, der auf Kundeninformationen der neuen Kernanwendung zugreift, kann die Protokollierung durch die Workflow-Komponente von JoKer erfolgen.

80 Vgl. Guba, Andreas; Gebert, Oliver: Online-Monitoring – Gewinnung und Verwertung von Online-Daten, in: Arbeitspapiere WI, Nr. 8/1998, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1998.

7 Abschließende Betrachtung und Ausblick

Nur die Betreiber von Web Sites, die gewährleisten können, daß Daten und Transaktionen vertrauenswürdig, verläßlich und konsistent sind, werden auf lange Sicht das Vertrauen von Kunden und Partnern gewinnen und den damit verbundenen strategischen Geschäftsvorteil für sich realisieren können.

Für einen Teil der Problembereiche hat die vorliegende Arbeit Konzeptvorschläge bereitgestellt. Der Leser dieser Arbeit muß dabei berücksichtigen, daß aufgrund der kurzen technologischen Innovationszyklen die Sicherheitsrisiken und somit auch die Verfahren zu deren Überwindung einem ständigen Wandel unterworfen sind; die Arbeit kann insofern nur den zum Erscheinungszeitpunkt aktuellen Fokus reflektieren.

Vor diesem Hintergrund ist der Inhalt von Kapitel 6 als pragmatischer Vorschlag zur Anbindung und Absicherung des KKIS zu interpretieren. Die SSL-Basis erlaubt es, mit vertretbarem Aufwand, den BKM-Kunden innovative und adäquat gesicherte Services über das Internet zur Verfügung zu stellen. Kritisch zusehen bleibt die „schwache“ 40-Bit-Verschlüsselung der beim Kunden verbreiteten Browser, obgleich selbst „schwache“ Verschlüsselung nicht trivial zu knacken ist. Dieser „schwachen“ Verschlüsselung kann man im Falle des Netscape-Browsers jedoch mit „Fortify for Netscape“ begegnen.

Es bleibt abschließend zu bemerken, daß obwohl die Verschlüsselungsverfahren ständig verbessert werden, immer leistungsfähigere Hard- und Software die Sicherheit der bekannten symmetrischen und asymmetrischen Verschlüsselungsverfahren zunehmend in Frage stellt. Dem Wettbewerb zwischen Schlüssellänge und Taktrate soll ein neuer, noch im Forschungsstadium befindlicher Ansatz Einhalt gebieten. Wissenschaftler versprechen sich von der Anwendung sogenannter elliptischer Kurven in Public-Key-Verfahren eine Steigerung der mathematischen Komplexität, die es einem Außenstehenden nahezu unmöglich machen soll, mit den bekannten Brute-Force-Attacken den Schlüssel herauszufinden.[81] Eine 160-Bit-Verschlüsselung mit elliptischen Kurven könnte eine vergleichbare Schutzwirkung wie ein 1024-Bit-RSA-Schlüssel aufweisen.[82]

Forschung, Politik und Wirtschaft müssen gleichermaßen Ihren Beitrag dazu leisten, daß aus dem Internet ein sicherer elektronischer Marktplatz wird. Nach Verabschiedung des Signaturgesetzes und dem zugehörigen Maßnahmenkatalog liegt es nun an der Industrie, den Aufbau der Public-Key- und Zertifikats-Infrastruktur voranzutreiben. Die Mehrzahl der Nutzer hat keine Vorstellung von den potentiellen Risiken und benötigt deshalb einfache und transparente Schutzmechanismen, die den gesicherten Umgang auch ohne ein tiefgehendes Verständnis der Technik ermöglichen. Dies führt zwangsläufig zu neuen Endgeräten, bei denen nicht nur reine Softwarelösungen, sondern auch Hardware-Basierte Konzepte wie Chipkarten eine wichtige Rolle spielen werden.

81 Vgl. Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, a. a. O., S. 548 und Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, a. a. O, S. 107-113.

82 Vgl. Menezes, A. J.: Elliptic Curve Public Key Cryptosystems, Norwell, MA: Kluwer Academic Publishers 1993.

Literaturverzeichnis

Afif, Noelani Maria: Digitale Signatur im Test, in: Information Week, 16/1999, S. 10.

Afif, Noelani Maria: Digitale Signatur schafft Sicherheit, in: Information Week, 14/1999, S. 16.

Afif, Noelani Maria: Sichere Abrechnung im Internet-Handel, in: Information Week, 19/1998, S. 12.

Afif, Noelani Maria; Fill, Christian: Sicherheit zahlt sich aus, in: Information Week, 11/1999, S. 18-19.

Bausparkasse Mainz AG (Hrsg.): Adressänderung, Online im Internet: http://www.bkm.de/2/998.htm, 22.07.1999.

SIX SIGMA EDV-Konzepte Kurt Haubner (Hrsg.): HBCI–Kompendium: der Einstieg in die neue Welt des Homebanking, München 1999.

Bausparkasse Mainz AG (Hrsg.): Bericht über das Geschäftsjahr 1998, Mainz 1999.

Bausparkasse Mainz AG (Hrsg.): Das Projekt, Online im Internet: http://www.bkm-dv.de/Framesets/229.htm, 12.06.1999.

Bausparkasse Mainz AG (Hrsg.): Die Bausparkasse Mainz AG, Online im Internet: http://www.bkm-dv.de/Framesets/230.htm, 12.06.1999.

Benloh, J.; Lampson, B.; Simon, D.;Spies, T.; Yee, B.: The Private Communications Technology Protocol, Online im Internet: http://www.lne.com/ericm/pct.html, 13.06.1999.

BROKAT Informationssysteme GmbH (Hrsg.): X.HBCI Banking, Stuttgart: BROKAT 1998.

Federrath, Hannes: Schlüsselgenerierung in Trust Centern?: Einseitig sicher ist nicht sicher genug, in: DuD Datenschutz und Datensicherheit, 2/1997, S. 98-99.

Fill, Christian: IT-Security; Zwischen Panik und Perfektion, in: Information Week,. 19/1998, S. 38-45.

Fill, Christian: Security-Tools unter einem Dach vereint, in: Information Week, 3/1999, S. 40.

Garfinkel, Simon; Spafford, Gene: Web Security & Commerce, Köln et al.: O´Reilley & Associates, Inc. 1997.

Gehlen, Susanne; Nobis, Thomas: Web der offenen Tür, Die größten Sicherheitslöcher im Internet, in: Computerwoche Spezial, 4/1998, S. 12-13.

Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, New York et al.: Wiley Computer Publishing 1998.

Globig, Klaus; Eiermann, Helmut: Datenschutz bei Internet-Angeboten, in: DuD Datenschutz und Datensicherheit, 9/1998, S. 514-517.

Görtz, Horst; Stolp, Jutta: Informationssicherheit in Unternehmen, Bonn, Reading , Mass.: Addison-Wesley-Longman, 1999.

Graefen, Rainer; Reuß, Annette: Verzeichnisdienste: Hoffnung für gestreßte Administratoren, in: Information Week, 3/1999, S. 38 f.

Guba, Andreas; Gebert, Oliver: Online-Monitoring - Gewinnung und Verwertung von Online-Daten, in: Arbeitspapiere WI, Nr. 8/1998, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1998.

Hammer, Volker: Wie nennen wir Infrastrukturen für die Schlüsselverwaltung, in: DuD Datenschutz und Datensicherheit, 2/1998, S. 91-92.

Hortmann, Michael: Wie sicher ist die PIN?: Zum Scheckkarten-Urteil des OLG Hamm, in: DuD Datenschutz und Datensicherheit, 9/1997, S. 532-534.

Hövel, Jörg auf dem: Nur ein bißchen Verschlüsseln ist schwierg: Kryptographie und ihre Beschränkung / Amerikanische Untersuchungen, in: Frankfurter Allgemeine Zeitung, 17.02.1998, S. T5.

Jörn, Fritz: Trotz aller Verschlüsselung muß man Vertrauen haben: Das asymmetrische Chiffrieren und die Rolle des Trust Center, in: Frankfurter Allgemeine Zeitung, 17.02.1998, S. T5.

Kerckhoffs, A.: La Cryptographie Militaire. Librairie Militaire de L. Baudon & Cie. 1883.

Kossel, Axel: Ein waches Auge, in: c´t Magazin für Computertechnik, 3/99, S. 142-145.

Krempel, Stefan: Alles auf eine Karte, in: Computerwoche Spezial, 4/1998, S. 54

Krempel, Stefan; Schmidt, Michael; Kuri, Jürgen: Lange Ohren, in: c´t Magazin für Computertechnik, 4/99, S. 174-181.

Kuri, Jürgen: Privatissimo, in: c´t Magazin für Computertechnik, 4/1999, S. 190-194.

Kyas, Othmar: Sicherheit im Internet, 2. Aufl., Bonn: Internat. MITP-Verlag 1998.

Luckhardt, Norbert: Büchse der Pandora, in: c´t Magazin für Computertechnik, 8/99, S. 17.

Luckhardt, Norbert: Deutscher Support für Krypto-Patch, Online im Internet: http://www.heise.de/ newsticker/data/nl-13.01.99-000/, 13.06.1999.

Luckhardt, Norbert: Deutsche Zertifikate in Netscape 4.5, Online im Internet: http://www.heise.de/newsticker/data/nl-27.10.98-000/, 07.07.1999.

Luckhardt, Norbert: Hunderte Online-Shops verraten Kundendaten, in: c´t Magazin für Computertechnik, 10/1999, S. 22.

Luckhardt, Norbert: Qnf jne rvasnpu, tryy?, Kryptologische Begriffe und Verfahren, in: c´t Magazin für Computertechnik, 12/96 S. 110.

Luckhardt, Norbert: Weitere Web-Hacks in Deutschland, Online im Internet: http://www.heise.de/newsticker/data/nl-08.10.98-000/, 08.10.1998.

Mack, Holger: Sicherheitsaspektevon Java-Applets, in: DuD Datenschutz und Datensicherheit, 9/1998, S. 509-513.

Menezes, A. J.: Elliptic Curve Public Key Cryptosystems, Norwell, MA: Kluwer Academic Publishers 1993.

Nehl, Roland: Schlüsselgenerierung in Trust Centern?: Vertrauen durch Trust Center, in: DuD Datenschutz und Datensicherheit, 2/1997, S. 100-101.

Netscape Communications (Hrsg.): SSL 3.0 Specification, Online im Internet: http://home.netscape.com/ eng/ssl3/ssl-toc.html, 12.07.1999.

Nusser, Stefan: Sicherheitskonzepte im WWW, Berlin et al.: Springer 1998.

o. V.: Anforderungen zur informationtechnischen Sicherheit bei Chipkarten: Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in: DuD Datenschutz und Datensicherheit, 5/1997, S. 254-261.

o. V.: Bankbetriebslehre, Bank-Enzyklopädie Bd. 2, Wiesbaden Dr. Gabler-Verlag 1975, S. 504.

o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, CD-ROM, Bonn, 1998.

o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, Online im Internet: http://www.bsi.de/gshb/deutsch/menue.htm, 08.07.1999.

o. V.: Bundesamt für Sicherheit in der Informationstechnik: Maßnahmenkatalog für digitale Signaturen. Entwurf (1997) , Online im Internet: http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/download/ kat.pdf, 12.01.1999.

o. V.: Homepage 2600, Online im Internet: http://www.2600.com/hacked_pages, 21.05.1999.

o. V.: Internet-Technik ist kein Sicherheitsrisiko mehr, in: Computer Zeitung, 18/1999, S. 29.

o. V.: Kommunikation im Internet bestimmt Erfolg, in: Frankfurter Allgemeine Zeitung, 05.03.1998, S. 27.

Oppliger, Rolf: IT-Sicherheit: Grundlagen und Umsetzung in der Praxis, Braunschweig, Wiesbaden: Verlag Vieweg 1997.

Oppliger, Rolf: Sicherheitsprotokolle für das Internet, in: DuD Datenschutz und Datensicherheit, 12/1997, S. 686-690.

Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg: dpunkt-Verlag 1998.

Rivest, R. L.: The MD4 Message Digest Algorithm, RFC 1320, April 1992.

Rivest, R. L.: The MD5 Message Digest Algorithm, RFC 1321, April 1992.

Runge, Alexander: Elektronische Unterschriften. Version 1.1 in: Arbeitsbericht / Bericht IM HSG/CCEM 43, 07/97, Hrsg.: Institut für Wirtschaftsinformatik: St. Gallen 1997, Online im Internet: http://www.businessmedia.org/netacademy/publications.nsf/all_pk/208, 27.07.1999.

Schierenbeck, Henner: Grundzüge der Betriebswirtschaftslehre, 12., überarb. Aufl., München et al.: Oldenbourg 1995.

Schmeh, Klaus: Safer Net: Kryptografie im Internet und Intranet, Heidelberg: dpunkt-Verlag 1998.

Schneier, Bruce: Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C, 1., korrigierter Nachdruck, Bonn et al.: Addison-Wesley 1997.

Scholvin-Wulff, Barbara: E-Commerce-Berater haben für Mittelständler wenig übrig, in Computerzeitung, 06.08.1998, S. 18.

Smith, Richard E.: Internet-Kryptographie, Bonn: Addison-Wesley-Longman 1998.

Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 8., vollst. überarb. und erw. Aufl., Berlin et al.: Springer 1997.

Stark, T.: Encryption for a small Planet, in: Byte, April/97.

Strobel, Stefan: Nebeneingang – Firewalls nicht nur für den Internet-Anschluß, in: iX, 10/98, S. 132-137.

Weck, Gerhard: Key Recovery - Möglichkeiten und Risiken, in: Informatik-Spektrum, 21/1998, S. 147-158.

Weck, Gerhard; Gerbisch, Sandra Ines: Gefahren lauern überall: IT-Sicherheits-konzepte helfen Risiken mindern, in: IT-Management, 03/1999, S. 48-53.

Wirtz, Brigitte: Biometrische Verfahren: Überblick, Evaluierung und aktuelle Themen, in: DuD Datenschutz und Datensicherheit, 3/1999, S. 129-134.

Wohlmacher, Petra; Fox, Dirk: Hardwaresicherheit von Smartcards, in: DuD Datenschutz und Datensicherheit, 5/1997, S. 260-264.

Woll, A.: Wirtschaftlexikon, 7., überarb. Aufl., München et al.: Oldenbourg 1993, S. 67.

Zwißler, Sonja: Homebanking Computer Interface (HBCI), in: DuD Datenschutz und Datensicherheit, 1/1999, S. 45-47.

Bisher erschienen

Stand: Dezember 2000 – Den aktuellen Stand der Reihe erfahren Sie über unsere Web Site unter http//wi.uni-giessen.de

Nr. 1/1996	Grundlagen des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 2/1996	Wettbewerbs- und Organisationsrelevanz des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 3/1996	Realisierungsaspekte des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 4/1996	Der Geschäftsprozeß als formaler Prozeß - Definition, Eigenschaften, Arten	Schwickert/Fischer
Nr. 5/1996	Manuelle und elektronische Vorgangssteuerung	Schwickert/Rey
Nr. 6/1996	Das Internet im Unternehmen - Neue Chancen und Risiken	Schwickert/Ramp
Nr. 7/1996	HTML und Java im World Wide Web	Gröning/Schwickert
Nr. 8/1996	Electronic-Payment-Systeme im Internet	Schwickert/Franke
Nr. 9/1996	Von der Prozeßorientierung zum Workflow-Management - Teil 1: Grundgedanken, Kernelemente, Kritik	Maurer
Nr. 10/1996	Von der Prozeßorientierung zum Workflow- Management - Teil 2: Prozeßmanagement und Workfflow	Maurer
Nr. 11/1996	Informationelle Unhygiene im Internet	Schwickert/Dietrich/Klein
Nr. 12/1996	Towards the theory of Virtual Organisations: A description of their formation and figure	Appel/Behr
Nr. 1/1997	Der Wandel von der DV-Abteilung zum IT-Profitcenter: Mehr als eine Umorganisation	Kargl
Nr. 2/1997	Der Online-Markt - Abgrenzung, Bestandteile, Kenngrößen	Schwickert/Pörtner
Nr. 3/1997	Netzwerkmanagement, OSI Framework und Internet SNMP	Klein/Schwickert
Nr. 4/1997	Künstliche Neuronale Netze - Einordnung, Klassifikation und Abgrenzung aus betriebswirtschaftlicher Sicht	Strecker/Schwickert
Nr. 5/1997	Sachzielintegration bei Prozeßgestaltungsmaßnahmen	Delnef
Nr. 6/1997	HTML, Java, ActiveX - Strukturen und Zusammenhänge	Schwickert/Dandl
Nr. 7/1997	Lotus Notes als Plattform für die Informationsversorgung von Beratungsunternehmen	Appel/Schwaab
Nr. 8/1997	Web Site Engineering - Modelltheoretische und methodische Erfahrungen aus der Praxis	Schwickert
Nr. 9/1997	Kritische Anmerkungen zur Prozeßorientierung	Maurer/Schwickert
Nr. 10/1997	Künstliche Neuronale Netze - Aufbau und Funktionsweise	Strecker
Nr. 11/1997	Workflow-Management-Systeme in virtuellen Unternehmen	Maurer/Schramke
Nr. 12/1997	CORBA-basierte Workflow-Architekturen - Die objektorientierte Kernanwendung der Bausparkasse Mainz AG	Maurer
Nr. 1/1998	Ökonomische Analyse Elektronischer Märkte	Steyer
Nr. 2/1998	Demokratiepolitische Potentiale des Internet in Deutschland	Muzic/Schwickert
Nr. 3/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 1)	Delnef
Nr. 4/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 2)	Delnef
Nr. 5/1998	Betriebswirtschaftlich-organisatorische Aspekte der Telearbeit	Polak
Nr. 6/1998	Das Controlling des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 7/1998	Eine kritische Beurteilung des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 8/1998	Online-Monitoring - Gewinnung und Verwertung von Online-Daten	Guba/Gebert
Nr. 9/1998	GUI - Graphical User Interface	Maul
Nr. 10/1998	Institutionenökonomische Grundlagen und Implikationen für Electronic Business	Schwickert
Nr. 11/1998	Zur Charakterisierung des Konstrukts “Web Site”	Schwickert
Nr. 12/1998	Web Site Engineering - Ein Komponentenmodell	Schwickert
Nr. 1/1999	Requirements Engineering im Web Site Engineering – Einordnung und Grundlagen	Schwickert/Wild
Nr. 2/1999	Electronic Commerce auf lokalen Märkten	Schwickert/Lüders
Nr. 3/1999	Intranet-basiertes Workgroup Computing	Kunow/Schwickert
Nr. 4/1999	Web-Portale: Stand und Entwicklungstendenzen	Schumacher/Schwickert
Nr. 5/1999	Web Site Security	Schwickert/Häusler
Nr. 6/1999	Wissensmanagement - Grundlagen und IT-Instrumentarium	Gaßen
Nr. 7/1999	Web Site Controlling	Schwickert/Beiser
Nr. 8/1999	Web Site Promotion	Schwickert/Arnold
Nr. 9/1999	Dokumenten-Management-Systeme – Eine Einführung	Dandl
Nr. 10/1999	Sicherheit von eBusiness-Anwendungen – Eine Fallstudie	Harper/Schwickert
Nr. 11/1999	Innovative Führungsinstrumente für die Informationsverarbeitung	Jäger-Goy
Nr. 12/1999	Objektorientierte Prozeßmodellierung mit der UML und EPK	Dandl
Nr. 1/2000	Total Cost of Ownership (TCO) – Ein Überblick	Wild/Herges
Nr. 2/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 1: XML-Grundlagen	Franke/Sulzbach
Nr. 3/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 2: Der Einsatz im Unternehmen	Franke/Sulzbach
Nr. 4/2000	Web-Site-spezifisches Requirements Engineering – Ein Formalisierungsansatz	Wild/Schwickert
Nr. 5/2000	Elektronische Marktplätze – Formen, Beteiligte, Zutrittsbarrieren	Schwickert/Pfeiffer
Nr. 6/2000	Web Site Monitoring – Teil 1: Einordnung, Handlungsebenen, Adressaten	Schwickert/Wendt
Nr. 7/2000	Web Site Monitoring – Teil 2: Datenquellen, Web-Logfile-Analyse, Logfile-Analyzer	Schwickert/Wendt
Nr. 8/2000	Controlling-Kennzahlen für Web Sites	Schwickert/Wendt
Nr. 9/2000	eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen	Schwickert/Ostheimer/Franke

Bestellung (bitte kopieren, ausfüllen, zusenden/zufaxen)

Adressat:

Professur für BWL und Wirtschaftsinformatik
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefax: (0 641) 99-22619

Hiermit bestelle ich gegen Rechnung die angegebenen Arbeitspapiere zu einem Kostenbeitrag von DM 10,- pro Exemplar (MwSt. entfällt) zzgl. DM 5,- Versandkosten pro Sendung.

Nr.	An
1/1996	
2/1996	
3/1996	
4/1996	
5/1996	
6/1996	
7/1996	
8/1996	
9/1996	
10/1996	
11/1996	
12/1996	

Nr.	An
1/1997	
2/1997	
3/1997	
4/1997	
5/1997	
6/1997	
7/1997	
8/1997	
9/1997	
10/1997	
11/1997	
12/1997	

Nr.	Anz
1/1998	
2/1998	
3/1998	
4/1998	
5/1998	
6/1998	
7/1998	
8/1998	
9/1998	
10/1998	
11/1998	
12/1998	

Nr.	Anz
1/1999	
2/1999	
3/1999	
4/1999	
5/1999	
6/1999	
7/1999	
8/1999	
9/1999	
10/1999	
11/1999	
12/1999	

Nr.	Anz
1/2000	
2/2000	
3/2000	
4/2000	
5/2000	
6/2000	
7/2000	
8/2000	
9/2000	

Absender:

_____
Organisation

_____
Abteilung

_____
Nachname, Vorname

_____
Straße

_____
Plz/Ort

_____
Telefon Telefax eMail

_____
Ort, Datum Unterschrift