

Arbeitspapier

"Datenschutzfreundliche Technologien"

In der Arbeitsgruppe haben mitgewirkt:

Walter Ernestus (Der Bundesbeauftragte für den Datenschutz), Dieter J. Ermer (Federführung) (Der Bayerische Landesbeauftragte für den Datenschutz), Dr. Martin Hube (Der Niedersächsische Landesbeauftragte für den Datenschutz), Marit Köhntopp (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Dr. Michael Knorr (Der Thüringer Landesbeauftragte für den Datenschutz), Dr. Gisela Quiring-Kock (Der Hessische Datenschutzbeauftragte), Dr. Uwe Schläger (Der Hamburgische Datenschutzbeauftragte), Gabriel Schulz (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern).

Wir danken Frau Sottong-Micas (Europäische Kommission, DG XV) und Herrn Weinand (Bundesamt für Sicherheit in der Informationstechnik) für ihre Mitarbeit.

| | |
|---|-----------|
| 1. EINLEITUNG..... | 3 |
| 2. NOTWENDIGKEIT FÜR DATENSCHUTZ DURCH TECHNIK..... | 3 |
| 2.1 RECHTLICHE FORDERUNGEN UND ENTWICKLUNGEN | 3 |
| 2.2 GRUNDLEGENDE BETRACHTUNG VON INFORMATIONSSYSTEMEN | 4 |
| 3. ANONYMISIERUNG..... | 5 |
| 4. PSEUDONYMISIERUNG..... | 5 |
| 4.1 SELBSTGENERIERTE PSEUDONYME | 6 |
| 4.2 REFERENZ-PSEUDONYME | 7 |
| 4.3 EINWEG-PSEUDONYME..... | 7 |
| 5. REALISIERUNGSHILFEN..... | 8 |
| 5.1 HASHFUNKTIONEN | 8 |
| 5.2 DIGITALE SIGNATUREN | 8 |
| 5.3 (SIGNATURSCHLÜSSEL-)ZERTIFIKAT | 8 |
| 5.4 BLINDE DIGITALE SIGNATUR | 8 |
| 5.5 BIOMETRISCHE VERFAHREN | 9 |
| 5.6 VERTRAUENSSTELLEN..... | 9 |
| 5.7 DER IDENTITY PROTECTOR..... | 10 |
| 6. ZUSAMMENFASSUNG UND HANDLUNGSEMPFEHLUNG | 11 |
| ANLAGE 1, LITERATURVERZEICHNIS | |
| ANLAGE 2, ANWENDUNGSMÖGLICHKEITEN UND EINSATZFELDER | |

1. Einleitung

Die Computertechnologie ist in alle Lebensbereiche eingedrungen und breitet sich mehr und mehr aus. Beim Einkaufen, Zahlen, Buchen und Reservieren mittels bequemer Chip- oder Magnetstreifenkarten, bei der Kommunikation mittels digitaler Netze, bei Arztbesuchen mit Krankenversichertenkarten oder evtl. zukünftig mit Patientenkarten, auch durch Teilnahme an Online-Diensten sowie an nationalen und internationalen Netzwerken fallen eine Fülle von Einzeldaten über den Nutzer an. Diese elektronischen Spuren sind geeignet, persönliche Profile über den Einzelnen hinsichtlich seines Verhaltens zu bilden.

Immer mehr Bürger benutzen diese Technologie. Doch nicht zuletzt aufgrund der Komplexität und der mangelnden Transparenz von Systemen der modernen Informations- und Kommunikationstechnik (IuK-Technik) für die Nutzer fehlen diesen in der Regel Kenntnis und Kontrolle über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der über sie erhobenen und gespeicherten Daten.

Der Schutz der Privatheit des Einzelnen wird bei Nutzung dieser Systeme bisher vorwiegend dadurch angestrebt, daß der Zugang zu den erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten mittels technischer und organisatorischer Maßnahmen beschränkt wird. Der Schutz der Privatheit des Einzelnen hängt somit lediglich von der Wirksamkeit der üblichen Sicherheitsmaßnahmen und der Gewissenhaftigkeit ab, mit der sie durchgeführt werden. Mit diesen Sicherheitsmaßnahmen werden nur die klassischen Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit der gespeicherten Daten verfolgt.

Es wächst die Erkenntnis, daß der zunehmenden Gefährdung der Privatheit des Einzelnen nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten wirksam begegnet werden kann. Die Nutzung von IuK-Technik durch natürliche Personen wird demzufolge auch zukünftig nur dann den Ansprüchen der Datenschutzfreundlichkeit gerecht, wenn sie nach dem Prinzip der **Datensparsamkeit** erfolgt, wobei so wenig personenbezogene Daten wie möglich erhoben, gespeichert und verarbeitet werden. **Datenvermeidung** ist die stets anzustrebende Form der Datensparsamkeit. In diesem Fall werden bei der Nutzung von IuK-Systemen keine personenbezogenen Daten erhoben, gespeichert und verarbeitet, die Nutzung der IuK-Systeme erfolgt also anonym. Inhaltlich sind diese Forderungen Bestandteil des in den Datenschutzgesetzen des Bundes und der Länder festgelegten Grundsatzes der Erforderlichkeit, der auch schon bisher bei der Ausgestaltung der IuK-Technik zu beachten war, allerdings mit der technischen Entwicklung zunehmende Bedeutung gewinnt.

Anhand von Betrachtungen konkreter Beispiele aus dem Medienbereich, dem elektronischen Zahlungsverkehr, dem Gesundheitsbereich, der Telekommunikation sowie aus den Bereichen Transport und Verkehr werden in der Anlage die in diesen Projekten gewählten Ansätze und Bemühungen zur Verwendung datenschutzfreundlicher Technologien aufgezeigt. Es werden Empfehlungen in allgemeiner Form und für den jeweiligen Bereich gegeben.

2. Notwendigkeit für Datenschutz durch Technik

2.1 Rechtliche Forderungen und Entwicklungen

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil – am Beispiel der Statistik – den Anspruch auf Anonymisierung anerkannt. Gemäß der bekannten Auffassung des Bundesverfassungsgerichts heißt es dort: "Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – ... die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung" (BVerfGE 65, 1-49-). In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: "Das Recht auf informationelle Selbstbestimmung schützt ... davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden" (BGH AfP 1994, 306-307-).

Auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, hat das Thema Anonymisierung aufgegriffen. Der Rat führt in Kap. 2.5 über Datenschutz folgendes aus: "Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern". Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über "Deutschlands Weg in die Informationsgesellschaft" wieder [BD776].

Der Grundsatz der Datenvermeidung ist auch im Informations- und Kommunikationsdienste-Gesetz (IuKDG), dort in Art. 2 Teledienstedatenschutzgesetz (TDDSG), und im Mediendienste-Staatsvertrag [MDSStV] enthalten. Danach haben Anbieter von Tele- bzw. Mediendiensten den Nutzern die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit dies technisch möglich und zumutbar ist [IuKDG].

Die europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr [95/46/EG] enthält den Grundsatz, daß eine Verarbeitung personenbezogener Daten nur stattfinden darf, soweit sie im Hinblick auf bestimmte und festgelegte Zwecke notwendig ist. Sie geht deshalb auch von dem Prinzip aus, daß das Recht auf Privatsphäre und Selbstbestimmung dadurch am wirksamsten geschützt wird, daß möglichst keine personenbezogenen Daten erhoben werden. Im Hinblick auf die Umsetzung dieses Grundsatzes fördert die Europäische Kommission die Entwicklung und Anwendung datenschutzfreundlicher Technologien, insbesondere im Rahmen des elektronischen Handels, sowie beispielsweise die Möglichkeit anonymen Zugangs zu Netzen und anonyme Zahlungsweisen [KOM97].

2.2 Grundlegende Betrachtung von Informationssystemen

Betrachtet man traditionelle informationsverarbeitende Systeme in ihrer komplexen Gesamtheit, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

1. **Autorisierung** (Vergabe einer Berechtigung und eines Berechtigungsprofils zur Nutzung des Systems z. B. bei Vertragsabschluß, Personalisierung von Chipkarten usw.)
2. **Identifikation und Authentikation** (Nachweisführung des Benutzers über seine grundsätzliche Berechtigung zur Nutzung des Systems)
3. **Zugriffskontrolle** (Prüfung des Berechtigungsprofils relativ zu der gewünschten Aktion/Dienstleistung des Systems)
4. **Protokollierung** (Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer zum Zwecke der Nachweisführung)
5. **Abrechnung** (Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer)

Als Begründung für die jeweils erhobenen, anfallenden, gespeicherten und verarbeiteten personenbezogenen Daten werden überwiegend Abrechnungszwecke, verbesserte Kundenbetreuung, statistische sowie Kontrollzwecke angegeben.

Die tatsächliche Identität des Benutzers ist für die Funktionalität eines IuK-Systems grundsätzlich jedoch nicht erforderlich. Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die tatsächliche Identität des Benutzers erforderlich sein und müßte dort offengelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht notwendig (vgl. [RGB95]).

Wenn in einem System stattfindende Aktionen überwacht werden müssen und diese Überwachung nicht ausschließlich innerhalb des Systems möglich ist, so ist eine Protokollierung erforderlich. So ist z. B. die in den Datenschutzgesetzen des Bundes und der Länder vorgeschriebene Eingabekontrolle (z. B. Nr. 7 der Anlage zu § 9 BDSG) i. d. R. nur mit Hilfe der Protokollierung realisierbar, da die Zulässigkeit der Datenerhebung bzw. der Datenspeicherung nicht maschinell geprüft werden kann.

Bereits bei der Konzeption von IuK-Systemen sollte daher generell und für jeden einzelnen Prozeß untersucht werden, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung in Frage kommt (siehe Abschnitte "Anonymisierung" und "Pseudonymisierung").

3. Anonymisierung

Anonymisierung ist eine Veränderung personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

In den Datenschutzgesetzen von Bund und Ländern ist Anonymisierung unterschiedlich definiert. So ist in einigen Datenschutzgesetzen (z. B. § 3 Abs. 7 BDSG, Art. 4 Abs. 8 BayDSG, § 3 Abs. 7 LDSG RP, § 2 Abs. 7 DSG-LSA) für eine Anonymisierung bereits "das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" ausreichend. Andere Datenschutzgesetze (z. B. § 3 Abs. 7 Nr. 5 DSG MV, § 3 Abs. 2 Nr. 4 SächsDSG, § 2 Abs. 2 Nr. 7 LDSG SH) stellen höhere Anforderungen. Hier wird unter Anonymisieren "das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können", verstanden.

Die Qualität der Anonymisierungsprozedur hängt von verschiedenen Einflußfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen.

Auch konkrete Einzelangaben in einem Datensatz/einer Transaktion (z. B. Beruf/Amt=Bundeskanzler, konkrete Einkommensangaben) sind für die Qualität der Anonymisierungsprozedur von Bedeutung und können die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, verringern. Sind im Wertebereich Werte vorhanden, die die Anonymität gefährden, müssen sie mit anderen zusammengefaßt werden. Ist eine solche Veränderung aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.

Das Ziel datenschutzfreundlicher Technologien ist es unter anderem, Daten schon ohne Personenbezug zu erheben oder bereits personenbezogen erhobene Daten so bald wie möglich zu anonymisieren. Ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen. Gelungene Beispiele hierfür sind anonyme Telefonkarten und anonyme Zahlkarten im öffentlichen Personennahverkehr. Beispiele für die Anwendung der Anonymisierung sind im Bereich der Statistik und in der Forschung zu finden.

4. Pseudonymisierung

Pseudonymisierung ist das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.

Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können. Die Reidentifizierung kann mitunter auch ausschließlich dem Betroffenen vorbehalten bleiben. Mit Referenz- und Einweg-Pseudonymen (siehe folgende Unterabschnitte) versehene Daten sind jedoch weiterhin personenbezogene Daten, da sie einer bestimmten oder bestimmbaren Person zugeordnet werden können.

Das Mittel der Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo Anonymisierung nicht möglich ist.

Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflußfaktoren ab, wie die Stärke der Anonymisierungsprozedur, nämlich vom Zeitpunkt der Pseudonymisierung, von der Rücknahmefestigkeit der Pseudonymisierungsprozedur, von der Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und von der Verkettungsmöglichkeit von einzelnen Transaktionen/Datensätzen desselben Betroffenen. Insbesondere können Transaktionen/Datensätze, die unter demselben Pseudonym getätigt/gespeichert wurden, miteinander verkettet werden.

Unter gleichen Bedingungen ist die Anonymisierung datenschutzfreundlicher als die Pseudonymisierung. Das Pseudonym kann dazu benutzt werden, den Personenbezug wiederherzustellen. Ansonsten kann ohne Berücksichtigung der genannten Faktoren nicht pauschal beurteilt werden, ob die Anonymisierung oder die Pseudonymisierung datensparsamer ist.

Je nach Verknüpfbarkeit und dem Geheimnisträger des Pseudonyms kann der Personenbezug

- nur vom Betroffenen (selbstgenerierte Pseudonyme),
- nur über eine Referenzliste (Referenz-Pseudonyme) oder
- nur unter Verwendung einer sog. Einweg-Funktion mit geheimen Parametern (Einweg-Pseudonyme)

wiederhergestellt werden.

Pseudonyme ermöglichen es, den Personenbezug herzustellen, so daß die Identität der Person nur in den vorab bestimmten Einzelfällen erkennbar wird.

Pseudonyme sollen zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme soll so mächtig sein, daß bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym generiert wird. Ist eine hohe Sicherheit erforderlich, muß die Menge der Pseudonymkandidaten mindestens so mächtig sein wie der Wertebereich sicherer kryptographischer Hashfunktionen (siehe Abschnitt "Hashfunktionen").

Pseudonyme sollten insbesondere nicht anwendungsübergreifend, sondern nur für jeweils ein Verfahren eingesetzt werden. Jede anwendungsübergreifende Benutzung eines einzigen Pseudonyms würde die Gefahr erhöhen, daß aus sämtlichen mit dem Pseudonym verbundenen Daten ein detailliertes Personenprofil erstellt werden kann, das wiederum den Rückschluß auf eine bestimmte Person erleichtert. Aber auch innerhalb einer Anwendung ist die Verwendung nur eines einzigen Pseudonyms nicht unproblematisch.

4.1 Selbstgenerierte Pseudonyme

Selbstgenerierte Pseudonyme werden ausschließlich vom Betroffenen vergeben und nicht mit Identitätsdaten gleichzeitig verwendet oder gespeichert. Somit kann auch der Personenbezug nur vom Betroffenen selbst wiederhergestellt werden, i. d. R. nicht jedoch durch den Betreiber der IuK-Systeme.

Erfüllt die Menge der möglichen Pseudonyme die obigen Kriterien nicht, so ist ein Abgleich der selbstgewählten Pseudonyme mit den schon benutzten notwendig. Dies ist nur akzeptabel, wenn sich im "Trefferfall" nicht ermitteln läßt, wer das Pseudonym ursprünglich gewählt hat. Kann das für eine Person in Frage kommende Pseudonym vorhergesagt werden, so kann zumindest ermittelt werden, ob Daten zu dieser Person bereits gespeichert sind. Diese Vorhersage dürfte z. B. bei selbstgewählten Vor- und Zunamen oder beim wählbaren Anteil von Autokennzeichen oft funktionieren.

Selbstgenerierte Pseudonyme sollten Verwendung finden bei wissenschaftlichen Studien, die einerseits aggregierte Auskünfte über bestimmte Personengruppen geben sollen, andererseits aber auch den Betroffenen die Möglichkeit einräumen möchten, sich über ihre persönlichen Einzelergebnisse unerkannt zu informieren. Da es für die auswertende Stelle nicht erforderlich ist, die erhobenen Daten personenbezogen auszuwerten, kann statt des Namens ein vom Betroffenen selbstgewähltes Pseudonym verwendet werden, mit dessen Hilfe der Betroffene – und nur er selbst – die Ergebnisse in Erfahrung bringen kann, die ausschließlich seinen Einzelfall betreffen.

4.2 Referenz-Pseudonyme

Bei Referenz-Pseudonymen kann der Personenbezug über entsprechende Referenzlisten wiederhergestellt werden. Ohne Hinzuziehung entsprechender Referenzlisten ist die Identität des Betroffenen i. d. R. jedoch nicht zu ermitteln.

Referenz-Pseudonyme eignen sich für Anwendungen, bei denen der Betroffene nur in bestimmten Ausnahmefällen ermittelt werden muß, beispielsweise bei fehlerhaften Zahlungsvorgängen. Um zu erreichen, daß die Pseudonyme nicht aufgelöst werden, ist es notwendig, die Referenzliste räumlich und organisatorisch getrennt von den pseudonymisierten Datensätzen z. B. in einer Vertrauensstelle (siehe Abschnitt "Vertrauensstellen") zu speichern. Als besserer Schutz gegen die unbefugte Aufdeckung eines Pseudonyms können die Codes, die in den Referenzlisten zur Wiederherstellung des Personenbezugs gespeichert sind, auch auf mehrere Vertrauensstellen verteilt werden. Nur wenn sämtliche arbeitsteilig operierenden Akteure bereit sind, ihre jeweiligen Referenzlisten zur Verfügung zu stellen, kann das verwendete Pseudonym einer bestimmten Person zugeordnet werden.

4.3 Einweg-Pseudonyme

Einweg-Pseudonyme zeichnen sich dadurch aus, daß sie mittels Einweg-Funktion aus personenbezogenen Identitätsdaten – zumeist auf der Basis asymmetrischer Verschlüsselungsverfahren – gebildet werden. Dabei werden Einweg-Funktionen verwendet, die mit hoher Wahrscheinlichkeit ausschließen, daß die Identitätsdaten zweier Personen auf ein gemeinsames Pseudonym abgebildet werden.

Der Zusammenhang zwischen Identitätsdaten und Pseudonym wird folglich nicht mehr durch eine Tabelle (wie bei Referenzpseudonymen), sondern durch eine explizit formulierte (parametrisierbare) Vorschrift hergestellt. Die Sicherheit sollte nicht auf der Geheimhaltung dieser Vorschrift, sondern auf der Geheimhaltung der Parameter beruhen. Bei Referenzpseudonymen ist statt dessen die Tabelle geheimzuhalten.

Sowohl der Betroffene als auch der Betreiber des Verfahrens können nur dann depseudonymisieren, wenn sowohl die Parameter bekannt sind als auch die Abbildungsvorschrift bekannt ist/benutzt wird:

- Soll festgestellt werden, zu welcher Person ein bestimmtes Pseudonym zugeordnet ist, muß lediglich mittels der Abbildungsvorschrift aus den Identitätsdaten sämtlicher Personen, aus deren Reihen der Betroffene ermittelt werden soll, das jeweilige Pseudonym gebildet und mit dem zuzuordnenden Pseudonym verglichen werden.
- Andererseits läßt sich ermitteln, ob eine oder mehrere Personen mit einem Pseudonym in einem Datenbestand verzeichnet ist (sind), wenn Identitätsdaten und Abbildungsvorschrift (samt Parameter) bekannt sind. Falls dies zutrifft, sind auch die unter den entsprechenden Pseudonymen gespeicherten Daten zuordenbar.

Der Unterschied zu Referenzpseudonymen besteht darin, daß die Identitätsdaten der Betroffenen in den meisten Anwendungen nicht gespeichert werden müssen. Analog zu den Referenzpseudonymen ist aber auch hier eine Funktionentrennung notwendig: Instanzen, die die Pseudonyme verwalten bzw. die geheimen Parameter kennen und solche, die nur mit pseudonymisierten Daten umgehen, müssen voneinander getrennt werden. Bei Einhaltung dieser Funktionentrennung erscheinen die pseudonymisierten Identitätsdaten für diejenige Instanz, die nur mit den pseudonymisierten Daten umgehen kann, wie anonymisierte Daten.

Einweg-Pseudonyme eignen sich zum einen für Längsschnittuntersuchungen, bei denen nachträglich erhobene personenbezogene Daten mit Bestandsdaten zusammengeführt werden, ohne daß der Personenbezug für die statistische Auswertung der Daten erforderlich ist. Zum anderen können Einweg-Pseudonyme bei Auskunftssystemen eingesetzt werden, die Auskunft über die Zugehörigkeit bzw. Nicht-Zugehörigkeit einer Person zu einer bestimmten Gruppe geben, ohne daß dabei personenbezogene Identitätsdaten gespeichert werden müssen.

5. Realisierungshilfen

5.1 Hashfunktionen

Hashfunktionen werden in vielfältigem Zusammenhang in Sicherheitsverfahren verwendet, z. B. zur Unterstützung der Authentikation, der Erkennung der Datenunversehrtheit oder dem Urheber- und Empfängernachweis.

Bei einer Hashfunktion handelt es sich um einen Algorithmus, der eine Nachricht (Bitfolge) beliebiger Länge auf eine Nachricht (Bitfolge) fester, kurzer Länge – dem sogenannten Hashwert – abbildet. Eine Hashfunktion soll über folgende Eigenschaften verfügen:

- **Einwegfunktions-Eigenschaft**, d. h. zu einem vorgegebenen Wert soll es mit vertretbarem Aufwand unmöglich sein, eine Nachricht zu finden, die eben diesen Wert als Hashwert hat. Dieser "vertretbare Aufwand" hängt vom Entwicklungsstand der einsetzbaren Technik und den Sicherheitsanforderungen des Anwenders ab.
- **Kollisionsfreiheit**, d. h. es soll mit vertretbarem Aufwand unmöglich sein, zwei Nachrichten mit demselben Hashwert zu finden.

Bei der Erzeugung von Pseudonymen ist besonders die Kollisionsfreiheit gefordert. Hashfunktionen sind im Gegensatz zu vielen Verschlüsselungsalgorithmen öffentlich bekannt und unterliegen damit intensiven Analysen von Experten, so daß ihre Stärken und Schwächen im allgemeinen bekannt sind. Zu den bekanntesten gehören MD-4, MD-5, SHA-1, RIPEMD und RIPEMD-160. Einige davon haben sich als unbrauchbar zur Erzeugung von Pseudonymen herausgestellt, da sie nicht kollisionsfrei sind. In Europa hat sich RIPEMD-160 als Standard durchgesetzt. RIPEMD-160 ist nach ISO/IEC 10118-3 genormt.

Zur Erzeugung von sicheren Pseudonymen empfiehlt es sich, eine Hashfunktion auszuwählen, die schon länger veröffentlicht und wissenschaftlich untersucht ist. Verschiedene Verfahren sind denkbar, vor Umsetzung ist allerdings unbedingt der Rat von Experten einzuholen.

5.2 Digitale Signaturen

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen läßt [SigG].

Verfahren zur digitalen Signatur sind aus elektronischen Kommunikationssystemen bekannt. Mit der digitalen Signatur kann der Nachweis der Urheberschaft eines Objektes (z. B. eines digitalen Schriftstücks wie einer E-Mail (elektronische Post)) erbracht werden. Ein direkter Rückschluß auf denjenigen, der das Objekt signierte, ist möglich – ja gewollt. Da die digitale Signatur (u. a. durch Anwendung von Hashfunktionen) jeweils speziell über dem zu signierenden Objekt gebildet wird, ist damit gleichzeitig die Integrität des signierten Objekts nachprüfbar.

Erzeugt der Betroffene selbst dezentral die Schlüssel, handelt es sich in gewisser Weise um ein spezielles selbstgeneriertes Pseudonym, weil der spezielle (private) Signaturschlüssel (zur Erzeugung der digitalen Signatur) nur dem rechtmäßigen Benutzer bekannt und zugänglich ist.

5.3 (Signaturschlüssel-)Zertifikat

Ein Zertifikat ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person [SigG]. Dabei handelt es sich um ein spezielles selbstgeneriertes Pseudonym der das Zertifikat ausstellenden Institution, mit dem die Zuordenbarkeit zweier, voneinander abhängiger Pseudonyme zu einer Person (öffentlicher Signaturschlüssel und zugehöriger privater Signaturschlüssel) sichergestellt wird.

5.4 Blinde digitale Signatur

Eine "blinde digitale Signatur" stellt eine Variante der digitalen Signatur dar, mit der die Anonymität des Benutzers gewahrt wird. Der Unterschied zwischen beiden Signaturformen besteht darin, daß bei der blinden digitalen Signatur kein Rückschluß auf denjenigen möglich ist, der das signierte Objekt verwendet (Beispiel:

eine Banknote entspricht einem blind digital signierten Objekt; der Benutzer der Banknote bleibt anonym). Die Echtheit des Objektes wird von einem außenstehenden Dritten durch seine digitale Signatur bestätigt (Zertifikat), der Benutzer tritt mit seiner eigenen Identität nicht in Erscheinung. Diese Form der digitalen Signatur wird z. B. für "Ecash" (siehe Anlage, Abschnitt "Elektronische Zahlungssysteme") verwendet.

5.5 Biometrische Verfahren

Bei der biometrischen Verschlüsselung werden körperliche Merkmale wie Augennetzhaut, Fingerabdruck usw. z. B. durch optische Geräte oder besondere Chipkarten derart digitalisiert und zu einer digitalen Zeichenfolge aufbereitet, daß diese als eindeutiges Merkmal für die betreffende Person verwendet werden können. Zur Feststellung von Identität und Authentizität der Person als Benutzer eines IuK-Systems ist das betreffende körperliche Merkmal erneut zu digitalisieren und mit dem gespeicherten Muster zu vergleichen. Der Berechnungsvorgang zur Erzeugung dieser identifizierenden Zeichenfolge ist nicht umkehrbar, er stellt eine Einwegfunktion dar. Insoweit ist ein derart erzeugtes biometrisches Merkmal einem Einweg-Pseudonym gleichzusetzen.

5.6 Vertrauensstellen

Vertrauensstellen sind für die Realisierung bestimmter Sicherheitsdienste und für die Akzeptanz ganzer IT-Infrastrukturen erforderlich. Die Funktion einer solchen Vertrauensstelle wird oft mit der eines Notars, also einer neutralen, unbeteiligten Instanz, verglichen. Dieser Instanz müssen in der Regel alle Beteiligten (das sind der Benutzer und ggf. seine Kommunikations- und Geschäftspartner sowie ggf. die Betreiber der verwendeten IuK-Systeme) im Hinblick darauf vertrauen, daß sie ihre Aufgaben korrekt erfüllt.

Der Benutzer vertraut beispielsweise darauf, daß die Geheimhaltung seiner wahren Identität bei Verwendung eines Pseudonyms gewährleistet wird bzw. daß – wenn rechtmäßig seine Identität aufgedeckt wird – er unverzüglich informiert wird, wann, gegenüber wem und warum die Aufdeckung erfolgte.

Das Vertrauen des Betreibers eines IuK-Systems erstreckt sich darauf, daß zur Wahrung seiner legitimen Interessen im definierten und vereinbarten Bedarfsfall (z. B. Aufdeckung von Leistungsmissbrauch) die tatsächliche Identität des Benutzers offengelegt wird.

Aufgaben von Vertrauensstellen können, neben den kommerziellen oder öffentlichen Trust Centern als sogenannte Trusted Third Parties (TTPs), auch unter der Kontrolle des Benutzers arbeitende Personal Trust Center (PTCs) übernehmen, z. B. "intelligente" Sicherheitstoken wie SmartCards. Man unterscheidet vier Aufgabenbereiche, die von Vertrauensstellen erfüllt werden können:

- **Schlüsselmanagement**
 - Schlüsselgenerierung und -zurücknahme
 - Speicherung von (öffentlichen) Schlüsseln
 - Verteilung und Löschung/Sperrung von Schlüsseln
- **Beglaubigungsleistungen**
 - Ausstellung von Zertifikaten für öffentliche Schlüssel
 - Personalisierung von Schlüsseln: Zuordnung zu einem Benutzer (Identität oder Pseudonym)
 - Registrierung von Benutzern (Identitätsbeglaubigung und ggf. Zuordnung zu Pseudonymen)
 - Personalisierung von PTCs
 - Zertifizierung/Zulassung von TTPs
- **Treuhänderfunktion**

treuhänderisches Hinterlegen beispielsweise von

 - personenbezogenen Daten, z. B. Identifikationsdaten
 - Schlüsseln zur Datensicherung
- **Serverfunktionen**

Online-Bereitstellung von Informationen für die Sicherheitsinfrastruktur, z. B.

 - Verzeichnisse von (öffentlichen) Benutzerschlüsseln
 - Authentisierungsinformationen (z. B. bei Kerberos)
 - Zeitstempel

– Warnungen bei kritischen Sicherheitsereignissen

Um eine größtmögliche Vertrauenswürdigkeit der Vertrauensstellen zu erreichen, ist ein hohes Maß an Zuverlässigkeit und Fachkunde erforderlich. Die geforderte Neutralität und Unabhängigkeit einer Vertrauensstelle darf nicht durch Interessenkollisionen eingeschränkt oder gefährdet werden; solche Probleme können durch ungeeignete Kombinationen mehrerer der oben genannten (Teil-)Aufgaben bzw. Rollen entstehen. Darüber hinaus sollten Aufgaben mit besonderen Sicherheitsanforderungen nicht von einer einzigen Vertrauensstelle erledigt, sondern auf mehrere Stellen verteilt werden. Außerdem sollten die Vertrauensstellen nach einer veröffentlichten Policy arbeiten, die eine klare Darstellung der Aufgaben und Sicherheitsanforderungen umfaßt und die möglichst benutzerüberprüfbar realisiert ist [FHK95].

Nicht alle der o. a. Aufgaben von Trust Centern sind zur Datenvermeidung und damit zur verstärkten Wahrung der Privatheit des Einzelnen geeignet, wie z. B. insbesondere die Generierung von Schlüsseln in Vertrauensstellen und das Bereithalten von öffentlichen Schlüsseln mit Identitäten.

Als Beispiele für Vertrauensstellen können hier die Funktionalität von First Virtual (siehe Anlage, Abschnitt "Elektronische Zahlungssysteme") sowie die im Entwurf des Signaturgesetzes [SigG] beschriebenen Zertifizierungsstellen für die öffentlichen Schlüssel im Rahmen der digitalen Signatur genannt werden.

Im übrigen gibt es mittlerweile bereits eine Reihe von Unternehmen in der Bundesrepublik Deutschland, die einige oder alle der o. a. Dienstleistungen kommerziell anbieten.

5.7 Der Identity Protector

Wie oben dargestellt, lassen sich IuK-Systeme, für die eine anonyme Nutzungsform nicht vollständig möglich ist, derart in unterschiedliche Einzelprozesse zerlegen, daß unmittelbar personenbezogene Daten (Identitätsdaten) nur erhoben, gespeichert und verarbeitet werden, wo dies unabdingbar nötig ist.

Durch geeignete technische Maßnahmen muß dafür Sorge getragen werden, daß die Bereiche des IuK-Systems, die den vollen Personenbezug mit den Identitätsdaten benötigen, strikt von jenen getrennt werden, die nur mit einem Pseudonym auskommen. D. h., nur die tatsächlich und unmittelbar benötigten Daten stehen dem jeweiligen Prozeß zur Verfügung. Eine Zusammenführung von Identitätsdaten und Pseudonymdaten ist nur unter vorab und genau definierten Umständen möglich.

Diese Aufgaben kann ein "Identity Protector" leisten. Er kann als Systemelement (Prozeß) betrachtet werden, das den Austausch von Identitätsdaten und Pseudonymdaten zwischen den übrigen Systemelementen steuert [BO96] [RGB95].

Für einen "Identity Protector" sind verschiedene Ausprägungsformen möglich:

- a) eigenständiges Element in einem IuK-System
- b) eigenständiges IuK-System, das unter der Kontrolle des Benutzers steht
- c) eigenständiges IuK-System, das unter der Kontrolle einer Vertrauensstelle steht (siehe Unterabschnitt "Vertrauensstellen")

Im Falle a) sollte der Identity Protector ein – auch für den Betreiber des IuK-Systems – unveränderbarer Baustein sein. Die Realisierung ließe sich als Softwarebaustein im IuK-System selbst, im zugrundeliegenden Betriebssystem oder auch als Hardwarekomponente mit zugehöriger Software (z. B. als "Black-Box-Lösung") bewerkstelligen.

Im Falle b) wäre eine Abbildung des Identity Protectors z. B. in Form einer Smartcard als intelligentes Sicherheitstoken und als PTC möglich.

Der Identity Protector kann folgende Funktionalitäten leisten:

- kontrollierte Offenlegung und Freigabe der Identität
- Generierung von Pseudonymen

- Umsetzung von Pseudonymen in weitere Pseudonyme
- Umsetzung von Identitäten in Pseudonyme (Pseudonymisierung)
- Umsetzung von Pseudonymen in Identitäten (Depseudonymisierung)
- vorbeugende Mißbrauchsbekämpfung (u. a. durch die erstgenannte Funktionalität)

Zur Realisierung eines Identity Protectors stehen alle oben genannten Hilfsmittel zur Verfügung. Nicht alle diese Techniken müssen aber für jede Ausprägung eines Identity Protectors verwendet werden.

Die Funktionstüchtigkeit und Unveränderbarkeit des Identity Protectors müßte konsequenterweise mittels Zertifizierung und (kryptographischer) Versiegelung durch eine unabhängige Vertrauensstelle sichergestellt werden.

6. Zusammenfassung und Handlungsempfehlung

Datenvermeidung und Datensparsamkeit spielen in der Anwendung der IuK-Technologie bisher nur eine untergeordnete Rolle. Um zukünftig den Ansprüchen an Datenschutzfreundlichkeit gerecht zu werden, muß das Streben nach Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen genauso beeinflussen wie die Forderung nach Datensicherheit.

Für die Akzeptanz von Multimedia wird die Sicherstellung des Datenschutzes und der Privatheit des Einzelnen von entscheidender Bedeutung sein. Es ist absehbar, daß in Zukunft Produkte und Dienstangebote bei im übrigen gleicher Qualität und gleichem Preis Wettbewerbsvorteile haben werden, wenn sie datenschutzfreundlicher als die anderen sind. Ein Produkt oder Dienstangebot, das mit möglichst wenig personenbezogenen Daten seiner Nutzer auskommt, wird dem anderen vorgezogen, das umfangreiche Datenpuren erzeugt.

Die Datenschutzbeauftragten des Bundes und der Länder wollen diesen Prozeß beschleunigen und in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten.

Neue Informations- und Kommunikationssysteme sollten folgende **Grundsätze** beachten:

- IuK-Systeme sollten so gestaltet werden, daß keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden, d. h. daß eine anonyme Nutzung möglich ist.
- In den Systemteilmereichen, in denen für einen definierten Zeitraum personenbezogene Daten für die spezifische Funktionalität unabdingbar sind, sollte festgelegt werden, ob und wann eine Anonymisierung, oder falls dies nicht möglich ist, eine Pseudonymisierung erfolgen kann.

Um diese Grundsätze bei der Entwicklung oder Modifizierung von IuK-Systemen in ausreichendem Maße berücksichtigen zu können, ist folgende **Vorgehensweise** empfehlenswert:

Zunächst müssen datenverarbeitende Systeme und Teilsysteme einschließlich ihrer Schnittstellen definiert werden. Bei dieser Definition muß auch eine Unterscheidung derjenigen Systeme und Teilsysteme erfolgen, in denen

1. ohne personenbezogene Daten gearbeitet werden kann,
2. personenbezogene Daten anonymisiert werden können,
3. personenbezogene Daten pseudonymisiert werden können bzw.
4. der direkt herstellbare Personenbezug unvermeidlich ist.

Ist eine Anonymisierung oder eine Pseudonymisierung erforderlich, so ist für das jeweilige System/Teilsystem eine entsprechende Prozedur zu finden,

- die die personenbezogenen Daten frühestmöglich anonymisiert bzw. pseudonymisiert,
- die nicht unzulässig beeinflusst werden kann (Integrität),
- die aus dem System/Teilsystem nicht mit geringem Aufwand wieder entfernt werden kann (Rücknahmefestigkeit),
- die den Betroffenen in einer hinreichend großen Menge möglicher Betroffener verbirgt und
- die die Verkettbarkeit von Einzeldaten oder Transaktionen zu Datenspuren unterdrückt.

Stellt sich heraus, daß die vorhandenen Risiken mit dem so konstruierten System nicht hinreichend reduziert werden können, so müssen ggf. Teile des Definitionsprozesses und Teile des Gestaltungsprozesses wiederholt werden.

Bereits heute ist eine Reihe von Technologien und Hilfsmitteln zur Erreichung von verbessertem Datenschutz durch Technik verfügbar. Die Technologie, die dafür gesorgt hat, daß personenbezogene Daten gespeichert, genutzt und weitergegeben werden können, ist auch zur Wahrung der Privatheit des Einzelnen nutzbar. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff "**Privacy enhancing technology (PET)**" eine Philosophie der Datenvermeidung und der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Verbraucher sollten durch gezielte Nachfrage die Verwendung datenschutzfreundlicher Technologien in IuK-Systemen fordern und fördern.

Auch der Gesetzgeber muß die Verwendung datenschutzfreundlicher Technologien fordern und fördern.

An Industrie und Dienstleistungsanbieter ergeht der Appell, für den Verbraucher transparentere Systeme zu schaffen und datenschutzfreundliche Technologien verstärkt in ihre Systeme einzubauen.

Anlage 1

Literaturverzeichnis

- [BD776] Entschließung zu der Empfehlung an den Europäischen Rat "Europa und die globale Informationsgesellschaft" und zu der Mitteilung der Kommission "Europas Weg in die Informationsgesellschaft: Ein Aktionsplan", Bundesrat, Drucksache 776/96, 10.10.1996, Bonn
- [BO96] John Borking: Der Identity Protector; Datenschutz und Datensicherheit (DuD) 11/96, Verlag Vieweg, Wiesbaden, 1997, S. 654-658
- [BlSch] Bleumer, G., Schunter, M.: Datenschutzorientierte Abrechnung medizinischer Leistungen; Datenschutz und Datensicherheit (DuD) 2/97, Verlag Vieweg, Wiesbaden, 1997, S. 88-97
- [CC] <http://www.cybercash.com>
- [DIGI] <http://www.digicash.com>
- [FV] <http://www.fv.com>
- [FHK95] Dirk Fox, Patrick Horster, Peter Kraaibeek: Grundüberlegungen zu Trust Centern; In: Patrick Horster (Hg.): Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung; DuD Fachbeiträge, Braunschweig/Wiesbaden Vieweg 1995, S. 1-10
- [FJKP 95] Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Mobilkommunikationsnetzen; Wissenschaftliche Zeitschrift der TU Dresden 44/6 (1995) 4-9.
- [GZ96] Grimm, R.; Zangeneh, K: Cybermoney im Internet. Ein Überblick über neue Bezahlssysteme im Internet (Gesellschaft für Mathematik und Datenverarbeitung, Institut für Telekooperationstechnik); Darmstadt, Januar 1996
- [IuKDG] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG), Deutscher Bundesrat, Drucksache 420/97, 13.06.97, Bonn
- [KOM97] Kommissionsvorschlag zum 5. Rahmenprogramm für Forschung und technologische Entwicklung, KOM (97)142 und Mitteilung der Kommission zum elektronischen Handel, KOM (97)157,
<http://www.cordis.lu/esprit/src/ecomcom.htm>
- [MDStV] Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag), 12.02.97, (Unterzeichnung vom 20.01.-12.02.1997)
- [MON] <http://www.mondex.com>
- [POM] Modell von Pommerening, DuD 2/97 ???
- [RaPM 96] Kai Rannenber, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit; it+ti 38/4 (1996), S. 7-10

- [RGB95] H. van Rossum, H. Gardeniers, J. Borking u.a.: "Privacy-enhancing Technologies, The path to anonymity", Volume I u. II, Achtergrondstudies en Verkenningen 5b, Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995
- [RDLM 95] Kai Rannenber, Herbert Damker, Werner Langenheder, Günter Müller: Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik; In: Kubicek, Müller, Neumann, Raubold, Roßnagel (Hg.): Jahrbuch Telekommunikation & Gesellschaft, 1995, R. v. Decker's Verlag, Heidelberg, 1995, S. 254 - 260
- [SigG] Signaturgesetz, Art. 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG), Deutscher Bundesrat, Drucksache 420/97, 13.06.97, Bonn
- [SiKT97] CeBIT-Sonderseite des Kollegs "Sicherheit in der Kommunikationstechnik", <http://www.iig.uni-freiburg.de/dbskolleg/cebit97/>, März 1997
- [SSONET] Das SSONET-Projekt: "Sicherheit und Schutz in offenen Netzen (SSONET)", TU Dresden, 27.08.96, <http://mephisto.inf.tu-dresden.de/RESEARCH/ssonet/ssonet.html>
- [ZWIS] Zwissler, S.: Risikoreduktion bei elektronischer Auslieferung; Datenschutz und Datensicherheit (DuD), 7/97, Verlag Vieweg, Wiesbaden, 1997, S. 411-415
- [95/46/EG] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr, Amtsblatt Nr. L 281, S. 31

Anlage 2

Anwendungsmöglichkeiten und Einsatzfelder

| | |
|--|-----------|
| 1. DATENSCHUTZ IM MEDIENBEREICH..... | 16 |
| 1.1 ALLGEMEINES..... | 16 |
| 1.2 VERFAHREN UND PROJEKTE | 16 |
| 2. DATENSCHUTZ BEI ELEKTRONISCHEM GELD..... | 17 |
| 2.1 FÄLSCHUNGSSICHERHEIT VERSUS ANONYMITÄT | 17 |
| 2.2 KLASSIFIZIERUNG VON ELEKTRONISCHEM GELD | 18 |
| 2.3 ELEKTRONISCHE ZAHLUNGSVERFAHREN | 19 |
| 2.3.1 <i>Ecash</i> | 20 |
| 2.3.2 <i>Cybercash</i> | 21 |
| 2.3.3 <i>First Virtual</i> | 22 |
| 2.3.4 <i>SET-Standard</i> | 23 |
| 2.3.5 <i>Geldkarte</i> | 23 |
| 2.3.6 <i>Mondex</i> | 24 |
| 2.4 HARDWAREBASIERENDE SICHERHEITSLÖSUNG - MeCHIP | 24 |
| 3. DATENSCHUTZFREUNDLICHE TECHNOLOGIEN IM GESUNDHEITSBEREICH..... | 25 |
| 3.1 VERNETZUNG / NETZE..... | 25 |
| 3.2 VERFAHREN UND PROJEKTE | 26 |
| 4. DATENSCHUTZFREUNDLICHE TECHNOLOGIEN IN DER TELEKOMMUNIKATION..... | 27 |
| 5. DATENSCHUTZFREUNDLICHE TECHNOLOGIEN IM BEREICH TRANSPORT UND VERKEHR | 28 |
| 5.1 "KLASSISCHE" EDV | 28 |
| 5.2 CHIPKARTENEINSATZ BEI BENUTZUNG VON VERKEHRSMITTELN..... | 28 |
| 5.3 ZAHLUNGS- UND ÜBERWACHUNGSSYSTEME FÜR DIE BENUTZUNG VON VERKEHRSSTRAßEN | 29 |
| 5.4 SONSTIGE ÜBERWACHUNGSSYSTEME FÜR VERKEHRSMITTEL..... | 30 |

7. Datenschutz im Medienbereich

1.1 Allgemeines

Die "Informationsgesellschaft" umfaßt sowohl den Freizeitbereich als auch die Arbeitswelt. "Multimedia" ist das Schlagwort, das die verschiedenen Medientypen wie Text, Ton, Bild und Video zusammenführt, ohne eine neue Technologie an sich zu bilden.

Multimedia-Angebote mit besonderer Datenschutzrelevanz sind die Tele- und Mediendienste.

Teledienste sind elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt [IuKDG], z. B. Telebanking, elektronischer Datenaustausch, Datendienste, Internet, Online-Dienste, Telespiele, Teleshopping, Telemedizin, Telearbeit.

Mediendienste sind an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste in Text, Ton oder Bild, die unter Benutzung elektromagnetischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters verbreitet werden [MDSStV]. Sie bestehen aus Verteil- und Abrufdiensten. Beispiele für Mediendienste sind Pay-TV, elektronische Presse, Teletext.

In der Praxis dürfte sich eine strikte Abgrenzung von Telediensten und Mediendiensten als äußerst schwierig erweisen.

Die zur Zeit entwickelten Angebote erstrecken sich von Bildtelefon und Videokonferenzen über Lernprogramme, digitale Nachschlagewerke und Informationssysteme bis zu interaktiven Spielen, Video-on-Demand (Videofilme auf Anforderung), Teleshopping, Online-Diensten und Telemedizin – alles von zu Hause aus zugänglich. Das Fernsehen wandelt sich vom Massenmedium zum individualisierten Informations- und Unterhaltungsmedium mit "Rückkanal".

Bei Inanspruchnahme der elektronischen Informations- und Kommunikationsdienste entstehen personenbezogene Daten, die nicht nur für Zwecke der Abrechnung nutzbar sind. Sie könnten auch für die Programmanbieter unter Marketingaspekten interessant sein. Es ließen sich detaillierte Informationen gewinnen, wann welcher Nutzer welche Fernsehsendungen, Videos oder elektronische Zeitungsartikel abgerufen, welche Produkte er beim Teleshopping bestellt, wohin er Reisen elektronisch gebucht oder welche Abfragen er in Informationssystemen vorgenommen hat. Das Kommunikations- und Konsumverhalten der Kunden könnte ausgewertet und persönliche Lebensgewohnheiten erforscht werden.

Das Informations- und Kommunikationsdienste-Gesetz des Bundes [IuKDG] und der Mediendienste-Staatsvertrag der Länder [MDSStV] haben den Grundsatz der Datensparsamkeit für die Anbieter von Online-Diensten und Internet-Zugängen festgelegt. Eine Registrierung des Nutzerverhaltens ist unzulässig. Die Anbieter von Multimedia-Diensten sind verpflichtet, auch die anonyme Inanspruchnahme und Bezahlung von Informationsdiensten als Option anzubieten, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

Soweit personenbezogene Daten unbedingt erhoben werden müssen, dürfen sie nur mit Einwilligung des Nutzers zu anderen Zwecken, z. B. für Werbung, verwendet werden. Die Nutzer müssen ausführlich über den Umgang mit ihren Daten informiert werden.

Da die elektronischen Informations- und Kommunikationsdienste auf der Telekommunikation beruhen, muß die datenschutzfreundliche Ausgestaltung der Technologie bereits dort ansetzen.

1.1 Verfahren und Projekte

- Beim digitalen Fernsehen ist für den Kunden vor allem die Möglichkeit neu, nur für die Programmangebote zu bezahlen, die auch wirklich gesehen wurden. Diese **Pay-per-View-Angebote** werden grundsätzlich verschlüsselt übertragen und müssen für den Empfang dekodiert werden. Hierzu benötigt man eine sogenannte Set-Top-Box, in die der Kunde seine Chipkarte einführt. Für die Freischaltung

werden zur Zeit verschiedene technische Verfahren eingesetzt:

- Bei der **zentralen Freischaltung** muß der Kunde zunächst dem Sender mitteilen, welche Sendung er sehen möchte. Zusammen mit dem Sendesignal werden dann die Nutzernummern der Interessenten unverschlüsselt übertragen, deren Decoder freigeschaltet werden soll.
- Für die **lokale Freischaltung** durch den Nutzer wird jede Sendung mit einer elektronischen Entgeltinformation (Token) gekoppelt. Die an einer Sendung interessierten Kunden geben ihren Wunsch mit der Fernbedienung an ihre Set-Top-Box weiter, die die Kosten für das Programmangebot von der Guthaben-Chipkarte im Decoder abbucht und die Sendung freischaltet.

Während bei der zentralen Freischaltung das vom Kunden gewünschte Programmangebot zu Abrechnungszwecken beim Sender gespeichert wird und durch die unverschlüsselte Übertragung der Nutzernummern sogar im gesamten Netz mit geringem Aufwand ausgewertet werden kann, braucht der Kunde bei der lokalen Freischaltung keine personenbezogenen Daten aus der Hand zu geben.

- Für einige Internet-Dienste, z. B. E-Mail, News oder WWW, stehen mehrere **Pseudo-Anonymous-Server** zur Verfügung, die die Absenderkennung durch ein Referenz-Pseudonym ersetzen. Bei den **Mixmaster-Remailern** wird die Zuordnung des Pseudonyms zum Benutzer nicht gespeichert, so daß keine Reidentifizierung des Absenders vorgenommen werden kann.
- Der **Identity Protector** von John Borking, Niederlande, ist ein Instrument zum Schutze der Privatsphäre, das die Identität von Personen innerhalb der verschiedenen Prozesse in einem Informationssystem anonymisiert oder pseudonymisiert [RGB95]. Näheres hierzu siehe Grundlagenpapier, Abschnitt 5.7 "Der Identity Protector".
- Bei dem Projekt **Sicherheit und Schutz in offenen Netzen (SSONET)** an der Technischen Universität Dresden geht es um den Entwurf, die Implementierung und die Validierung eines Prototyps für mehrseitige Sicherheit [SSONET]. Die zu entwickelnde Sicherheitsarchitektur soll konkret für Internet, Mobile Computing, Teledienste und Workflow-Systeme detailliert untersucht und umgesetzt werden. Das Projekt läuft vom 01.05.96 bis zum 30.04.99.
- Ebenfalls an der TU Dresden ist in einer Studienarbeit eine Software für ein Videokonferenzsystem entwickelt worden, mit der sich geheime Informationen unbemerkt von abhörenden Dritten in die Bewegtbildübertragung einbetten lassen (**rechnergestützte Steganografie**).
- Auf der CeBIT '97 hat das interdisziplinäre Ladenburger Kolleg "**Sicherheit in der Kommunikationstechnik**" (gefördert von der Gottlieb Daimler- und Karl Benz-Stiftung), in dem Teilnehmer aus Hochschulen, öffentlichen und privaten Forschungseinrichtungen sowie führenden Unternehmen der Branche mitarbeiten, u. a. innovative und datensparsame Protokolle und Topologien für eine Netz- und Dienststruktur vorgestellt [SiKT97]. Durch eine dezentrale Ansiedlung von Vertrauensinstanzen und sensitiven Daten in Kommunikationsnetzen soll das Risiko des Mißbrauchs reduziert und den Nutzern die Möglichkeit gegeben werden, selbst auszuwählen, welchen Instanzen sie vertrauen.

8. Datenschutz bei elektronischem Geld

1.1 Fälschungssicherheit versus Anonymität

Fälschungssicherheit und Anonymität scheinen zwei Anforderungen an elektronisches Geld zu sein, die sich auf den ersten Blick grundlegend widersprechen. Daß es dennoch möglich ist, beide Aspekte zu integrieren und somit datenschutzfreundliche Technologien im elektronischen Zahlungsverkehr zu implementieren, wird im folgenden gezeigt.

Kauf- und Zahlungsvorgänge zeichnen sich dadurch aus, daß sowohl der Käufer als auch der Verkäufer die Ware bzw. das Entgelt weitgehend betrugsfrei erhalten. Während beim Handel mit höherwertigen Gütern die Betrugsmöglichkeiten dadurch reduziert werden, daß beide Handelspartner ihre Identität bewußt preisgeben,

um ggf. nachträgliche Forderungen besser durchsetzen zu können, erfolgt die Bezahlung niederwertiger Güter traditionell anonym mittels Bargeld. Das Betrugsrisiko ist aufgrund des niedrigen Warenwerts und aufgrund der Anwesenheit beider Handelspartner recht gering.

Geringwertige Güter und Dienstleistungen werden zunehmend nicht mehr mit Bargeld bezahlt, sondern mittels elektronischem Geld als dessen digitale Ausdrucksform. Während sich Bargeld dadurch auszeichnet, daß es während des Bezahlvorgangs intuitiv auf Echtheit überprüft wird, läßt sich elektronisches Geld nicht durch den Empfänger verifizieren. **Das Bezahlen erfolgt mittels digitaler Daten, die fälschbar sind.** Digitales Geld ist zum einen leicht zu duplizieren, zum anderen sind die Duplikate von den Originalen nicht zu unterscheiden.

Beim Bezahlen im Internet sind zudem der Zahlende und der Entgeltempfänger räumlich voneinander getrennt. Ihre Kommunikation ist normalerweise flüchtig, ungesichert und nicht beweiskräftig. Beim Bezahlen von Informationen ergibt sich zudem die Schwierigkeit, daß der Austausch *Information gegen Geld* nicht zeitgleich erfolgt, sondern in der Regel zuerst die Information übertragen wird (nach dem Grundsatz: "zuerst die Ware, dann das Geld"), so daß sich der Dienstleister nicht unbedingt auf das Bezahlversprechen des in der Regel anonym agierenden Kunden verlassen kann. In umgekehrter Reihenfolge riskiert aber der Kunde, im voraus für etwas zu bezahlen, das er anschließend in der erwarteten Form nicht erhält [ZWIS].

Das erhöhte Manipulationsrisiko von elektronischem Geld wird meistens dadurch kompensiert, daß der Entgeltempfänger die Identität des Zahlenden überprüft (beispielsweise mittels PIN) und dessen Identitätsdaten speichert, um sich im Mißbrauchsfalle nachträglich noch an den Kunden wenden zu können. **Damit wird im Gegensatz zu Bargeld die Anonymität des Kunden aufgehoben**, sofern er sich nicht bereits anderweitig offenbart hat, beispielsweise durch Angabe seiner Lieferanschrift oder seiner Internet- oder Electronic-mail-Adresse.

Bleibt das Bezahlen mit elektronischem Geld nicht anonym, besteht die Gefahr, daß die Zahlungsdaten zu detaillierten Nutzungs- bzw. Kundenprofilen ausgewertet werden.

Die Anonymität beim Bezahlen setzt voraus, daß der Kunde nicht nur gegenüber dem Händler oder seiner Bank, sondern gegenüber sämtlichen an der Zahlungsabwicklung beteiligten Akteuren anonym bleibt. Falls die Identität des Kunden durch eine gezielte Zusammenarbeit von Händler und Bank aufgehoben werden kann, kann nicht mehr von Anonymität gesprochen werden.

Durch den Einsatz von **Referenz-Pseudonymen** (s. Abschnitt 4.2 Hauptteil) kann zumindest die Identität des Kunden gegenüber einzelnen Instanzen, beispielsweise gegenüber dem Händler, verborgen werden. Der Kunde agiert somit nicht vollständig anonym, aber gegenüber einzelnen Akteuren zumindest pseudonym.

Solche Referenz-Pseudonyme sind Voraussetzung für eine arbeitsteilige Datenhaltung. So ist es möglich, daß der Händler zwar Kenntnis über die pseudonym abgewickelten Kaufvorgänge hat, aber den Namen des Käufers nicht kennt. Umgekehrt weiß die Bank zwar den Namen des Kunden, kennt jedoch nur die Kaufsumme und den Händler, wengleich häufig auch aus dem Händlernamen bereits Kaufvorlieben von Kunden abgeleitet werden können.

Unabhängig davon, ob Zahlungsverfahren eingesetzt werden, die anonymes Bezahlen ermöglichen, ist darauf zu achten, daß die über das Internet übertragenen personenbezogenen Daten zumindest vertraulich bleiben. Ist dies nicht sichergestellt, besteht die Gefahr, daß beispielsweise Kreditkartennummern von Außenstehenden mitgelesen und zur Überweisung auf fremde Konten mißbräuchlich genutzt werden. Dies beeinträchtigt zwar nicht unmittelbar die Datenschutzinteressen des Kunden, kann aber beträchtlich dessen Bankkonto "erleichtern". Da das Abhörissiko im Internet sehr hoch ist, läßt sich **Vertraulichkeit** im Internet nur dadurch garantieren, daß sicherheitsrelevante Zahlungsdaten verschlüsselt übertragen werden.

1.1 Klassifizierung von elektronischem Geld

Elektronisches Geld unterscheidet sich durch mehrere Merkmale. Diese etwas ausführlicher zu behandeln ist insofern interessant, als sämtliche Ausprägungen nicht nur die Manipulationssicherheit prägen, sondern auch entscheidenden Einfluß auf die Anonymität der Zahlungsverfahren haben [GZ96]:

- **Art der Zahlung**

Das elektronische Geld kann gegenüber der herausgebenden Bank entweder im voraus vor der Weitergabe an den Händler gekauft (**Prepaid-Verfahren**) oder erst nach der Einlösung der Händlerforderung verrechnet werden (**Postpaid-Verfahren**). Während Postpaid-Verfahren kein anonymes Bezahlen ermöglichen, da der Kunde zumindest der Bank bekannt sein muß, sind Prepaid-Verfahren hierzu geeignet. Dies setzt jedoch voraus, daß der Kunde auch bei der Verrechnung der Geldeinheiten (Clearing) nicht identifiziert werden kann.

- **Art des Wertetransfers**

Elektronisches Geld kann in Form von Transaktionen oder in Form von Bargeld transferiert werden. **Transaktionsorientierte Verfahren** orientieren sich an Lastschriftverfahren. Geldbeträge werden dabei unter Angabe des Absenders und des Empfängers transferiert, so daß der Zahlungsvorgang nicht mehr anonym ist. Ob die Zahlungsvorgänge nur temporär zur Zahlungsabwicklung oder über einen längeren Zeitraum auch zur Verteilung von Geldwerten auf einzelne Konten benötigt werden, hängt wiederum vom Stellenwert dritter Instanzen ab, beispielsweise Clearingstellen.

Bargeldorientierte Verfahren sind aus datenschutzrechtlicher Sicht zu favorisieren, da keine Geldbeträge übermittelt werden, sondern ein Bündel von einzelnen Geldeinheiten. Die Fälschungssicherheit wird durch digitale Signierung jeder Geldeinheit realisiert. Das Bezahlen mit bargeldorientierten Verfahren ist jedoch nur dann vollständig anonym, wenn nicht zwecks Geldflußanalysen auf dem elektronischen Geldschein vermerkt wird, durch wessen Hände er gegangen ist. Geldflußanalysen sind hinsichtlich der Manipulationsicherheit, aber auch hinsichtlich der Überprüfung von unerlaubter Geldwäsche von Bedeutung.

- **Art des Geldkreislaufs**

Die meisten Zahlungsverfahren stellen einen geschlossenen Kreislauf zwischen dem Kunden, dem Händler sowie der Kunden- und Händlerbank dar. Jede Forderung, die der Händler gegenüber dem Kunden aufgrund einer ausgelieferten Ware oder einer erbrachten Dienstleistung hat, wird direkt über die Händler- und Kundenbank eingelöst. Das Manipulationsrisiko ist aufgrund der Abgeschlossenheit des Verfahrens zwar relativ gering. Dennoch ist jede erworbene Ware oder getätigte Dienstleistung grundsätzlich von den dazwischengeschalteten Banken nachvollziehbar. Es ist allerdings möglich, das Bezahlen arbeitsteilig derart zu gestalten, daß einerseits der Händler keine Kenntnis über die Identität des Kunden hat, andererseits die Bank, die im Auftrag des Kunden dem Händler den Geldbetrag ausbezahlt, jedoch keine Kenntnis über die getätigten Dienstleistungen erhält.

Datenschutzfreundlicher sind *Face-to-Face*-Verfahren, bei denen das elektronische Geld auch von Kunde zu Kunde bzw. von Händler zu Händler ohne Zwischenschaltung einer Bank weitergegeben werden kann. Der Zeitpunkt, zu dem elektronisches Geld in Giralgeld umgewandelt wird, bleibt dabei jedem Kunden selbst überlassen. Da derartige Verfahren in der Regel bargeldorientiert sind, können die mit dem elektronischen Geld bezahlten Dienstleistungen nicht mehr zentral, sondern lediglich dezentral beim Kunden oder beim Händler bzw. auf einem von ihnen verwalteten Medium (z. B. Chipkarte) gespeichert werden.

- **Art der Geldbörsenplattform**

Elektronische Zahlungsverfahren sind entweder hardwaregestützt (z. B. auf Basis von Chipkarten) oder hardwareunabhängig. Chipkartengestützte Zahlungssysteme sind aufgrund von Hardwaremechanismen wesentlich manipulationssicherer als hardwareunabhängige Verfahren, die ausschließlich auf softwarebasierten Verschlüsselungstechniken basieren. Somit wäre eigentlich zu vermuten, daß bei chipkartengestützten Verfahren tendenziell weniger personenbezogene Daten erhoben werden. Diese Einschätzung läßt sich anhand der im Einsatz befindlichen Verfahren jedoch nicht bestätigen.

Bei chipkartengestützten und zugleich transaktionsorientierten Verfahren empfiehlt es sich, möglichst personenungebundene Chipkarten, sogenannte *White Cards*, zu verwenden. Sonst besteht die Gefahr, daß durch Auswertung von Verrechnungskonten die Anonymität des Kunden aufgehoben wird.

1.1 Elektronische Zahlungsverfahren

Im folgenden werden sechs elektronische Zahlungsverfahren dargestellt. Den Verfahren werden für die Betrachtung relevante Merkmale zugeordnet (siehe Abbildung), deren Ausprägungen auch eine Basis für eine datenschutzgerechte Einschätzung bilden.

1.1.1 Ecash

Ecash [DIGI] ist eine bestimmte Form digitaler Geldmünzen (Cyberbucks), die hardwareunabhängig ohne ein körperliches Trägermedium ihrem Besitzer die Durchführung von Zahlungsvorgängen über öffentliche Computernetze so ermöglichen, als würde dieser mit echten Münzen bezahlen. Das Ecash zugrunde liegende technologische Verfahren, das vom niederländischen Kryptologen David Chaum entwickelt wurde und das von der Firma DigiCash angeboten wird, ist schon in den USA und Finnland im Einsatz. Auch die Deutsche Bank hat eine Lizenz für Ecash erworben und testet das Zahlungsverfahren in einem Pilotprojekt.

Ecash ist ein bargeldorientiertes Prepaid-Verfahren, das jedoch an ein Buchgeldguthaben gekoppelt ist, beispielsweise auf einem herkömmlichen Girokonto. Vergleichbar mit regulären Banknoten besitzt jede digitale Münze eine einmalige Seriennummer, die zur Überprüfung der Einmaligkeit des elektronischen Geldes dient. Im Gegensatz zu Bargeld werden bei Ecash die digitalen Münzen nur einmal in Umlauf gebracht und nach dem Kauf vom Händler sofort bei der Bank eingelöst, um ein unerlaubtes Erstellen von Münz-Duplikaten zu erschweren. Ecash ist somit ein geschlossenes Verfahren, das zur Zeit noch keinen Face-to-Face-Umlauf erlaubt. Um zu verhindern, daß die Bank über die Seriennummer einen direkten Bezug von Käufer und Händler ableiten und daraus entsprechende Kundenprofile erzeugen kann, kommt bei Ecash die sogenannte *blinde digitale Signatur* (s. Abschnitt 5.2 Hauptteil) zum Einsatz.

Um mit Ecash zu zahlen, muß der Käufer gegen Belastung seines Kontos zunächst digitale Werteinheiten (Münzen) von seinem Bankinstitut in seine *Geldbörse* auf dem PC laden. Mittels einer speziellen Software, die der Ecash-Teilnehmer auf seinem PC vorhält, erzeugt er einen Datensatz, der u. a. den gewählten Betrag und eine nach dem Zufallsprinzip generierte Seriennummer enthält. Diese Seriennummer wird mittels eines mathematischen Verfahrens mit einer Zufallszahl (Blendungsfaktor) verdeckt. Anschließend werden die Daten verschlüsselt an die Bank übermittelt. Die vom Kunden verdeckte Seriennummer kann die Bank nach der Entschlüsselung nicht identifizieren, da sie nicht den Blendungsfaktor kennt. Somit wird sichergestellt, daß die Bank im nachhinein nicht feststellen kann, welchem Kunde welche Münze mit welcher Seriennummer ausgegeben wurde.

Die Bank bucht den Betrag vom Konto des Käufers ab, validiert den Datensatz mit ihrer digitalen Signatur und übermittelt diesen in verschlüsselter Form wieder auf den PC des Käufers. Unter erneutem Einsatz des Blendungsfaktors wird hier die Seriennummer in ihrer ursprünglichen Form wieder hergestellt.

Mit Ecash kann über das Internet bei allen Händlern Ware bezahlt werden, die sich Ecash angeschlossen haben. Der Käufer transferiert die Geldmünzen verschlüsselt über das Netz zum Händler. Dieser läßt die Echtheit und Originalität der ihm angebotenen Münzen online von der ausstellenden Bank mittels digitaler Signatur prüfen. Da sich die Bank die Seriennummer merkt, würde eine zum zweitenmal eingereichte Münze als ungültig zurückgewiesen.

Nach Prüfung und positiver Bestätigung durch die Bank kann schließlich der Händler die Vertragserfüllung realisieren. Das vom Händler eingezahlte Ecash wird von der Bank auf herkömmlichem Weg seinem Konto gutgeschrieben, oder er erhält dafür wiederum erneut einen äquivalenten elektronischen Wert als Münze mit einer neuen Seriennummer.

| | Zahlung | | Werttransfer | | Geldkreislauf | | Geldbörsenplattform | | Zahlungsvorgang insgesamt | | |
|---------------|-----------|----------|------------------------|-------------------|---------------|--------------|---------------------|---------------------|---------------------------|---------------------------------|--------------------|
| | post-paid | pre-paid | transaktionsorientiert | bargeldorientiert | geschlossen | face-to-face | chipkarten-gestützt | hardware-unabhängig | anonym | pseudonym gegenüber dem Händler | mittels Treuhänder |
| Ecash | | x | | x | x | | | x | x | | |
| Cybercash | x | | x | | x | | | x | | x | x |
| First Virtual | x | | x | | x | | | x | | x | x |
| SET | x | | x | | x | | | x | | x | |
| Geldkarte | | x | x | | x | | x | | | x | |
| Mondex | | x | | x | | x | x | | | x | |

Elektronische Zahlungsverfahren im Vergleich

Ecash erlaubt als Prepaid-Verfahren anonyme Zahlungen sowohl gegenüber der Bank als auch gegenüber dem Händler. Der Einsatz der blinden Signatur stellt sicher, daß die der elektronischen Münze zugeordnete Seriennummer keine Rückschlüsse auf den Kunden ermöglicht. Damit kann das Kaufverhalten eines Kunden nicht nachvollzogen werden, denn er bezahlt wie bei Bargeld ohne Datenspuren zu hinterlassen. Ecash unterscheidet sich damit wesentlich von anderen Online-Zahlungsverfahren.

Die Anonymität des Käufers ist natürlich nur soweit gewährleistet, wie der Kunde nicht beim Verkäufer Ware bestellt, die auf dem herkömmlichen Weg zugesandt werden muß. In diesem Fall muß sich der Käufer aber nur gegenüber dem Verkäufer identifizieren. Die Bank kann den Weg der Münzen auch weiterhin nicht bis zum Kunden zurückverfolgen, obwohl sie letztendlich dessen Zahlungsverkehr abrechnet.

Die Zahlungsdaten werden zudem verschlüsselt übertragen, so daß auch die Vertraulichkeit der Transaktion gegenüber Dritten gewährleistet ist.

1.1.1 Cybercash

Cybercash ist ein netzfähiges Zahlungssystem auf der Basis von Kreditkarten. Der Zahlungsvorgang wird vermittelt und unterstützt durch sogenannte Treuhänder, die die Verrechnung durch Kreditkarte oder ein Bankeinzugsverfahren durchführen. Cybercash wurde als reales System im Jahr 1994 in den USA eingeführt und realisiert alle Transaktionen über das Internet.

Sowohl Käufer als auch Händler sind Vertragspartner des Cybercash-Treuhänders. Jeder Cybercash-Teilnehmer erhält eine spezielle Software, mit der ein eigenes Schlüsselpaar generiert wird, bestehend aus einem privaten und einem öffentlichen Schlüssel. Der Käufer übermittelt dem Cybercash-Treuhänder seinen öffentlichen Schlüssel sowie seine mit dem öffentlichen Schlüssel von Cybercash chiffrierte Kreditkartennummer. Damit ist der Kunde bei Cybercash registriert und kann bei allen Cybercash angeschlossenen Händlern über das Internet einkaufen.

Auf eine Kaufanfrage erhält der Kunde vom Händler ein entsprechendes Angebot. Hat sich der Kunde zum Kauf entschlossen, gibt er dem Händler hierüber eine Bestätigung. Diese Bestätigung, die unter anderem die mit dem öffentlichen Schlüssel von Cybercash verschlüsselte Kreditkartennummer des Kunden und seine Produktauswahl beinhaltet, ist vom Kunden digital signiert. Damit wird der Kaufwunsch des Kunden im Rahmen von Cybercash verbindlich und nachweisbar. Der Händler kann die ihm übermittelte Kreditkartennummer nicht entschlüsseln und sendet diese ergänzt um weitere Angaben, wie beispielsweise den Kaufbetrag, an den Cybercash-Server. Dieser nimmt nach der Entschlüsselung der Daten direkt Verbindung zu der entsprechenden Kreditkartengesellschaft des Käufers auf, um das Clearing einschließlich der Authentisierung des Käufers einzuleiten. Das Ergebnis dieser Aktion wird dem Händler mitgeteilt, der dem Käufer wiederum bei Vorliegen einer positiven Bestätigung eine von ihm digital signierte Quittung als Beweis der Kauftransaktion übermittelt.

Cybercash arbeitet nach dem Postpaid-Verfahren; ein Kaufauftrag führt immer zur Belastung des Kundenkontos. Eventuelle Reklamationen können nur außerhalb des Cybercash-Verfahrens bearbeitet werden.

Der Käufer bleibt bei Cybercash nicht anonym, da zahlreiche Daten über den Kaufvorgang gespeichert werden. Der Käufer agiert jedoch mittels verschlüsselter Kreditkartennummer zumindest gegenüber dem Händler pseudonym.

Der Treuhänder besitzt neben dem Namen und der Anschrift des Kunden dessen Kreditkartennummer, die er zur Verrechnung der Kaufbeträge bei der Kreditkartengesellschaft benötigt. Die Kreditkartengesellschaft kennt ebenfalls den Kunden, weiß aber nicht, was er gekauft hat.

Personenbezogene Kundenprofile können nur erstellt werden, wenn sämtliche Akteure ihre jeweiligen Datenbestände untereinander austauschen. Da der Händler die Kreditkartennummer nur in verschlüsselter Form kennt, können Händler und Kreditkartengesellschaft ohne den Treuhänder keine Kundenprofile generieren. Insofern setzt ein Datenmißbrauch ein treuwidriges Verhalten aller Beteiligten voraus.

Fälschungssicherheit und Vertraulichkeit der übermittelten Zahlungsdaten wird bei Cybercash durch den Einsatz kryptographischer Funktionen sichergestellt. Die Zahlungsdaten werden sowohl verschlüsselt übertragen als auch verschlüsselt auf dem Rechner des Händlers gespeichert. Da der Käufer bei der

Transaktion seinen Kaufauftrag zusätzlich mit seiner digitalen Signatur versieht, ist sein Auftrag zudem nachträglich beweisbar.

1.1.1 First Virtual

First Virtual [FV] ist ein mit Cybercash vergleichbares kreditkartengestütztes Abrechnungssystem, das in den USA zum Einkaufen im Internet eingesetzt wird. Artikel, Bücher, Zeitschriften, Bilder, Nachrichten, Software etc., aber auch Waren außerhalb des Internets können über First Virtual gekauft und bezahlt werden.

Es basiert auf gewöhnlichen Internetdiensten wie E-Mail, FTP und WWW. Das System erfordert somit seitens der Kunden keine spezielle Software, um Produkte im Internet anzubieten bzw. diese zu kaufen.

First Virtual übernimmt in der Abrechnung zwischen Käufer und Händler die Treuhänder- bzw. die Vermittlerfunktion, analog Cybercash. Die Belastung des Kunden erfolgt über dessen Kreditkarte, wobei im Gegensatz zu Cybercash bei der Transaktion die Kreditkartennummer nicht mit übertragen wird. Dem Anbieter der Leistung schreibt First Virtual den Betrag auf beliebigem Wege gut.

Jeder Kunde meldet seine Teilnahme über den entsprechenden WWW-Server von First Virtual an und erhält von First Virtual eine vertrauliche Benutzerkennung zugesandt. Über dieses Pseudonym wird jede zukünftige Kauftransaktion des Kunden abgewickelt. Der Kunde übermittelt seine Kreditkartennummer unverschlüsselt per Brief oder Telefon an First Virtual. Die Kreditkartennummer wird von First Virtual auf einem nicht mit dem Internet verbundenen Rechner gespeichert; per E-Mail wird dem Kunden die Freischaltung der Zugangsberechtigung bestätigt.

Ein Zahlungsvorgang wird bei First Virtual dadurch in Gang gesetzt, daß der Kunde einen Kaufantrag mit seiner Benutzerkennung per elektronischer Post abschickt. First Virtual fragt beim Käufer zurück, ob er das Produkt tatsächlich bestellt hat und ob er es auch bezahlen möchte. Erst nach einer positiven Bestätigung durch den Käufer wird dessen Kreditkartenkonto letztendlich belastet. Durch eine negative Bestätigung kann sich der Käufer sowohl vor einer schlechten Produktqualität als auch vor Fehlbestellungen schützen, die Unbefugte in seinem Namen auslösen können. Diese Vorgehensweise schützt den Kunden auch dann, wenn ein Verdacht auf illegale Benutzung seiner Kreditkarte besteht. In einem solchen Fall stellt First Virtual Nachforschungen an, ändert die Benutzerkennung und überweist dem Verkäufer kein Geld.

Da der Kunde in der Regel über das Bezahlen erst dann entscheidet, nachdem er die Informationsprodukte gelesen hat, setzt dieses Verfahren Vertrauen in die Ehrlichkeit der Kunden voraus und bedeutet damit ein gewisses Risiko für den Informationsanbieter. Obwohl diese Verfahrensweise seitens First Virtual durch seine Gründer bewußt angestrebt wurde, ist aber auch eine Notbremse gegen allzuhäufige Stornierungen eingebaut. Wer zu häufig die Zahlung verweigert, verliert seine Benutzerkennung.

First Virtual ist ein hardwareunabhängiges, transaktionsorientiertes Postpaid-Verfahren mit geschlossenem Geldkreislauf. First Virtual ist ebenso wie Cybercash kein anonymes Zahlungsverfahren; es ermöglicht dem Käufer jedoch, pseudonym gegenüber dem Händler aufzutreten.

Das System First Virtual verzichtet auf den Einsatz kryptographischer Mittel. Die Kommunikationsinhalte der Transaktionen werden unverschlüsselt über das Internet übertragen; allerdings erfolgt keine Übermittlung der Kreditkartennummer des Kunden. Durch Einsatz der Benutzerkennung erübrigt sich auch die Übertragung persönlicher Identifikationsangaben des Kunden.

Die übermittelten Daten sind daher nur soweit vor unbefugtem Zugriff gesichert, wie dies die Internetdienste Electronic Mail, FTP und WWW zulassen, auf die das System zurückgreift. Ein Schutz vor Verlust der Vertraulichkeit der übertragenen Nachrichten ist somit nicht gegeben.

Auch die Fälschungssicherheit ist aufgrund fehlender Sicherheitsmechanismen nicht gewährleistet. Das gleiche trifft auf den Kaufvorgang zu, der nicht beweisbar ist und keinem Kunden eindeutig zugeordnet werden kann, da hierfür der Einsatz entsprechender Mechanismen, wie z. B. der digitalen Signatur, fehlt. Da First Virtual dem Käufer jedoch das Recht einräumt, vom Kauf Abstand zu nehmen, kann dieser dennoch eventuelle Nachteile zu seinen Ungunsten abwenden.

1.1.1SET-Standard

Für das Bezahlen mit Kreditkarten im Internet werden dem Verfahren SET (Secure Electronic Transaction) als zukünftigem Zahlungsverkehrsprotokoll große Chancen eingeräumt. Microsoft, Visa und Mastercard haben beschlossen, SET zu einem allgemeinen Standard zu entwickeln. Mit SET sollen die Protokolle SEPP (Secure Electronic Payment Protocol) von Mastercard, Cybercash, IBM und Netscape sowie STT (Secure Transaction Technology) von Visa und Microsoft abgelöst werden. SET verwendet sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren; die Schlüssel werden durch entsprechende Instanzen zertifiziert.

Der Kunde zahlt durch Angabe seiner Kreditkartennummer, die er am PC eingibt. Die SET-Software verschlüsselt die Kreditkartendaten und leitet sie zusammen mit einer digitalen Signatur an den Verkäufer weiter. Dieser kann die verschlüsselten Kartendaten nicht lesen und leitet sie ergänzt um den Kaufbetrag an das Kreditkartenunternehmen weiter. Das Kreditkartenunternehmen bestätigt dem Verkäufer die Solvenz des Kunden und schreibt dem Händler den Betrag gut.

Der SET-Standard ermöglicht zwar kein anonymes, jedoch ein pseudonymes Einkaufen. Während der Händler nur über das gekaufte Produkt und den Preis informiert ist, nicht aber den Namen des Käufers weiß, kennt die Kreditkartengesellschaft die Identität des Käufers sowie den bezahlten Betrag, erhält aber keine Information über das gekaufte Produkt.

Im Gegensatz zu Cybercash tritt bei SET allerdings kein Treuhänder als Vermittler zwischen Händler und Kreditkartenunternehmen auf. Somit kennt das abrechnende Kreditkartenunternehmen den Händler, bei dem der Kunde einkauft, so daß zumindest kundenbezogene Teilprofile erstellt werden können.

Der SET-Standard gewährleistet die Vertraulichkeit und Fälschungssicherheit der Transaktionsdaten sowie die Authentizität zwischen Käufer und Verkäufer, so daß Kaufvorgänge nicht abgestritten werden können.

1.1.1Geldkarte

Zum Bezahlen im Internet eignet sich grundsätzlich auch die seit Anfang des Jahres bundesweit im Einsatz befindliche Geldkarte des deutschen Kreditwesens, wengleich das Bezahlen und Aufladen zur Zeit noch spezielle Händler- und Bankterminals voraussetzt. Denkbar wäre es jedoch auch, das Bezahlen über Netze mittels Geldkarte zu realisieren – entsprechende Planungen liegen in den Schubladen der Entwickler. Die Transaktionen werden dann nicht mehr über Händler- und Bankterminals transportiert, sondern per Internet direkt von der Geldkarte vom Kunden zum Händler bzw. von der Bank zum Kunden. Die Realisierung dieses Szenarios setzt voraus, daß die in den Terminals implementierten Mechanismen zur Manipulationssicherheit durch geeignete Instrumente auf Netzebene, beispielsweise Verschlüsselungsmaßnahmen, ersetzt werden.

Aus datenschutzrechtlicher Sicht ist der Einsatz der Geldkarte insofern problematisch, als ein sehr komplexes Clearingverfahren konzipiert wurde, das kartenbezogen jede einzelne Zahlungstransaktion erfaßt. Die von den Händlern eingereichten Umsätze werden zunächst in Börsenevidenzzentralen auf Echtheit und Doppeleinreichungen geprüft und anschließend mit Börsenverrechnungskonten verrechnet, die von den Banken für jeden Kunden eingerichtet worden sind. Während das Börsenverrechnungskonto nur Auskunft über den Saldo einer jeden Karte gibt, führen die Börsenevidenzzentralen zusätzlich für jede Karte eine Börsenumsatzdatei, die sämtliche mit einer Karte getätigten Umsätze bzw. Transaktionen festhält. Der Transaktionsdatensatz enthält nicht nur den Kaufbetrag, das Kaufdatum und die Kaufzeit sowie einen identifizierbaren Händlerschlüssel, sondern auch das zum Kaufzeitpunkt aktuelle Kartensaldo. Die Börsenumsatzdatei stellt somit ein Schattenkonto dar, das sämtliche mit der elektronischen Geldkarte getätigten Kaufvorgänge parallel mitverfolgt. Da die Geldkarte in der Regel auf der EC-Karte untergebracht ist, sind die Kontoauszüge nicht nur kartenbezogen, sondern zugleich personenbezogen.

Das Führen von Schattenkonten hat hauptsächlich zwei Gründe:

- Zum einen ist das Vertrauen der Kreditwirtschaft in die Fälschungs- und Revisionsicherheit des Verfahrens nicht groß genug, um auf ein einzelfallbezogenes kartenbezogenes Clearing verzichten zu wollen. Durch die Schattenkonten wird doppelte Sicherheit zu erreichen versucht.

- Zum anderen sollen dem Bankkunden bereits vorausbezahlte, aber noch nicht ausgegebene Geldwerte erstattet werden können. Elektronische Geldwerte sollen dem Bankkunden jedoch nur bei technischem Defekt der Geldbörse, nicht jedoch bei deren Verlust zurückgegeben werden.

Da die Geldkarte eine vorausbezahlte Geldbörse ist, besteht normalerweise keine Notwendigkeit, personenbezogene Zahlungsdaten zu Buchungszwecken zu erheben und zu speichern. Es ist daher zu hoffen, daß langfristig auf das Führen von Schattenkonten verzichtet wird und nur noch Schattensalden – wie das bereits bei der österreichischen EC-Karte praktiziert wird – gespeichert werden.

1.1.1Mondex

Ein hardwaregestütztes Verfahren stellt das von der Westminster Bank und der Midland Bank zusammen in Großbritannien herausgegebene Mondex dar [MON]. Mondex erlaubt nicht nur die Übertragung elektronischen Geldes im geschlossenen Kreislauf zwischen Kunde, Händler und Bank, sondern auch *face-to-face* zwischen einzelnen Kunden. Außerdem kann Mondex zum Online-Bezahlen über öffentliche Netze eingesetzt werden. Mondex ist somit auch zum Bezahlen im Internet geeignet, wengleich hierzu noch einige Ergänzungen notwendig sind.

Das Bezahlen per Mondex geschieht mittels Chipkarte und zusätzlicher *Wallets*, die für die sichere Übertragung der Geldtransaktionen zuständig sind. Bei Bedarf kann sich der Kunde über das Wallet auch die letzten zehn getätigten Transaktionen anzeigen bzw. ausdrucken lassen.

Mondex ist aus datenschutzrechtlicher Sicht insofern interessant, als beim Einkaufen mittels Mondex weniger personenbezogene Daten gespeichert werden als bei der vergleichbaren Geldkarte des deutschen Kreditwesens. Anstatt sehr aufwendig den mit jeder Geldbörse getätigten Umsatz nachzuvollziehen, um hierüber flächendeckend für jede im Umlauf befindliche Geldbörse Mißbrauchsfälle sofort erkennen zu können, wird bei Mondex zunächst nur überprüft, ob mehr elektronisches Geld im Umlauf ist, als seinerzeit herausgegeben wurde. Dabei wird – wie bei Papiergeld – ein gewisser Prozentsatz von gefälschtem Geld sogar in Kauf genommen.

Um den Anteil von falschem elektronischen Geld zu ermitteln, werden stichprobenartig für einzelne Schnittstellen im Zahlungssystem detaillierte Geldflußanalysen erstellt. Die Geldflußanalysen basieren auf Zahlungsdaten, die erhoben werden, wenn die Wallets über das Mondex-Kommunikationssystem mit der Betreiberbank verbunden sind.

1.1Hardwarebasierende Sicherheitslösung – MeCHIP

Das MeCHIP-System der Firma ESD bei Leipzig stellt eine hardwarebasierte Sicherheitslösung für den Datentransfer zwischen dem Kunden-PC (MeCLIENT) und dem Rechnersystem (MeSERVER) des Anbieters (z. B. einer Bank) dar. Es verkörpert kein neues Zahlungssystem. Hiermit wird die bei softwarebasierenden Sicherheitssystemen existierende Sicherheitslücke beim Kunden-PC abgedeckt. Ausgangspunkt eines Angriffes auf den Kunden-PC könnte beispielsweise ein für den Benutzer unbemerkter, durch Shareware, Spiele oder direkt aus einem öffentlichen Netz eingeschleuster Virus sein, der im Datenspeicher des PC abgelegte und noch nicht verschlüsselte sicherheitsrelevante Daten (Paßwort, Schlüsselwörter, Kreditkarten-Nr., Konto-Nr. etc.) manipuliert oder ausliest und an einen fremden Zielrechner sendet. Beim MeCHIP-System kommen sowohl asymmetrische als auch symmetrische Ver- und Entschlüsselungsmethoden (RSA- und Standard-DES-Verfahren mit Modifikationen) zum Einsatz.

Kern dieser Schutztechnologie ist der sogenannte MeCHIP, der auf Seiten des MeClient als Hardware sowie beim MeServer als Softwarelösung eingesetzt wird und alle sicherheitsrelevanten Aktionen realisiert. Die Benutzung des MeCHIP ist paßwortgesichert. Jeder Chip verkörpert ein Unikat, indem der Schaltkreis verschieden ist. Somit ist es möglich, jedem Benutzer eine eindeutige Identifikation zuzuordnen, eine Art digitale Identität. Der MeCHIP besitzt einen direkten Anschluß an die Tastatur des MeClient. Somit werden alle sicherheitsrelevanten Daten, die am absendenden PC mittels Tastatur oder anderer externer Eingaben in der Regel unverschlüsselt eingegeben werden, direkt in den MeCHIP übertragen. Dort werden sie signiert und spezifisch verschlüsselt, d. h., der mit einem Zufallsgenerator erzeugte eigentliche Schlüssel wird vor der Verschlüsselung der Daten noch mit dem eindeutigen und hardwareabhängigen Schlüssel des MeCHIP verschlüsselt. Letzterer Schlüssel ist nur noch dem MeServer bekannt, weshalb nur dieser Daten für einen bestimmten MeCHIP ent- und verschlüsseln kann.

Die signierten und verschlüsselten Daten werden anschließend über offene Netze mit dem MeTransportprotokoll zum Zielsystem übertragen. Hier werden vom MeServer chipspezifisch die Daten entschlüsselt sowie die Signatur überprüft und eventuelle Datenmanipulationen erkannt. Nach der erfolgreichen Überprüfung wird die Transaktion vom MeServer bestätigt. Damit sichert der MeCHIP den Informationsfluß von der Eingabe am MeClient bis zur Entschlüsselung auf dem MeServer. Das eingesetzte Transaktionsprotokoll ist paketorientiert und unabhängig von der gewählten Transportschicht. Hier involvierte Sicherheitsmechanismen sollen u. a. das unbemerkte Einfügen, Entfernen und Wiedereinspielen von Datenpaketen verhindern.

Das MeCHIP-System kann unabhängig vom Übertragungsweg (bspw. Internet, T-Online), vom übertragenen Inhalt und von der eingesetzten Zahlungsart (bspw. Kreditkarte, Ecash) eingesetzt werden.

Die Hamburger Sparda-Bank verwendet das MeCHIP-System beim Homebanking. Der MeCHIP wird auf den Druckeranschluß des Kunden-PC gesteckt und mit der Tastatur verbunden. Somit verschlüsselt er alle über die Tastatur eingegebenen Kundendaten, bevor sie in den RAM des PC gelangen. Die vom traditionellen Online Banking gewohnten Transaktionsnummern entfallen. Der Kunde muß sich nur noch seine PIN merken.

Die MeCHIP-Technik ermöglicht dem Empfänger, den Absender eindeutig zu identifizieren. Das Verfahren ist so angelegt, daß jedem Benutzer der MeCHIP-Technologie eine eindeutige Identifikation zugeordnet wird. Auf diesem Prinzip beruht das Vertrauen, daß sich Kunde und Anbieter bei diesem System entgegenbringen.

Inwieweit der Kunde allerdings zum "gläsernen" Konsumenten wird, wenn das MeCHIP-Sicherheitssystem (in eventuell angepaßter Form) zur Absicherung der Transaktionen beim Online-Shopping eingesetzt wird, hängt primär von dem hier verwendeten Zahlungssystem ab.

9. Datenschutzfreundliche Technologien im Gesundheitsbereich

Mit der flächendeckenden Einführung der Krankenversichertenkarte (KVK) gemäß § 291 SGB V wurde zwangsläufig in der gesamten Bundesrepublik Deutschland eine Infrastruktur geschaffen, die die elektronische Verarbeitung aller medizinischer Daten (Leistungsdaten, Diagnosedaten, Verlaufsdaten), die ein Leistungserbringer (Arzt, Krankenhaus, Hebamme etc.) über einen Patienten speichert, zur Folge hat. War vor der Einführung der KVK ein Großteil der Leistungserbringer nicht mit elektronischen Datenverarbeitungsanlagen ausgestattet, so änderte sich dies mit der Einführung schlagartig; fast jeder Leistungserbringer verfügt heute über einen Arbeitsplatzcomputer mit Drucker und Chipkartenlesegerät (Kartenterminal). Der weitere Ausbau wird – schon heute absehbar – in der Vernetzung über moderne Telekommunikationssysteme (ISDN, Internet) vorgenommen werden.

Damit ergeben sich zwei Themenbereiche:

- die (digitale) Kommunikation über medizinische Daten, insbesondere auch über moderne Telekommunikationssysteme (ISDN, Internet)
- die zunehmend automatisierte bzw. rechnergestützte Verarbeitung personenbezogener Daten im Rahmen von Behandlung und Forschung

1.1 Vernetzung / Netze

Derzeit wird im Gesundheitsbereich in folgende Richtung argumentiert:

Die Nutzung der vorhandenen Infrastruktur nur zum Zweck der Abrechnung schein auf die Dauer nicht wirtschaftlich, ließen sich doch durch den Einsatz der Technik ein Großteil der im Gesundheitswesen vorhandenen Informations- und Kommunikationsdefizite beheben. Diese wirkten sich bei der Qualität der

Patientenversorgung aus und verursachten in nicht unerheblichen Maße Zusatzkosten für die Versicherungsgemeinschaft. Typische Beispiele für die vorhandenen Defizite seien:

- Bei der Überweisung vom Haus- zum Facharzt, vom Haus- oder Facharzt ins Krankenhaus etc. werden oftmals keine Befunde oder Ergebnisse von Voruntersuchungen mitgeliefert, so daß verschiedene Untersuchungen (Röntgen, EKG, Labortests) erneut durchgeführt werden. Dies stellt nicht nur für den Patienten eine erhebliche Belastung, z. B. durch wiederholtes Röntgen dar, sondern trägt darüber hinaus zur Steigerung der Kostenbelastungen bei.
- Arztbriefe, die bei einer Krankenhausentlassung dem nach- oder weiterbehandelnden Arzt als Basisinformation dienen sollen, erreichen zum Teil erst nach Wochen ihren Empfänger. Die zumeist handschriftlichen, häufig schwer lesbaren Niederschriften wären oftmals ohne Rückfragen und den damit verbundenen Zeitverzug für eine Fortsetzung der Behandlung nicht geeignet.
- Wichtige Informationen, wie etwa solche über besondere Vorerkrankungen, Risikofaktoren, Allergien, oder Arzneimittelunverträglichkeiten, stehen zwar oftmals dem Hausarzt zur Verfügung, aber nicht den behandelnden Fachärzten oder gar dem Notfallarzt.
- Gesundheitsvorsorgemaßnahmen sind teilweise nur aufgrund einer breiten Auswertung von vorliegenden Krankheitsverläufen möglich. Hierzu sind zunächst die Daten in einer elektronischen Krankenakte zu führen.
- Epidemiologische Forschungen benötigen regelmäßig institutionsübergreifend Zugriff auf die Daten eines Patienten, um für das Gesundheitswesen fundierte Zahlen und Fakten zu liefern.

An der Verbesserung der Kommunikation wird seit Jahren intensiv in wissenschaftlichen Untersuchungen und Modellprojekten gearbeitet. Zum einen kommen dabei Chipkarten zur Speicherung der wichtigsten Informationen eines Patienten zum Einsatz ("Patientenkarten"; Offline-Lösung), zum anderen werden die Möglichkeiten von modernen Telekommunikationsnetzen erprobt. Dies geschieht zur Unterstützung von Diagnosen durch Spezialisten über weite Entfernungen durch elektronische Übermittlung von Voruntersuchungsergebnissen per Datentransfer oder durch Zugriffe auf Patientendaten, die auf verschiedenen Rechnern – Hausarzt, Facharzt, Krankenhaus etc. – gespeichert werden.

Die Datenschutzbeauftragten stellen sich dieser Diskussion.

1.1 Verfahren und Projekte

Das zentrale Problem bei den bisher geplanten oder erprobten Verfahren dreht sich um die Frage, mit welchen Maßnahmen die Daten eines Patienten gegen jeden anderen Zugriff als den der in der konkreten (Behandlungs-)Situation zugriffsberechtigten Person geschützt werden können. Daneben stehen die Forderungen der Krankenkassen und der medizinischen Forschung zur elektronischen Auswertung der gespeicherten Daten zur Qualitätssicherung, Prognosen, Planzahlen und der medizinischen Forschung zur Verbesserung der Versorgung. Dies eröffnet ein breites Feld an möglichen Anwendungen für Anonymisierungs- und Pseudonymisierungsverfahren. Neben der klassischen Behandlungssituation Patient – Arzt, bei der personenbezogene Daten zwangsläufig anfallen (s. o. Spiegelstrich 1 bis 3), gibt es eine Reihe anderer Vorgänge im Gesundheitswesen, bei denen der Personenbezug nicht unbedingt benötigt wird (s. o. Spiegelstrich 3 bis 5). In all diesen Fällen könnten datenschutzfreundliche Technologien einen erheblichen Beitrag leisten, sowohl für das Vertrauen des Patienten bezüglich des Umgangs mit seinen Daten als auch für den Arzt zur Beweis- und Qualitätssicherung.

Praktische Erfahrungen mit dem Einsatz datenschutzfreundlicher Technologien liegen bereits vor:

- Krebsregister (Krebsregistergesetz in Schleswig-Holstein) (vgl. auch Bundeskrebsregistergesetz)

- Pseudonymisierungs-Technik im Bereich der Qualitätssicherung in der Nierenersatztherapie (QuaSiNiere)
- Pseudonymisierung bzw. Anonymisierung im Bereich der epidemiologischen (medizinischen) Forschung (Ursachenforschung)

Neben diesen konkreten Anwendungen wurden in der Vergangenheit bereits **Modelle** entwickelt, in denen ebenfalls datenschutzfreundliche Technologien eingesetzt werden könnten. Beispiel hierzu sind:

- Krankenkassenabrechnung [POM] [BISch]
- Pseudonymisierung von Arztdaten beim Einsatz einer Apothekenkarte (Struif, GMD)
- Einsatz von Gruppenschlüsseln beim Zugriff auf med. Daten in Krankenhäusern [BISch]
- Führung von Registern, z. B. Herzschrittmacher, künstliche Hüftgelenke etc. (Planungen der Deutschen Krankenhausdachgesellschaft – DKG – zum Führen eines Herzschrittmacherregisters zur Qualitätssicherung dieser Geräte, Pseudonym = Serien-Nummer des Gerätes)
- Diensteanbieter im Gesundheitswesen, z. B. "Home-Care".
Neben Beratung der Behandlung von kleineren Krankheiten (Schnupfen, Husten) sollen hier auch Beratungen bezüglich Ernährung, Sucht und im Bereich der Prävention, z. B. Geschlechtskrankheiten oder AIDS, angeboten werden. "Home-Care"- Dienste werden allerdings nur dann angenommen werden, wenn eine gewisse Anonymität des Benutzers gewährleistet ist und die Kostenfrage mit den Kassen geklärt worden ist. Für beide Einsatzgebiete bieten sich Pseudonymisierungs- und Anonymisierungsverfahren an. (*Die genauen Vorstellungen werden derzeit im Forum Info 2000 Arbeitsgruppe Gesundheitswesen beraten und präzisiert*)

Die Beispiele Krebsregister und QuaSiNiere zeigen die Möglichkeiten und auch die Grenzen für den Einsatz von datenschutzfreundlichen Technologien im Gesundheitswesen.

Wichtige, in Zukunft anstehende Fragen wie nationalstaatenübergreifende Datenübermittlung, Einrichtung einer Treuhänderstelle eventuell auch im Ausland, Sicherheit (Zertifizierung) von Pseudonymisierungsalgorithmen, verfahrenübergreifende Pseudonyme etc. sind allerdings noch nicht in Angriff genommen worden. Hierzu zählen auch Modelle, die im Rahmen der Informationsgesellschaft und zur Senkung der Gesundheitskosten zur Diskussion stehen.

10. Datenschutzfreundliche Technologien in der Telekommunikation

Bezüglich des Einsatzes datenschutzfreundlicher Technologien und zugehöriger Bewertungsmodelle wird auf das Papier der Arbeitsgruppe "Datenvermeidung in der Telekommunikation" des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder verwiesen.

In diesem Papier wird zunächst der Systembegriff für Telekommunikationssysteme (TK-Systeme) präzisiert. Dazu wird unter anderem ein allgemeines TK-Datenmodell eingeführt. In diesem Zusammenhang können auch die Begriffe Datenvermeidung, Anonymisierung und Pseudonymisierung näher definiert und ein Bewertungsmodell entwickelt werden. Mit den zuvor entworfenen Hilfsmitteln werden anschließend einige gebräuchliche TK-Verfahren untersucht. Um Wege zur Minimierung der in diesen Verfahren anfallenden personenbezogenen Daten aufzuzeigen, werden einige besonders geeignete Technologien näher vorgestellt.

11. Datenschutzfreundliche Technologien im Bereich Transport und Verkehr

Im Bereich Transport und Verkehr gibt es folgende alte und neue Entwicklungen mit Relevanz für den Datenschutz:

1.1 "Klassische" EDV

Der "klassische" Einsatz von EDV im Bereich Transport und Verkehr entspricht dem EDV-Einsatz in anderen Bereichen. Als Beispiele seien hier die dv-gestützten Verfahren zur Kfz-Zulassung, zur Verwaltung von Führerscheinen, zur Verkehrskontrolle, zur Unfallaufnahme und zur Verwaltung von Daten über Kunden und Personal von Verkehrsbetrieben genannt. Soweit datenschutzfreundliche Technologien hier einsetzbar sind, wäre dies auch für viele andere Bereiche von Bedeutung. Durch mehr Datensparsamkeit sind sicherlich vielfach datenschutzfreundlichere Verfahren möglich. Dies hat aber seine Grenzen. So ist die Führung einer Kfz-Führer-Sünderdatei unter Pseudonymen zwar weitgehend möglich und wird bei Nutzung relationaler Datenbanksysteme auf technischer Ebene sogar praktiziert. Letztendlich muß aber die Zusammenführung der Sünder-Daten mit den Personendaten immer möglich sein.

1.1 Chipkarteneinsatz bei Benutzung von Verkehrsmitteln

Zur Zeit werden an vielen Stellen im Öffentlichen Personennahverkehr (ÖPNV) und im Fährverkehr Chipkarten zur Bezahlung von Fahrkarten oder als Fahrkartenersatz eingeführt (z. B. in Skandinavien, Pilotprojekte in Deutschland). Es werden im wesentlichen folgende Einsatzmöglichkeiten erprobt:

- a. Postpaid-Karte, Speicherung aller Fahrten, Ermittlung des günstigsten Tarifs (Bestpreisermittlung), Bezahlung über Lastschriftverfahren
- b. Prepaid-Karte, Aufladung eines Geldbetrages, von dem der Fahrpreis abgebucht wird. Prepaid-Karten sind entweder
 - b.1 anonym (nur einmal benutzbare Karten wie Telefonkarten oder mit Bargeld aufladbare Karten),
 - b.2 oder die Aufladung erfolgt personenbezogen durch Überweisung vom Girokonto, die Abbuchung des Fahrpreises erfolgt anonym vom aufgeladenen Geldbetrag.

Häufig wird, zum Teil aufgrund von Forderungen der Datenschutzbeauftragten, neben der Postpaid-Karte auch die Prepaid-Karte alternativ angeboten. Neben diesen Unterscheidungen gibt es viele weitere Unterscheidungsmerkmale der chipkartengestützten Fahrkartensysteme wie kontaktlose oder nicht kontaktlose Chipkarten und Multifunktionskarten.

Beispiele für geplante und eingeführte Systeme oder Projekte:

- EC-Karte (zu b.2): Abbuchung vom Girokonto
Anbieter: Banken und Sparkassen /ÜSTRA in Hannover u. a.
- Pay-Card (alternativ b.1 oder b.2): Abbuchung über Telefonrechnung oder Barzahlung
Anbieter: Telekom/DB, ÖPNV in Hamburg, Stuttgart, München, Rhein-Main
- FAHRSMART (alternativ a oder b.1): Abrechnung und Abbuchung durch Terminals des ÖPNV
Anbieter: KVG Lüneburg, Oldenburg
- NORDERNEY-Card (im wesentlichen b.1): Fährticket nach Norderney, multifunktionale Berechtigungskarte für Kureinrichtungen, ÖPNV auf Norderney usw.;
zumindest die Gästekarte kommt ohne jeglichen Personenbezug aus, weil jeder Gast eine Karte erwerben und diese beim Verlassen der Insel vorzeigen muß. Es ist möglich, Schattenkonten ohne personenbezogene Daten zu führen, die bei einer Zerstörung und u. U. auch bei einem Verlust der Karte die Erstellung eines Duplikats ermöglichen.
Anbieter: Kurverwaltung, Reederei, Stadt Norderney u. a.

Neben Dauerkarten wie Monats- oder Jahreskarten sind Prepaid-Karten eine datenschutzfreundliche Alternative. Prepaid-Karten sind in der Verwendung allerdings umständlicher als Postpaid-Karten, so daß möglicherweise viele Kunden auf diese Alternative verzichten. Deshalb sollte auch das Postpaid-Verfahren

möglichst datenschutzgerecht gestaltet werden. Bei Postpaid-Verfahren ist durch eine strikte Trennung von Kontoabbuchung und Fahrpreisberechnung eine datenschutzfreundliche Technologie möglich. Das Kreditinstitut übernimmt die Ausgabe der Postpaid-Chipkarten an die Kunden, speichert die Personalien und das zugehörige Konto. Es bekommt den Gesamtpreis der monatlichen oder vierteljährlichen Fahrtkosten vom Verkehrsbetrieb übermittelt und übernimmt die Überweisung des Gesamtpreises an den Verkehrsbetrieb. Bei der Überweisung an den Verkehrsbetrieb wird ein kartenbezogenes Pseudonym verwendet, der Verkehrsbetrieb erfährt somit nicht, wem die Karte gehört. Der Verkehrsbetrieb speichert für jedes Pseudonym die für die Abrechnung erforderlichen Daten (Fahrpreisdaten, Bestpreisermittlung usw.), gibt aber nur den ermittelten Gesamtpreis an das Kreditinstitut weiter.

1.1 Zahlungs- und Überwachungssysteme für die Benutzung von Verkehrsstraßen

Die politischen Ziele und Kriterien, die mit der Erhebung von strecken- und zeitbezogenen Straßenbenutzungsgebühren (road-pricing) im Zusammenhang mit Autobahnmaut, Citymaut oder Parktickets verfolgt werden, sind u. a.

- Verkehrslenkung,
- gerechte Anlastung der Wegekosten,
- private Finanzierungsmöglichkeiten,
- Verbesserung der Infrastruktur Autobahn, Schienenverkehr und
- Umweltschutz (Schadstoffemission, Rohstoffverbrauch),

wobei die Gewichtung für Autobahn-Maut-Systeme sich von der für City-Maut-Systeme durchaus unterscheidet.

Erprobt wurden solche Systeme u. a.

1. mit dem Feldversuch des baden-württembergischen Verkehrsministeriums auf der B 27 in Stuttgart,
2. mit dem Feldversuch des Bundesverkehrsministeriums auf der A 555 zwischen Bonn und Köln.

Die Forderungen der Datenschützer zur Anonymität, Vertraulichkeit, Integrität, Transparenz und Rücknahmefestigkeit haben sich von den Herstellerfirmen nicht umfassend realisieren lassen.

Einige der Forderungen waren umsetzbar. Unter dem Aspekt der Datenschutzfreundlichkeit lassen sich insbesondere folgende Erkenntnisse festhalten:

- Prepaid-Karten bieten bessere Voraussetzungen zur Wahrung der Anonymität als Postpaid-Karten
- Offene Systeme können datenschutzfreundlicher gestaltet werden als geschlossene Systeme, weil sie ohne Speicherung von Zu- und Abfahrt auskommen, indem beim Vorbeifahren an einer Maut-Stelle die Gebühr fällig bzw. abgebucht wird
- Dezentrale Speicherung im Bereich des Benutzers (z. B. auf einer Chipkarte) könnte zur Vermeidung von Bewegungsprofilen genutzt werden

Größere Probleme wurden bei den Kontrollverfahren sichtbar. Es dürfte schwierig sein, ein Kontrollverfahren zu entwickeln, das einerseits hinreichend beweissicher ist und andererseits den Anforderungen des Datenschutzes genügt.

Beide Feldversuche wurden beendet, ohne daß eine Umsetzung für einen Echtbetrieb erfolgt wäre. Für den Autobahn-Maut-Versuch hat dies neben offenen Datenschutzfragen sicher u. a. auch mit der Systeminfrastruktur und ihren Kosten sowie mit der Durchsetzbarkeit solcher Verfahren zu tun.

In der Diskussion ist immer wieder die streckenbezogene Autobahn-Maut für LKW. Hier sind die technischen Gegebenheiten (z. B. Nutzung von GPS und Mobilfunk) anders als im Bereich von PKW und Motorrädern. Ob und inwieweit wirklich der Persönlichkeitsschutz in diesem Bereich der fast ausschließlich beruflichen Nutzung weniger beeinträchtigt wird, muß spätestens kurz vor der Einführung solcher Systeme geklärt werden.

Für den PKW-Bereich wird spätestens dann die Maut-Diskussion neu geführt werden,

- wenn die Elektronik und Computerisierung im Fahrzeug sowie die (Mobil-) Kommunikation mit dem Fahrzeug weiter fortgeschritten ist,
- wenn Systeme der Verkehrstelematik größere Verbreitung gefunden haben (u. a. Staumfahrung, Leitsysteme mit elektronisch gespeicherten Straßenkarten, Diebstahlschutz bzw. Ortung von (gestohlenen) Fahrzeugen, Notruf, elektronische Geldbörse etc. für Park(-haus)gebühren) und
- wenn damit geringere (zusätzliche) Infrastrukturkosten entstehen.

1.1 Sonstige Überwachungssysteme für Verkehrsmittel

Als Beispiele für sonstige Überwachungssysteme für Verkehrsmittel seien hier die Systeme zur Verkehrslenkung, zur Standortbestimmung und zur Ermittlung, Verarbeitung und Weitergabe anderer Daten, z. B. bei Taxiunternehmen, Autovermietern, Speditionen, Bussen und Privatfahrzeugen, genannt.

Eine Überwachung von Verkehrsmitteln ist auf vielfältige Weise möglich:

- Videoüberwachung (z. B. an verkehrsreichen Kreuzungen),
- Überwachung durch andere elektronische Einrichtungen außerhalb der Fahrzeuge (z. B. Induktionsschleifen, Lichtschranken),
- Einrichtungen im Fahrzeug, die bei Bedarf zu Hilfe genommen werden (Fahrtenschreiber),
- Einrichtungen im Fahrzeug, die über Funk abgefragt werden können (Standortbestimmungen über Bakensysteme oder GPS, Funksprechverkehr, sonstige Daten wie Geschwindigkeit, Motorkontrolle usw.)

Von besonderer Bedeutung sind neuere Entwicklungen zu Einrichtungen im Fahrzeug, die über Funk abgefragt werden können (z. B. bei Taxizentralen in Hamburg oder Kassel). Alternative, datenschutzfreundlichere Technologien, die den erforderlichen Funktionsumfang abdecken, sind nicht erkennbar. Vielmehr muß im Einzelfall überprüft werden, ob der Funktionsumfang tatsächlich erforderlich ist. So ist zu prüfen, ob tatsächlich eine Überwachung per Funk durch die Zentrale notwendig ist oder ob eine passive Nutzung etwa von GPS durch den Fahrer ausreicht. Ebenso ist zu erfragen, ob Videoüberwachungen tatsächlich erforderlich sind oder ob eine Überwachung durch Induktionsschleifen usw. ausreicht.