

Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“

Autoren:

Thomas Jandach (Der Landesbeauftragte für den Datenschutz Baden-Württemberg), Marit Köhntopp (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Ursula Meyer zu Natrup (Berliner Datenschutzbeauftragter), Peter Schaar (Der Hamburgische Datenschutzbeauftragte), Wilfried Seiffert (Der Niedersächsische Landesbeauftragte für den Datenschutz), Kurt Urban (Der Landesbeauftragte für den Datenschutz Brandenburg), Andreas Waldenspuhl, René Weichelt (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern), Holger Weigel (Der Hessische Datenschutzbeauftragte), Franz-Josef Wesener (Federführung), Michael Wilms (Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen).

Datenschutzfreundliche Technologien in der Telekommunikation

1 EINLEITUNG.....	3
2 MODELLE UND KRITERIEN.....	4
2.1 TK-DATENMODELL.....	4
2.2 DATENSPARSAMKEITSMODELL – ELEMENTE ANONYMER NUTZUNG	6
2.3 BEWERTUNGSSCHEMA FÜR ANONYME NUTZUNG VON TK-SYSTEMEN	7
3 TELEKOMMUNIKATIONS DATEN IN NETZEN UND MEDIEN	9
3.1 ZUSAMMENHANG VON KONTEXTDATEN UND NUTZUNG.....	9
3.2 INTEGRATED SERVICES DIGITAL NETWORK (ISDN).....	10
3.3 X.25-DIENSTE	11
3.4 BREITBANDKOMMUNIKATION	12
3.5 ATM.....	13
3.6 ZELLULARE MOBILFUNKNETZE	13
3.7 INTERNE TELEKOMMUNIKATIONSANLAGEN	16
3.8 DECT	17
3.9 SATELLITENKOMMUNIKATION.....	19
3.10 INTERNET	20
4 MÖGLICHKEITEN DER DATENVERMEIDUNG UND -REDUZIERUNG.....	22
4.1 SCHUTZ VON SENDER UND EMPFÄNGER.....	22
4.1.1 Verteilung von Nachrichten	22
4.1.2 Bedeutungslose Nachrichten: Dummy Traffic.....	23
4.1.3 Überlagerndes Senden nach David Chaum: DC-Netz	23
4.1.4 Mixe.....	23
4.1.5 Verhinderung der Peilbarkeit	26
4.1.6 Änderung des Aufenthaltsmanagements	26
4.2 DATENMINIMIERUNG BEI DER ENTGELTABRECHNUNG	27
4.2.1 Einsatz von Chipkarten für die Bezahlung von Telekommunikationsdienstleistungen	27
4.2.2 Elektronisches Geld zur Bezahlung von Telekommunikationsdienstleistungen	29
4.2.3 Möglichkeiten zur Reduzierung oder zur völligen Vermeidung der Speicherung von Verbindungsdaten für Abrechnungszwecke	29
4.2.4 Möglichkeiten zur Minimierung von Bestandsdaten	31
4.2.5 Datenminimierung bei Entgeltabrechnungen an Nebenstellenanlagen	32
4.2.6 Zusammenfassende Bewertung.....	32
5 HANDLUNGSEMPFEHLUNG.....	33
1 ATM	37
2 ZELLULARE MOBILFUNKNETZE.....	37
3 DECT.....	40
4 SATELLITENKOMMUNIKATION.....	43
5 TCP/IP ALS GRUNDLAGE ZUM INTERNET.....	44
6 SCHUTZ VON NACHRICHTENINHALTEN.....	50
7 ANWENDUNG DES DATENMODELLS FÜR WÄHL- UND FESTVERBINDUNGEN IM DIGITALEN FESTNETZ	50

Datenschutzfreundliche Technologien in der Telekommunikation

1 Einleitung

Die globale Informations- und Kommunikationslandschaft des 21. Jahrhunderts gewinnt an Struktur. Die Neuordnung und Liberalisierung der Telekommunikation (TK) in Deutschland wird Ende 1997 abgeschlossen sein. Die Akteure des boomenden Telekommunikationsmarktes sind bereits heute dabei, sich ihren Marktanteil in einem harten Wettbewerb zu erkämpfen. „Mitspieler“ oder besser „Betroffene“ sind alle, die telefonieren, fernsehen, fernkopieren, Briefe, Texte und Dokumente über Datenleitungen schicken oder Telebanking oder Teleshopping betreiben. Moderne Telekommunikationstechnik bringt es mit sich, daß deren Benutzerinnen und Benutzer immer mehr elektronische Spuren hinterlassen ohne zu wissen, welche Daten an welchem Ort, für welche Dauer und für welchen Zweck gespeichert werden. Mit den Datenspuren wächst die Gefahr des Mißbrauchs und der Zusammenführung von Telekommunikationsdaten zu komplexen Persönlichkeitsprofilen.

„Ein konsequenter Datenschutz zählt zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft“ ist Erkenntnis und Handlungsversprechen der Bundesregierung in ihrer Initiative „Info 2000 - Deutschlands Weg in die Informationsgesellschaft“. Für die Einlösung dieses Versprechens reichen bisherige Sicherheitsansätze nicht aus. Bisher wurden Integrität, Verfügbarkeit und Vertraulichkeit der Daten zum Schutz der Hersteller und Betreiber von Informations- und Kommunikationstechnik präferiert. Zukünftig ist der Schutz der persönlichen Daten der einzelnen und damit der Schutz der informationellen Selbstbestimmung in den Vordergrund zu stellen. Dies muß bereits beim Design und bei der Entwicklung technischer Systeme geschehen. Hierbei ist Datenvermeidung und, wenn dies nicht möglich ist, weitgehende Datensparsamkeit anzustreben. Begriffe wie Anonymisierung und Pseudonymisierung werden zunehmend eine große Rolle bei der Kommunikationssicherheit spielen.

Es ist zu begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes den Grundsatz der Datenvermeidung normieren. Damit sind zukünftig Ausgestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten, keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Weitere wichtige Grundsätze sind, daß die Anonymität der Nutzerinnen und Nutzer soweit wie möglich gewahrt werden muß und daß, soweit die Erhebung und Nutzung von personenbezogenen Daten im Rahmen eines Vertragsverhältnisses erfolgt, dies nur unter strenger Zweckbindung im Rahmen des Vertragszwecks geschehen darf. Zum Schutz der personenbezogenen Daten ist im übrigen sicherzustellen, daß durch geeignete technische Maßnahmen der nicht autorisierte Zugriff auf diese Daten ausgeschlossen wird. Diese wichtigen Datenschutzgrundsätze sind auch in das allgemeine Telekommunikationsrecht zu übernehmen.

Das vorliegende Arbeitspapier versucht Kriterien für datenschutzfreundliche Technik zu definieren, es beschreibt die bei verschiedenen Telekommunikationsdiensten anfallenden personenbezogenen Daten und gibt Hilfestellung bei der Bewertung von neuen Telekommunikationslösungen. Es zeigt auf, daß datenschutzfreundliche Technologien auf dem Gebiet der Telekommunikation heute bereits zur Verfügung stehen. Die Darstellung der Lösungsmöglichkeiten beschränkt sich bewußt auf Beispiele der Datenvermeidung und Datenreduzierung. So wird z. B. das wichtigste Sicherungsverfahren zur Gewährleistung von Vertraulichkeit - die Verschlüsselung - nur erwähnt, nicht jedoch ausführlich dargestellt. Anbieter höherer Dienste (ab Schicht 5 des OSI-Modells) werden ebenfalls nicht besonders behandelt.

Das Arbeitspapier wurde von den Arbeitskreisen „Technische und organisatorische Datenschutzfragen“ und „Medien“ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt. Es ist als Orientierungshilfe für Datenschutzbeauftragte und Entscheidungsträger bei Systementscheidungen gedacht. Es wendet sich auch an Hersteller von Telekommunikationsanlagen, an Netzbetreiber sowie an Telekommunikationsdiensteanbieter und fordert sie auf, möglichst anonyme oder zumindest datensparsame Lösungen zu entwickeln und bereitzustellen. Weiter kann es als Information für eine datenschutzbewußte Öffentlichkeit dienen.

Das Arbeitspapier basiert auf dem veröffentlichten technischen Stand vom Frühjahr 1997. Es erhebt keinen Anspruch auf Vollständigkeit. So konnten einige Berichtsteile nicht mit der wünschenswerten Tiefe dargestellt

werden, da einige angesprochene Hersteller bzw. Diensteanbieter erbetene Informationen nicht bzw. nicht ausreichend geliefert haben. Es ist beabsichtigt, das Arbeitspapier bei neuen Erkenntnissen, Entwicklungen und Erfahrungen fortzuschreiben. Änderungs- und Erweiterungsvorschläge werden gerne entgegengenommen.

2 Modelle und Kriterien

2.1 TK-Datenmodell

Telekommunikationsdaten werden in der folgenden Untersuchung nach ihrer (potentiellen) Dynamik und ihrem Zweck unterteilt. Dabei wird in Kauf genommen, daß die verwendeten Begriffe in Rechtsvorschriften (z. B. §§ 4 - 6 Telekommunikationsdienstunternehmen-Datenschutzverordnung [TDSV], § 3 Telekommunikationsgesetz [TKG]) teilweise anders definiert bzw. benutzt werden. So umfaßt die Definition von Verbindungsdaten in § 5 TDSV auch Daten, die verarbeitet werden, ohne daß der Teilnehmer die Absicht hat, eine Telekommunikationsverbindung aufbauen zu wollen, oder ohne daß eine Verbindung zustande kommt. Solche Daten werden im folgenden unter Verbindungsvorbereitungsdaten gefaßt. Außerdem enthält § 6 TDSV keine Definition von Entgeltdaten; vielmehr wird vorausgesetzt, daß zur Berechnung dieser Daten die Verbindungsdaten im Sinne der TDSV, also noch unter Einschluß von Verbindungsvorbereitungsdaten, herangezogen werden müssen.

Diesem Arbeitspapier liegt die nun folgende Gliederung der Telekommunikationsdaten zugrunde. Die Beispiele zu den Datenarten dienen dabei zur Erläuterung. In vorhandenen und geplanten Telekommunikationssystemen müssen nicht alle Datenarten und nicht alle Beispieldaten anfallen.

Inhaltsdaten

Inhaltsdaten sind Daten, deren Übermittlung der Zweck der TK-Verbindung ist. Inhaltsdaten werden immer in einer bestimmten Codierung übermittelt. Der Codiervorgang selbst (z. B. Filterung mit Bandpass, Modulation, Digitalisierung) ist teilweise ein Netzdienst. Inhaltsdaten können sich deshalb nur auf die Art der Kommunikation beziehen (Sprache, Daten, Kurzinformationen [Pager]). Zu unterscheiden ist, ob es sich um eine analoge oder um eine digitale Übertragung handelt, ob eine dienstebezogene Verbindung (FAX, Mail, Internet, etc.) vorliegt oder eine transparente Übertragung zu einem vorbestimmten Partner genutzt wird (Datex-P, ISDN, Satellitenfestverbindung etc.). Für die Nutzung ist es wichtig, ob die übertragenen Daten zwischengespeichert, überprüft oder anderweitig bearbeitet werden.

Kontextdaten

Unter Kontextdaten werden die Daten verstanden, mit denen zu Zwecken der Telekommunikation umgegangen wird, die aber von den Inhaltsdaten verschieden sind. Es wird zwischen statischen und dynamischen Kontextdaten unterschieden. **Statische Kontextdaten** sind die klassischen Bestandsdaten, also diejenigen Daten, die kaum veränderlich sind und sich auf das Vertragsverhältnis zwischen Kunden und TK-Dienstleister beziehen. Unter dem Begriff **dynamische Kontextdaten** werden die Kontextdaten zusammengefaßt, die nicht nur ausnahmsweise zeitlichen Veränderungen unterworfen sind.

Bestandsdaten

Die obige Definition von Bestandsdaten entspricht inhaltlich der in § 4 TDSV. Diese Datenart läßt in digitalen Netzen teilweise Rückschlüsse auf die verwendeten Endgeräte (z. B. durch die Festlegung der benutzbaren Dienstarten) bzw. die Benutzungsstruktur (z. B. gewähltes Tarifmodell) zu. Als Bestandsdaten sind die Informationen aus den Antragsformularen und Erfassungsbögen zu Grunde zu legen :

- Informationen über einen Teilnehmer bzw. über einen Verbindungspartner
(Frau / Herr / Firma; Nachname; Vorname; Straße, Hausnummer; Postleitzahl, Ort; Telefonnummer; Mail-Adresse; Personalausweis-, Reisepaß-Nr., Meldebescheinigung; Immatrikulationsbescheinigung (bei Studententarif); Geburtsdatum; Staatsangehörigkeit)
- Vertragskonditionen
(Vertragslaufzeiten; Tarifart; Anschlußart; technische Anforderungen; vertragliche Leistungen; Support; Entstörung; Zahlungsmodalitäten [z. B. Kreditkarte]; Geldinstitut; Bankleitzahl; Kontonummer; Abrechnungsmodus)

- Besonderheiten
(Zusatzleistungen; Verbindungsart; Dienstleistungen, bevorzugte Telefonnummern)
- Technische Bestandsdaten
zu verwendende Normen
Profile (zugelassene Verbindungsarten und Leistungsmerkmale)
Authentifizierungsdaten

Verkehrsdaten

Verkehrsdaten sind Daten, mit denen der TK-Dienstleister umgeht, um Netzbetreuung durchführen zu können. Bereits an dieser Stelle sei angemerkt, daß Verkehrsdaten nicht personenbezogen zu sein brauchen. Der TK-Dienstleister benötigt nur Auslastungsdaten verschiedener Netzressourcen. Da auch Ressourcen zur Verarbeitung von Verbindungsvorbereitungsdaten notwendig sind, kann auch diese Datenart zu Verkehrsdaten verdichtet werden. Verkehrsdaten können nicht mehr Informationen enthalten als Verbindungsdaten und Verbindungsvorbereitungsdaten. Zu den Verkehrsdaten können gehören:

- Statussignalisierung: Überlastung, Normal, kein Betrieb
- Fehlermeldung: Ausfall, Defekte, Warnmeldungen, Unzulässigkeiten
- Auslastungsangaben: Zeitverlauf, Häufigkeit, Umfang
- Teilnehmerverhalten: Übertragungsart, Rufnummern, Zeiten, Reihenfolge
- Angaben zur Verbindungsqualität: Bitfehlerraten, bei Funkverbindungen auch Feldstärken

Diese Daten können von verschiedenen Kommunikationsbereichen angefordert werden (Vermittlungskomponenten, Netzzugänge, Kommunikationswege, Endgeräte, Kommunikationspartner).

Entgeltdaten

Entgeltdaten sind Daten, die die Ressourcenbenutzung durch einzelne Teilnehmer nach bestimmten Regeln widerspiegeln. Sie werden aus Verbindungsdaten oder Bestandsdaten abgeleitet. Es ist denkbar, daß auch Verbindungsvorbereitungsdaten zu Entgeltdaten verarbeitet werden. Entgeltdaten unterliegen einer größeren Veränderung als Verkehrsdaten. Sie können nicht mehr Informationen enthalten als Verbindungsdaten, Verbindungsvorbereitungsdaten und Bestandsdaten. Aus diesen Informationen können die Entgeltdaten zusammengestellt werden.

- Verbindungsdaten: Teilnehmerkennung, Anzahl der Verbindungen, Dauer der Verbindungen, Zeiten, Impulse, Volumen
- Verbindungsvorbereitungsdaten: Aufenthalt, Berechtigung, Teilnehmerverhalten, Signalisierung, Benachrichtigungs- und Speicheroptionen
- Bestandsdaten: Verbindungspartner, Vertragskonditionen, Zahlungsmodalitäten und Besonderheiten.

Verbindungsdaten

Zu Verbindungsdaten zählen ausschließlich Daten, die zum Aufbau, zum Aufrechterhalten und zum Abbau von tatsächlich aufgebauten Verbindungen benutzt werden. Dazu gehören insbesondere Signalisierungsdaten, die den genannten Zwecken dienen, sowie Daten über die gewählten Routen. Sofern der Aufenthaltsort in einem Netz zum Routing herangezogen wird, sind die entsprechenden Lokalisationsdaten, die anlässlich einer Verbindung verarbeitet werden, gleichfalls Verbindungsdaten. Verbindungsdaten können sein:

- Versions- und Satzkenung,
- Fernmeldekontonummer (Nummer des anrufenden Anschlusses), Kennung des rufenden Teilnehmers,
- Zielrufnummer, Kennung des gerufenen Teilnehmers,
- Kartenummer und Standortkennung (bei Verwendung von Telefonkarten),
- Funkzelle oder andere Lokalisationsinformation bei Mobilfunkteilnehmern,
- Datum und Uhrzeit des Beginns und des Endes der Verbindung,
- Gesprächsdauer,

- verwendetes Kommunikationsprotokoll (z. B. ITR6),
- Dienstekennung (Sprache, Daten, Fax, ...),
- Dienstmerkmale (insbes. Art des genutzten Dienstes, z. B. Sprachtelefon),
- Transaktionskennung (z. B. Dienstwechsel innerhalb einer Verbindung),
- Verbindungsart (ankommend, abgehend, Notruf),
- Zusatzdienste,
- Zähler für (im D-Kanal) übertragene Nachrichten zwischen beiden Teilnehmern,
- Tarifikennung,
- Datenvolumen.

Verbindungsvorbereitungsdaten

Mit Verbindungsvorbereitungsdaten werden die Daten bezeichnet, die verarbeitet werden, um die Erreichbarkeit eines TK-Teilnehmers zu gewährleisten, ohne daß tatsächlich TK-Verbindungen aufgebaut werden. Solche Daten sind potentiell besonders dynamisch, da sie auch in den Zeiten Änderungen unterliegen können, in denen der TK-Teilnehmer keine Verbindungen herstellt bzw. zuläßt. Zu Verbindungsvorbereitungsdaten können z. B. Lokalisationsdaten und Daten über die momentane Erreichbarkeit, wie Anrufumleitungen, Anrufbeantworter-/Faxbox-/Mailboxzustände, Erreichbarkeit nur für bestimmte Personen etc. gehören. Die Inhalte der Verbindungsvorbereitungsdaten setzen sich aus folgenden Informationen zusammen:

- Endgeräte Kennung,
- Authentifizierungscode,
- Diensteanforderung,
- Erreichbarkeit des Sender/Empfängers (z. B. nach „Einbuchen“),
- Wege / Umwegelenkung,
- Regelung von Netzübergängen,
- Lokalisation.

In vielen Fällen sind Teilmengen der Daten aus der oben angegebenen Klassifikation bei verschiedenen an der Telekommunikation beteiligten Stellen gespeichert. Dabei sind unterschiedliche Verteilungsmodelle denkbar. Besonders problematisch sind die Konstellationen, die mehrere Netzbetreiber und Vermittler umfassen. Dies ist insbesondere für die Telekommunikationskunden zumeist nicht transparent, d. h. nicht durchschaubar.

2.2 Datensparsamkeitsmodell – Elemente anonymer Nutzung

Kriterien für die Sicherheit in der Informationstechnik umfassen traditionell keine Mechanismen, die der Datenvermeidung und Reduktion personenbezogener Daten im Verarbeitungsprozeß dienen. Nach klassischem Verständnis sind die Festlegungen über Art und Umfang der zu verarbeitenden personenbezogenen Daten vorgegeben und durch die Systemverantwortlichen nicht veränderbar. Inzwischen wurden jedoch Konzepte ausgearbeitet, die verallgemeinerbare Anforderungen zum Datenschutz aus technischer Sicht widerspiegeln. Die meisten Kriterienkataloge für den technischen Datenschutz resultieren aus einer Systemsicht, die die Betroffenen mit umfaßt („Gesamtsystem“). Hierzu ist es sinnvoll, eine geeignete Schnittstelle zu definieren, an der eine Kommunikation zwischen dem Betroffenen und dem eigentlichen System („Kernsystem“) stattfindet. Zu betrachten wären dann die Kommunikation zwischen Betroffenenem und System sowie die Datenverarbeitung innerhalb des Systems. Diese Betrachtungsweise macht deutlich, daß der Betroffene sich dem System in verschiedener – möglicherweise nicht personenbezogener – Weise präsentieren kann. Hinsichtlich des Personenbezuges der „von außen“ in das Kernsystem eingegebenen Daten sowie der im Kernsystem vorgenommenen Modifikationen an diesen Daten kann daher ein Modell aufgestellt werden, das Kriterien beinhaltet, die den Grad der anonymen Nutzungsmöglichkeit beschreiben und nach absteigendem Datensparsamkeitsgrad angeordnet werden.

Datenvermeidung

Es gelangen keine personenbezogenen Daten in das Kernsystem. Auch der Betroffene kann seine eigenen Spuren im System nicht wiedererkennen.

Benutzerkontrollierte Pseudonymisierung

Der Betroffene benutzt selbstgenerierte, nur durch ihn reidentifizierbare Transaktionspseudonyme. Die drei Merkmale Selbstgenerierung, Reidentifizierung nur durch den Betroffenen, transaktionsorientierte Pseudonymgenerierung (d. h.: für jede Transaktion ein neues Pseudonym) sind konstitutiv. Daraus folgt, daß diese Pseudonymisierung vor Eintritt in das Kernsystem erfolgen muß. Wird auch nur auf eines von den o. g. Merkmalen verzichtet, so ist der Grad der Datensparsamkeit einer solchen Pseudonymisierung, auch wenn sie vorab erfolgt, lediglich so einzustufen wie der einer „sonstigen Pseudonymisierung“ (s. u.).

Anonymisierung

Darunter wird eine rücknahmefeste Prozedur verstanden, die personenbezogene Daten nach ihrem Anfallen im Kernsystem in der Weise verändert, daß sie keinen Personenbezug mehr aufweisen. Sofern von diesen (harten) Kriterien abgewichen wird, ist kein stärkerer Schutz als durch „sonstige Pseudonymisierung“ zu erwarten. Eine Aufweichung ist durch alle unter diesem Punkt genannten Fehler möglich. Die hier gegebene Definition der Anonymisierung entspricht dem herkömmlichen Verständnis dieses Begriffs.

Sonstige Pseudonymisierung

Wenn die Pseudonymisierung erst im System erfolgt, dann kann eine Reidentifikation in Abhängigkeit von folgenden Faktoren erfolgreich sein:

- Der Betroffene ist auf Grund einer geringen Teilnehmerzahl identifizierbar.
- Verschiedene Transaktionen desselben Betroffenen können verkettbar sein.
- Der Zeitpunkt der Pseudonymisierung kann zu spät gewählt sein; dies wäre der Fall, wenn die Pseudonymisierung erst nach dem Ablauf der datenschutzrechtlich brisanten Verfahrensschritte erfolgen würde.
- Im übrigen könnte die Pseudonymisierung gestört oder nachträglich aus dem System entfernt werden. (Dies betrifft die Integrität und die Rücknahmefestigkeit.)

Die **sonstige Pseudonymisierung** bildet hinsichtlich des Grades an Datensparsamkeit quasi ein Auffangbecken für alle Pseudonymisierungsformen, die nicht den oben aufgestellten Anforderungen für die „benutzerkontrollierte Pseudonymisierung“ genügen.

Vertraulichkeitssicherung

Sofern aus bestimmten Gründen keine, den obigen Datensparsamkeits-Kriterien entsprechende Methode angewendet werden kann, bleibt nur noch die (klassische) Vertraulichkeitssicherung der verbliebenen personenbezogenen Daten. Diese letzte Sicherungsstufe ist insbesondere bei Referenz- und Einwegpseudonymen notwendig; hier werden Referenzlisten und Schlüssel von parametrisierten Einwegfunktionen zu schützen sein.

Diese Abstufung in 5 Kategorien kann aber nicht als strenge Ordnung betrachtet werden. Sie hängt sehr stark von der Umsetzung der einzelnen Prinzipien, also der Qualität ihrer Implementierung ab. So ist z. B. eine „starke“ Implementation einer nachträglichen Pseudonymisierung meist datenschutzfreundlicher als eine „schwache“ Implementierung einer Anonymisierung; z. B. kann die frühzeitige innerhalb des Kernsystems erfolgende Vergabe kurzlebiger Pseudonyme für die Rechte Betroffener weniger einschränkend sein, als eine Anonymisierung, die erst nach einem Jahr erfolgt. Unter gleichen Bedingungen ist jedoch die Anonymisierung der sonstigen Pseudonymisierung vorzuziehen.

2.3 Bewertungsschema für anonyme Nutzung von TK-Systemen

Das TK-Datenmodell und das Datensparsamkeitsmodell können kombiniert werden, um ein Hilfsmittel zur Bewertung von bestehenden und geplanten TK-Systemen zu erhalten. Zur Anwendung des Datensparsamkeitsmodells muß eine geeignete Schnittstelle zwischen Betroffenen und System gewählt werden. Das Kernsystem wird dabei in der Weise abgegrenzt, daß die Schnittstelle zwei verschiedene „Vertrauensbereiche“ trennt. Unabhängig von dem physischen Anschluß wird eine logische, virtuelle Verknüpfung zu dem Teilnehmer/Endgerät hergestellt. An der Schnittstelle werden wichtige Prüfungen, wie die Authentifikation des Teilnehmers (bzw. des Endgerätes), gewisse Berechtigungsprüfungen etc., vorgenommen. Die Ergebnisse dieser Prüfungen werden dann innerhalb des Vertrauensbereiches in der Regel nicht erneut kontrolliert. Da die Abgrenzung zwischen dem „**Kern-**“ und dem „**Gesamt-**“ **System** logischer Art ist, könnten Teile des Vertrauensbereiches des Teilnehmers physisch beim Betreiber des TK-Systems lokalisiert

sein. Umgekehrt könnten sich auch Teile des Vertrauensbereiches des Netzbetreibers beim Nutzer befinden, z. B. lokale Abrechnungsböden des Netzbetreibers beim Nutzer. Ausgehend von der Unterteilung eines (Gesamt-) Telekommunikationssystems nach

Teilnehmer - Endgerät - TK-Netz

können die beiden ersten Elemente dem Bereich des Betroffenen und das letzte Element dem Bereich des Kern-Systems zugeordnet werden. Die Schnittstelle besteht somit zwischen dem Endgerät und dem eigentlichen TK-Netz. Im Festnetz ist die Anschlußdose die definierte Schnittstelle. Im Mobil- und Satellitenfunk bildet die (erste) Luftübertragungsstrecke die Schnittstelle.

Die oben eingeführte Einteilung ist auch in der übrigen Datenkommunikation anwendbar. So ist z. B. bei dem Paketvermittlungsdienst X.25 der Übergang zwischen der Datenendeinrichtung (DTE) und der Datenverbindungseinrichtung (DCE) die Schnittstelle. Auch für TK-Systeme, die auf höheren ISO/OSI-Schichten aufbauen, kann diese Trennung durchgeführt werden. Ein Internet-Provider etwa, der einen Internet-Zugang über Wählverbindungen gestattet, läßt beim Zugriff auf den POP-Mail-Server automatisch prüfen, ob eine Zugriffsberechtigung besteht – unabhängig von der Verbindungsart (z. B. PPP direkt zum Provider oder über eine TCP-Verbindung von einem anderen Rechner aus). Hier ist also der Mail-Server die Schnittstelle.

Mit Hilfe der folgenden Matrix können Systeme in der Weise bewertet werden, daß für jede Datenart der erreichte Grad an anonymer Nutzung ermittelt wird (siehe Beispiel im Anlage 7). Je weiter links in der Tabelle die Bewertung erfolgt, desto datenschutzfreundlicher ist dieses Profil. Sind die Bewertungen für alle Datenarten in der ersten Spalte zu finden, so liegt der Idealfall einer anonymen Nutzungsform vor.

	Daten- vermeidung	Benutzerkontroll ierte Pseudonymisierung	Anonymisierung	Sonstige Pseudonymisierung	Vertraulichkeit ssicherung
Bestandsdaten					
Verkehrsdaten					
Entgeltdaten					
Verbindungsdate n					
Verbindungsvorb ereitungsdaten					

Die Spaltenüberschriften ergeben sich direkt aus dem Datensparsamkeitsmodell. Die Zeilenbeschriftungen folgen dem TK-Datenmodell. Die Inhaltsdaten wurden nicht übernommen, da der übermittelte Inhalt von der Gestaltung des TK-Systems bis auf Codierung und Verschlüsselung nicht direkt beeinflußt wird. Insofern könnte für die Inhaltsdaten nur die Vertraulichkeitssicherung bewertet werden.

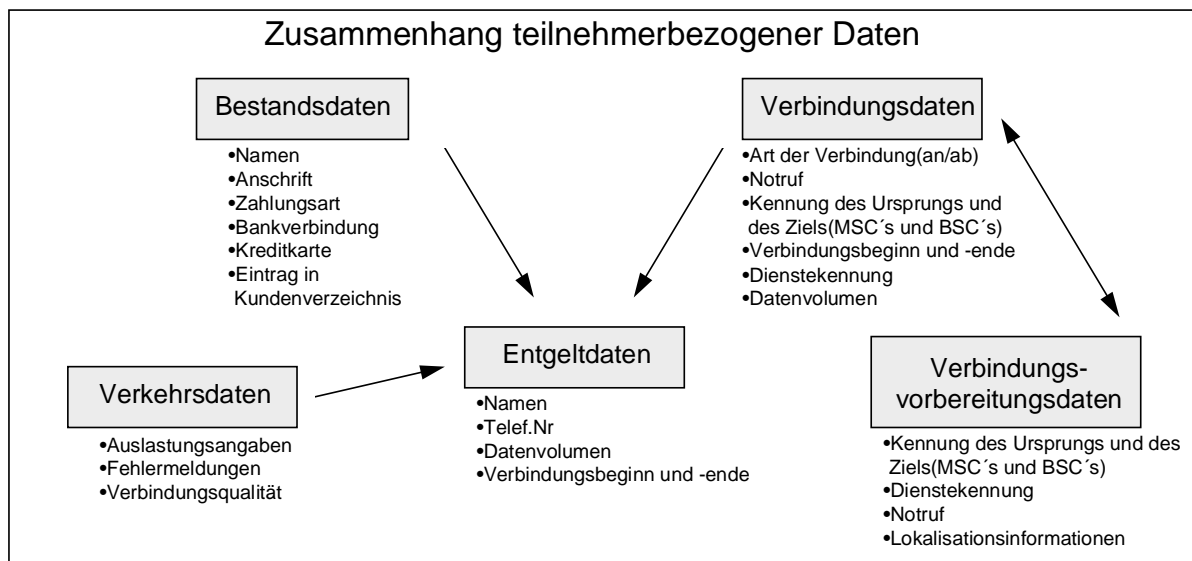
Als Ergebnis erhält man ein „Datensparsamkeitsprofil“. Wenn die Matrix als Planungshilfsmittel verwendet wird, können sich für ein System je nach Implementation verschiedene Profile ergeben. Ferner ist es u. U. möglich, in einer Datenart Verbesserungen auf Kosten einer anderen zu realisieren.

Die oben beschriebene Methodik läßt sich gleichermaßen auf leitungsvermittelnde und paketvermittelnde Dienste anwenden.

3 Telekommunikationsdaten in Netzen und Medien

3.1 Zusammenhang von Kontextdaten und Nutzung

Kontextdaten entsprechend den Definitionen aus Kapitel 2.1 werden sowohl für den ordnungsgemäßen Ablauf einer Kommunikation, wie auch bei der Erstellung und Überwachung der Netze und Abrechnungen genutzt. Art und Umfang der Datensammlung, sowie deren Verteilung und Auswertung werden von den jeweiligen Netzbetreibern bestimmt.



Voraussetzung für die Nutzung eines TK-Netzes ist die Freischaltung der entsprechenden Ressourcen durch die Netzbetreiber. Hierzu ist im allgemeinen der Abschluß eines Vertragsverhältnisses und in der Folge daraus die Speicherung von **Bestandsdaten** erforderlich.

Bevor es zu einer Kommunikationsverbindung zwischen den Teilnehmerinnen und Teilnehmern in einem TK-Netz kommt, laufen Funktionen ab, um die Möglichkeit der Kommunikation vorzuprüfen. Hierbei werden **Verbindungs-vorbereitungsdaten** benötigt, die sich auf Berechtigungen, Identifizierungen und Erreichbarkeit aber auch auf technische Vorprüfungen der Verbindung beziehen können. Diese Daten können in den aktiven Kommunikationskomponenten der Netztechnik vorgehalten werden oder auch bei Bedarf über den Netzverbund zusammengestellt werden.

Wird eine Verbindung hergestellt, fallen für den Aufbau, die Aufrechterhaltung und den Abbau **Verbindungsdaten** an, die unabhängig von den Inhaltsdaten und den Bestandsdaten von allen und zwischen allen Beteiligten ausgetauscht werden müssen, damit eine ordnungsgemäße Kommunikation zustande kommen kann. Hierbei kann auf die Verbindungs-vorbereitungsdaten zurückgegriffen werden, so daß diese eine Teilmenge der Verbindungsdaten werden.

Zur Erstellung der Rechnungen werden **Entgeltdaten** ermittelt, die sich aus den Verbindungs-vorbereitungs- und Verbindungsdaten ergeben. Sie werden mit den aus den Bestandsdaten erforderlichen Daten in Verbindung gebracht und in einen den Anforderungen der Kundinnen und Kunden oder den Erfordernissen des Anbieters benötigten Zusammenhang gestellt.

Zur Netzbetreuung werden von den TK-Dienstleistern **Verkehrsdaten** gesammelt. Aus ihnen ist die Auslastung der Netzressourcen ersichtlich. Die Daten werden aus den Übertragungsverfahren und Protokollen, durch einen eigenen Informationsaustausch zwischen den technischen Einrichtungen gebildet, die zum Betrieb

der TK-Dienstleistung notwendig sind. Abhängig von den eingesetzten Mitteln sind diese Daten an verschiedenen Stellen oder aber an einer zentralen Stelle verfügbar.

3.2 Integrated Services Digital Network (ISDN)

Das ISDN (Integrated Services Digital Network) ist ein Netz zur transparenten Übertragung beliebiger Daten. Die Inhaltsdaten werden über sogenannte Basiskanäle (B-Kanäle) mit einer Übertragungsrate von je 64 kbit/s übertragen.

Die Verbindungen werden über miteinander kommunizierenden Vermittlungseinrichtungen hergestellt, die sogenannten **vermittelnden Netzknoten** (VNK). An den VNK gibt es sowohl digitale Anschlüsse (ISDN-Anschlüsse) als auch analoge Anschlüsse (ANIS).

Der Verbindungsaufbau und die Steuerung der Verbindung erfolgen über einen Zeichengabe- bzw. Signalisierungskanal (D-Kanal), der beim ISDN-Basisanschluß im Zeitmultiplex-Verfahren über dieselbe Kupferzweidrahtleitung geführt wird wie die **B-Kanäle**. Die Zeichengabekanäle bilden ein eigenes logisches Netz, wobei ein Zeichengabekanal für viele B-Kanäle die Steuerungsnachrichten übertragen kann. Durch die von den Inhaltsdaten getrennte Signalisierung wird es z. B. möglich, daß auch während einer bestehenden Verbindung einem Teilnehmer der Verbindungswunsch eines Dritten signalisiert wird, wobei dessen Anschlußnummer und ggf. weitere Informationen auf einem Display angezeigt werden. Die Konventionen für die Übertragung von Steuerungsinformationen im ISDN sind im sog. **D-Kanal-Protokoll** festgelegt, welches die drei unteren Schichten des OSI-Referenzmodells abdeckt. Neben der deutschen Variante (1TR6) unterstützt das von der Telekom betriebene ISDN auch den europäischen D-Kanal-Standard EDSS1 (European Digital Subscriber Signalling System Number One).

Beim Verbindungsaufbau von einem digitalen Endgerät des A-Teilnehmers (Anrufer) überträgt dieses über den D-Kanal eine Setup-Protokoll-Daten-Unit (PDU) an den VNK, an die der A-Teilnehmer angeschlossen ist (A-VNK). Der A-VNK schaltet - zusammen mit den übrigen beteiligten VNK - einen D-Kanal zum angewählten B-Endgerät. Sofern das B-Endgerät frei ist, wird ihm der Verbindungswunsch (die Setup-PDU) signalisiert und ein B-Kanal geschaltet, auf dem die Teilnehmer transparent Daten übertragen können.

In sämtlichen beteiligten VNK werden für die Dauer der Verbindung und bei Verbindungsversuchen die kompletten Quell- und Zielrufnummern und weitere - dienstebezogene - Verbindungssteuerungsdaten gespeichert. Soweit die Verbindungssteuerungsdaten an das Endgerät des B-Teilnehmers übertragen werden, können sie von diesem weiterverarbeitet werden - auch dann, wenn eine Verbindung nicht zustande gekommen ist, weil z. B. die verfügbaren B-Kanäle besetzt waren. Die A-Rufnummer wird von dem B-VNK nicht an den B-Teilnehmer übertragen, wenn der A-Teilnehmer für seinen Anschluß die Rufnummernanzeige ausgeschlossen hat.

In den VNK entstehen bei Nutzung bestimmter ISDN-Dienstmerkmale zusätzliche Verbindungsvorbereitungsdaten und Verbindungsdaten. So wird bei der Rufumleitung die Rufnummer des Umleitungsziels gespeichert. Bei Fangschaltungen werden im B-VNK die Verbindungsdaten des A-Teilnehmers gespeichert, der die Verbindung aufgebaut hat.

Für jede erfolgreiche Verbindung wird in dem für den A-Teilnehmer zuständigen VNK mindestens ein Kommunikationsdatensatz erzeugt. Wenn während einer bestehenden Verbindung ein Dienstwechsel erfolgt, wird ein weiterer Datensatz angelegt. Wenn keine Verbindung zustande kommt, wird kein Kommunikationsdatensatz angelegt; die Verbindungsvorbereitungsdaten werden gelöscht.

Der Kommunikationsdatensatz enthält folgende Informationen:

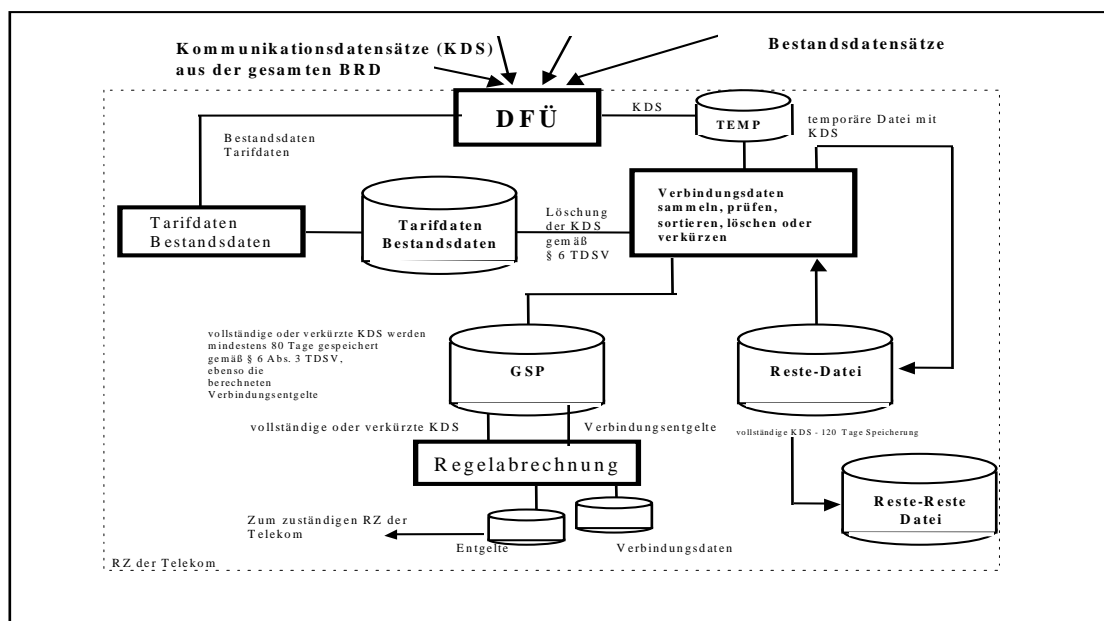
- Versions- und Satzkennung,
- Fernmeldekontonummer (Nummer des anrufenden Anschlusses),
- Zielrufnummer,
- Datum und Uhrzeit des Beginns und des Endes der Verbindung,
- Gesprächsdauer,
- verwendetes Kommunikationsprotokoll (z. B. 1TR6),
- Dienstmerkmal (insb. Art des genutzten Dienstes, z.B. Sprachtelefon),
- Transaktionskennung (z. B. Dienstwechsel innerhalb einer Verbindung),
- Tarifkennung,
- Zähler für im D-Kanal übertragene Nachrichten zwischen beiden Teilnehmern.

Eine Besonderheit stellen Verbindungen dar, die mittels Telefonkarten hergestellt werden. In den Datensatz solcher Verbindungen fließen zusätzlich die jeweiligen Standortkennungen der Kartentelefone ein.

Die Kommunikationsdatensätze werden in den VNK in relationalen Datenbanken gespeichert. Die benutzte Software zur Kommunikationsdatenerfassung enthält standardmäßig Module zur bloßen Summenzählung, Rufnummernkürzung und Zuordnung zu Tarif- und Zeitzonen. Es besteht also keine technische Notwendigkeit, für Abrechnungszwecke oder für Verkehrsmessungen die vollständigen Kommunikationsdaten in den VNK zu speichern. Spätestens beim Formatieren der Daten könnten die Einzelinformationen entsprechend aggregiert oder gekürzt werden.

Die Kommunikationsdatensätze (KDS) werden mindestens einmal täglich mittels File-Transfer an ein spezielles Rechenzentrum (RZ) der Telekom übersandt; in den A-VNK sind sie somit maximal 24 Stunden gespeichert.

Aus den verarbeitungsfähigen KDS werden im RZ täglich die Verbindungsentgelte errechnet und - geordnet nach Fernmeldekontonummer (FKTO) und genutzten Diensten - in einem kumulierten Gebührenspeicher (GSP) abgelegt. Einmal monatlich wird der Inhalt des GSP per File-Transfer oder per Magnetband an die für die Erstellung und den Versand der Telefonrechnung zuständigen Rechenzentren versandt. Unmittelbar nach Berechnung der Entgelte werden die KDS - je nach Kundenwunsch (TDSV § 6 Abs. 4) - entweder gelöscht oder um die letzten drei Stellen der angerufenen Nummer gekürzt oder vollständig für weitere mindestens 80 Tage gespeichert. Die Speicherdauer von 80 Tagen liegt dann vor, wenn die KDS am Vortag vor Verschickung des GSP erzeugt, von den A-VNK übermittelt und abgerechnet wurden. KDS, die zu Beginn der laufenden Abrechnungsperiode erzeugt wurden, werden max. 80 plus x Tage gespeichert, wobei x max. 30 Tage (ein Abrechnungszyklus) betragen kann. Dies entspricht den Regelungen der TDSV § 6 Abs. 3 (siehe Bild).



Nicht verarbeitungsfähige KDS z. B. bei Unplausibilitäten der Bestandsdaten, werden in der „Reste-Datei“ gespeichert und einem neuen Verarbeitungszyklus zugeführt. Dies wird in der Hoffnung nach Ergänzung oder Korrektur der Bestandsdaten 120 Tage lang erneut versucht, um damit das Entgelt einem gültigen FKTO zuordnen zu können. Datensätze, die auch nach dieser Zeit noch nicht verarbeitungsfähig sind, werden in eine andere Datei (Reste-Reste-Datei) umgespeichert. In der Vergangenheit hat die Telekom die Reste-Reste-Datei nach einer angemessenen Frist, ohne die Datensätze in Rechnung zu stellen, gelöscht.

3.3 X.25-Dienste

In paketvermittelten Netzen nach dem CCITT-X.25-Standard (hierzu gehört als wichtigster deutscher Dienst das von der Deutschen Telekom AG betriebene Datex-P) werden zwischen den Teilnehmern keine

Leitungsverbindungen geschaltet; die Verbindungen sind vielmehr virtuell, d. h. die Datenpakete können auf unterschiedlichen Wegen vom Sender zum Empfänger geleitet werden.

Der Datex-P Dienst wird von der Deutschen Telekom zum Teil im Rahmen der ISDN-Infrastruktur abgewickelt (so sind z. B. in dem Vermittlungssystem S12 ISDN- und X.25-Funktionalitäten gekoppelt; der Zugang zu Datex-P ist über B- und D-Kanäle des ISDN möglich).

Die Administration von X.25-Netzen kann auf unterschiedliche Weise erfolgen. Der Datex-P Dienst der Deutschen Telekom wird zentral von einem Datennetzkontrollzentrum (DNKZ) administriert. Hier werden neben den Gebührendaten laufend System- und Statistikdaten des Netzes gesammelt und ausgewertet. Zu den Aufgaben des DNKZ gehört u. a. die Pflege von Teilnehmerkennungen und Anschlußdaten. Die Daten werden zunächst unsortiert in Datenbanken gesammelt, ohne das ein unmittelbarer Bezug zum Teilnehmer vorliegt. Ohne zusätzliche technische Maßnahmen lassen sich auch keine Kommunikationsprofile der Teilnehmer erstellen.

Die Abrechnung kann in den X.25-Diensten auf unterschiedliche Art erfolgen. Hier wird beispielhaft das bei Datex-P benutzte Verfahren beschrieben. In der X.25-Vermittlungseinrichtung wird bei jeder Verbindung ein Gebührendatensatz erzeugt und am Ende der Verbindung an das DNKZ gesendet. Die Gebührendatensätze werden zunächst chronologisch abgelegt und anschließend von einem zentralen Datensammelrechner rufnummern- bzw. kennungsbezogen (bei DATEX-P20) sortiert und in Gebührenrechenzentren der Telekom mit den Bestandsdaten der Teilnehmer (Name, Anschrift) verknüpft.

3.4 Breitbandkommunikation

Überblick

Nach allgemeinem technischen Sprachgebrauch werden unter Breitbandkommunikation diejenigen Kommunikationsverbindungen eingeordnet, die mindestens die gleiche Übertragungsgeschwindigkeit benötigen, die auch für die Übertragung eines Videobildes in Echtzeit notwendig ist (2 Mbit/s). Dabei geht man davon aus, daß künftig alle breitbandigen Übertragungsdienstleistungen im Breitband-ISDN auf der ATM-Technologie beruhen werden. Im ATM sind alle Anwendungen der vermittelten Breitbandkommunikation enthalten.

Für die weitere Betrachtung werden noch die verteilte Breitbandkommunikation (Kabelfernsehen), deren Weiterentwicklung und einige bemerkenswerte Sondernutzungen dieses Mediums erwähnt.

Entstehung von Telekommunikationsdaten

Beim herkömmlichen Kabelfernsehen werden bei den Netzträgern nur **statische Kontextdaten**, also die **Bestandsdaten** wie Kundename, Anschrift und Bankverbindung sowie **Entgeltdaten**, die allerdings statisch an die Bestandsdaten gekoppelt sind, gespeichert. Die gleichen Daten können unabhängig vom Netzträger nochmals bei der Nutzung verschlüsselter Kanäle (Premiere) anfallen.

Bei der Nutzung digitaler Fernsehsendungen (Pay-per-View) entstehen, je nach eingesetztem Verfahren, dynamische **Entgeltdaten**, die zur Erstellung von Mediennutzungsprofilen geeignet sind (vgl. Entschlüsselung „Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen“ der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die vorbereitete Anlage des AK Medien).

Bei den vorhandenen Kupferkoaxial-Kabeln hat die technologisch bedingte Bandbreitenbegrenzung und die Gefahr der Störung anderer Telekommunikationssysteme zunächst die Entwicklung von Sondernutzungen gebremst. Dennoch wurden in der Vergangenheit verschiedene Projekte durchgeführt, bei denen unterschiedliche Abschnitte des vorhandenen Netzes für Anwendungen des Fernwirkens und -messens, der Videoübertragung, der Telefonie oder andere Telekommunikationsdienstleistungen Verwendung fanden (Rückkanal-techniken).

Mit der Nutzung dieser Dienste fallen dann ggf. weitere Daten an, die je nach Anwendung das ganze Spektrum des Datenmodells umfassen können und danach einer eigenen Einordnung bedürfen.

Weitere Entwicklung

Die weitere Entwicklung der Breitbandkommunikation ist derzeit schwer abzuschätzen, da der Ausbau sowie die Entwicklung neuer Technologien stark vom Bedarf und der Nachfrage abhängt. Eine mögliche Variante kann sich in Form des flächendeckenden Einsatzes von Breitbandkommunikation auf Basis von

Glasfasertechnologien ergeben. Damit kann die aufwendige Umrüstung vorhandener koaxialer Netze entfallen und es stehen dem Netzbetreiber alle digitalen Techniken für ein umfassendes Dienstangebot zur Verfügung. Dabei entstehen jedoch keine neuen Strukturen der Telekommunikation und die Einordnung in das bestehende Datenmodell kann auf Basis bisheriger Überlegungen erfolgen.

3.5 ATM

ATM steht für **A**synchroner **T**ransfer **M**odus und bildet die Technik, die dem Breitband-ISDN (B-ISDN) zugrunde liegt. Nutzungsmöglichkeiten sind beispielsweise Hochgeschwindigkeitsdatenübertragung, Bildtelefon, Videokonferenzen, Kabel-TV-Übertragung (CATV), Live- und Echtzeitanwendungen oder auch kombinierte Dienste. ATM bietet zur Zeit die relativ hohe Übertragungsgeschwindigkeit von 155 MBit/s, ein Ausbau auf 622 MBit/s bzw. 2,5 GBit/s ist geplant. Das ATM-Verfahren paßt sich flexibel der zu übertragenden Bandbreite an. Über eine Verbindung können Daten von verschiedenen Diensten zur selben Zeit zu unterschiedlichen Zielen geführt werden, z.B. für Multimedia-Anwendungen.

Seit 1994 werden Netzübergänge zu anderen Hochgeschwindigkeits-Netzen für verbindungslose und verbindungsorientierte Dienste aufgebaut; Netzübergänge zum Euro-ISDN und DATEX-P sind in Planung. ATM wird zumeist über Festnetze realisiert, es gibt jedoch ebenfalls ATM-Richtfunksysteme.

ATM und Sicherheit

ATM gewährleistet keine sichere Übertragung. So gibt es keine abschnittsweise Fehlersicherung, sondern lediglich Checksummen über die Headerinformationen. Ebenso fehlt eine abschnittsweise Flußsteuerung, die bei Überlast einzelner Strecken eine neue Wegewahl veranlassen könnte. Kommunikationsdaten fallen in ähnlichem Umfang wie bei ISDN an.

In bezug auf „Authentication“, „Confidentiality“, „Data Integrity“ und „Access Control“ erarbeitet das Technical Committee des ATM-Forums zur Zeit eine „Security Specification“, die im Entwurf vorliegt („Phase I ATM Security Specification (Draft)“, ATM Forum BTD-Security-01.02, April 1997). Ein Ziel ist beispielsweise die Verschlüsselung bei der Übertragung auf der Ebene des Zellstroms (alternativ Header- und Nutzdatenverschlüsselung oder nur Nutzdatenverschlüsselung) oder auf der Ebene des virtuellen Kanals (Ende-zu-Ende-Verschlüsselung der Nutzdaten). Wegen der hohen Geschwindigkeit ist auch eine schnelle Verschlüsselung mit der Möglichkeit eines schnellen Schlüsselwechsels erforderlich.

Bei den Vermittlungsstellen können Telekommunikationsdaten z. B. mitgelesen, kopiert oder umgeleitet werden. Für den Benutzer ist bislang der gewählte Weg für die Zellen durch das ATM-Netz nicht beeinflußbar oder transparent. So ist es dem Benutzer nicht möglich, einen Weg über Vermittlungsstellen seines Vertrauens zu erzwingen oder bestimmte Vermittlungsstellen explizit auszuschließen.

3.6 Zellulare Mobilfunknetze

Mobilfunknetze sind Telekommunikations-Netze, die eine drahtlose Kommunikation zwischen beweglichen Stationen (Teilnehmern) und Übergänge zu festen Stationen (Netzen) unterstützen. Sie werden heute für unterschiedliche Zwecke (z. B. Sprache, Daten, Kurznachrichten, Funkruf) benutzt. Allen Netzen gemeinsam ist die Signalübertragung mittels elektromagnetischer Wellen.

Wesentlicher Bestandteil der Mobilfunknetze ist eine Netztechnik, die eine **automatische Vermittlung**, eine **Gebührenaufzeichnung** und einen **Anschluß an das öffentliche Fernsprech-Festnetz** ermöglicht.

Modulare großflächige Netze sind zellular strukturiert. Das Prinzip besteht darin, daß das zu versorgende Gebiet in eine Vielzahl kleiner Zellen eingeteilt wird. In jeder Zelle wird eine Funkfeststation als Basisstation installiert. Mehrere Basisstationen werden über eine Funkvermittlungsstelle (MSC = Mobile-Switching-Center) mit dem öffentlichen TK-Netz verbunden. Die Steuerung im Netz muß dafür sorgen, daß zu jedem Zeitpunkt dem System bekannt ist, in welcher Zelle sich der mobile Teilnehmer befindet. Der hierfür erforderliche Datenaustausch der einzelnen MSCs erfolgt über Festnetze.

In Deutschland ist seit 1986 das **C-Netz** im Einsatz. Dieses Netz ist bereits ein zellulares Netz, arbeitet im 450-MHz-Frequenzbereich allerdings noch mit analoger Sprachübertragung. Im C-Netz ist jeder mobile Teilnehmer über eine einheitliche Zugangskennziffer 0161 mit nachfolgender siebenstelliger Rufnummer automatisch erreichbar.

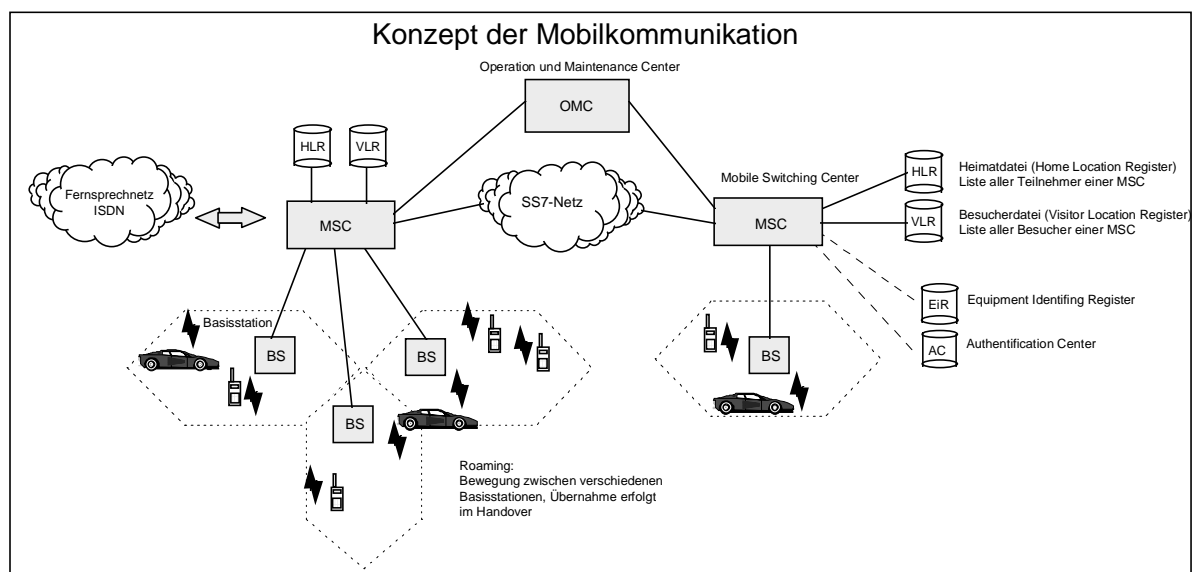
Eine weitere Stufe in der Entwicklung der Mobilkommunikation stellen digitale **GSM-Netze** (Global System Mobile) dar. Als GSM-Netze sind in Deutschland die Netze **D1 der Telekom**, **D2 von Mannesmann-Mobilfunk** eingeführt. Ein weiteres Mobilfunknetz ist mit dem **GSM1800-Netz E-plus von Thyssen** aufgebaut worden.

Zugangskennziffer:

D1-Netz	Deutsche Telekom MobilNet GmbH	0171
D2-Netz	Mannesmann Mobilfunk GmbH	0172
E-Plus-Netz	E-Plus Mobilfunk GmbH	0177
E2-Netz(ab 1998)	VIAG Interkom	0175

Das mobile Datenkommunikationssystem **Modacom** unterstützt die Datenübertragung im Paket-Modus. Die Schnittstelle zu den drahtgebundenen Teilnehmern und zu Hostrechnern (Datenbanken) bildet das öffentliche Datenpaketnetz Datex-P der Telekom. Die Vermittlung und Übertragung von Datenpaketen erfolgt im Datex-P Netz nach dem Protokoll X.25. Da in Funknetzen andere Bedingungen herrschen als in drahtgebundenen Netzen, sind auch andere Übertragungs- und Vermittlungsprotokolle anzuwenden. Modacom arbeitet mit dem RD-LAP (Radio Data Link Access Protocol). RD-LAP ist ein herstellereigenes Protokoll der Firma Motorola, dem Lieferanten für die Infrastruktur von Modacom.

Die Systemarchitektur und die dazu erforderlichen Netzkomponenten ähneln sehr dem Aufbau der zellularen Mobilkommunikationssysteme zur Sprachübertragung.



TK-Daten in Mobilfunknetzen

Die Speicherung der einzelnen Daten in den unterschiedlichen Mobilfunknetzen verläuft generell in gleicher Weise. Wie bei der Beschreibung der Inhalte des TK-Datenmodells ausgeführt, beruhen die Kontextdaten auf den Erfordernissen der technischen wie organisatorischen Bedingungen der jeweiligen TK-Netze. Bei den Mobilfunknetzen wird eine Aufgabenbearbeitung und damit auch eine Verteilung und ein Abgleich von Daten in verschiedenen Komponenten des Kernsystems durchgeführt. Die Zuordnung zum TK-Datenmodell ergibt sich wie folgt:

Inhaltsdaten

Die Übertragung der Inhaltsdaten in den Mobilfunknetzen erfolgt transparent zwischen den beteiligten Partnern. Eine Speicherung erfolgt lediglich bei der Nutzung von erweiterten Diensten (Mailbox, Anrufbeantworter, X.400 Gateway, ...). Es liegt somit in der Hand des Teilnehmers, welche Daten er in welcher Weise über das TK-Netz versendet.

Kontextdaten

Bestandsdaten sind alle Informationen über Teilnehmerinnen und Teilnehmer, die nach der Beantragung und Einrichtung durch den Telekommunikationsanbieter gespeichert wurden. Der Umfang der Daten und ihre Profile sind von den Netzbetreibern im Rahmen der gesetzlichen Vorgaben (TKG, TDSV) bestimmt.

Die Daten werden nur auf einem Datenverarbeitungssystem vorgehalten. Sie werden bei der einmaligen Erstellung der SIM-Chipkarte (Subscriber Identity Module) und des dazugehörigen symmetrischen geheimen Schlüssels, der Erstellung des Benutzerprofils (IMSI=International Mobile Subscriber Identification), sowie bei Bearbeitung der Abrechnungsdaten benötigt. Eine Untermenge dieser Daten werden als Bestandsdaten in jedem MSC (Mobile-Switching-Center) in den Bereichen der HLR (Home Location Register) und VLR (Visitors Location Register) hinterlegt. Das OMS (Operating and Maintenance System) bildet und verwaltet die Bestandsdaten über das Telefonverzeichnis und die Chipkarten.

Verbindungsvorbereitungsdaten werden in der Beglaubigungsinstanz **AC** (Authentication Center), in den HLRs und dem VLRs hinterlegt. Mit ihnen wird die Berechtigung, das Profil und der Aufenthalt jedes potentiellen Teilnehmers in bezug auf die angeforderten Dienste geprüft.

Verbindungsdaten

In der Mobilkommunikation ist auf Grund der Flexibilität der Endgeräte ein umfangreicher Datenbestand und eine dynamische Verwaltung und Verteilung dieser Daten erforderlich. Informationen zum Aufbau und zur Aufrechterhaltung einer TK-Verbindung müssen an die beteiligten Stellen gelangen. Von diesen sind alle zur Abrechnung erforderlichen Informationen zu sammeln und weiterzuleiten.

In der Besucherdatei **VLR** (Visitors Location Register) sind Daten über Teilnehmer gespeichert, die sich temporär im zugehörigen **MSC** (mobile switching center) -Bereich aufhalten. Es sind dies die von einer entfernten MSC übertragenen HLR-Daten.

Bei jeder Nutzung der Telekommunikationsdienstleistungen muß eine virtuelle Verknüpfung zwischen den beteiligten Instanzen gewährleistet sein. Hierzu sind die erforderlichen Verbindungs-/ Lokalisationsdaten von den Vermittlungskomponenten (MSC) zu erstellen, zwischenspeichern und an die Datennachverarbeitung weiterzuleiten. Hierzu muß eine Zuordnung der Teilnehmerprofile zu den Verbindungsdaten hergestellt werden.

Entgeltdaten

Die Erstellung und Sammlung aller hierfür benötigten Daten kann nur durch eine zentrale Bearbeitung erfolgen. Damit ist der Informationsaustausch aller hierzu erforderlichen Inhalte über das Netzwerk notwendig. Als Datenquellen dienen Informationen aus den Kommunikationskomponenten des Kernsystems der Mobilfunknetze (AC, MSC, OMC). Es werden die notwendigen Daten aus den Bestandsdaten (Name, Anschrift, Bankverbindung, ...), mit den Informationen aus Verbindungsvorbereitungs- und Verbindungsdaten (Art der Verbindung, Datenvolumen, Dienstekennung, ...) zur Erstellung einer Rechnung zusammengetragen.

Verkehrsdaten

Mit Hilfe der Betriebszentrale dem **OMC** (= **Operation and Maintenance Center**) können die Funktionen des Netzes überwacht und Fehler erkannt werden, um Reparatur- und Wartungsmaßnahmen zu veranlassen.

Das **OSS** (= **Operational Support System**) stellt den administrativen Teil des GSM-Netzes dar und wickelt die Verwaltung der Teilnehmer und der von ihnen beanspruchten Dienstleistungen ab. Es bildet die Datennachverarbeitung.

Beide Komponenten bilden zusammen das **OMS** (**Operating and Maintenance System**), das Betriebs- und Wartungssystem.

Mobilfunknetze und Sicherheit

Der Aufbau der Mobilfunknetze erfolgt in erster Linie mit dem Ziel, die geforderten Dienstleistungen zu erfüllen und eine funktionsgerechte Steuerung und Überwachung aller Aktivitäten für den Betreiber zu

ermöglichen. Datenvermeidung und mehrseitige Sicherheit haben bei der Systementwicklung keine Rolle gespielt.

Aus dieser Sichtweise sind die bislang realisierten Sicherheitsfunktionen und Schutzmechanismen entstanden. So bietet die IMSI (IMSI=International Mobile Subscriber Identification) die Sicherheit, daß das Fälschen von SIM-Karten unmöglich gemacht wird und über die IMSI eine vom System generierte und nur dem System bekannte Codierung als Kriterium für den Netzzugang existiert.

Die Art ihrer Ausgestaltung und die Nutzung eventuell erweiterter Schutzmechanismen wird nicht offengelegt und scheint kein werbewirksames Leistungsmerkmal für die Betreiber zu sein.

Folgende Schutzmechanismen sind zum Teil realisiert:

- Zugangsschutz auf Rechner, Datenbanken, Vermittlungsknoten
- Verschlüsselte Übertragung von
Nutzdaten vom Endgerät zur Basisstation
Verbindungsdaten (bekannt vom D1 Netz)
Abrechnungsdaten (bekannt vom D1 Netz)
- Persönliche Identifikationsnummer (PIN) für die Benutzung des Endgerätes
- Gerätebezogene Kennnummer mit Kontrolle im AC.

3.7 Interne Telekommunikationsanlagen

Zusätzlich zur Telekommunikation im öffentlichen Bereich werden geschäftlich interne Telekommunikationsanlagen eingesetzt, um betriebsintern und nach außen eine effektive und wirtschaftliche Kommunikation sicherzustellen. Die Anlagen speichern parallel zum Anbieter öffentlicher TK-Leistungen die Verbindungsdaten aller abgehenden Gespräche für eine eigene Gebührendatenverarbeitung. In bezug auf die Entgeltabrechnung besitzen private TK-Anlagen im allgemeinen folgende Leistungsmerkmale:

- Trennung der Telefonkosten der Mitarbeiterinnen und Mitarbeiter nach dienstlichen und privaten Gesprächen.
- Aufteilung der dienstlichen Telefonkosten auf mehrere innerbetriebliche Kostenstellen oder unterschiedliche Nutzerkreise der TK-Anlage.
- Zuordnung der privaten Telefonkosten auf die einzelnen Mitarbeiterinnen und Mitarbeiter mit der Möglichkeit des detaillierten Nachweises.
- Überprüfungsmöglichkeit der monatlichen Telefonrechnung des Anbieters der Telekommunikationsleistung.
- Möglichkeit der stichprobenartigen Kontrolle über die geführten dienstlichen Gespräche, um eine mißbräuchliche Nutzung der dienstlichen Fernsprecheinrichtungen für private Zwecke zu unterbinden.

Die meisten Hersteller von TK-Anlagen bieten ein sehr variables zweistufiges Verfahren zur Gebührendatenverarbeitung an. Bei diesem Verfahren werden in einer ersten Stufe alle Verbindungsdaten am Gesprächsende kurzzeitig in einem Verbindungsdatensatz in der TK-Anlage abgelegt. In einem zweiten Schritt werden sie dann in bestimmten Zeitintervallen - mindestens jedoch täglich - an einen separaten Gebührencomputer übermittelt und können dort in vielfältiger Weise selektiert, ergänzt und ausgewertet werden. Der Gebührencomputer speichert in der Regel für jedes abgehende dienstliche oder private Gespräch bis zum Ausgleich der Rechnung einen Gebührendatensatz, der im Grundbestand den Entgeltdaten des TK-Datenmodelles entspricht, wobei herstellerbedingte Abweichungen möglich sind.

Während der Gebührenabrechnung erfolgt in den meisten Anlagen eine Zuordnung der Gebührendatensätze zu einer Stammdatendatei (Bestandsdaten), die zum Teil auch als internes Telefonverzeichnis genutzt wird.

Wie die Gebührenabrechnungen konkret vorgenommen werden und welche Ausdrücke zulässig sind, ist in Dienstanschlußvorschriften oder Fernsprechvorschriften und Dienstvereinbarungen mit Personal- oder Betriebsräten sehr unterschiedlich geregelt. Die einzelnen Hersteller der Telekommunikationsanlagen bieten in

ihrer Gebührendatenverarbeitung meist ein umfangreiches Spektrum unterschiedlicher Auswertelisten an, aus denen der Nutzer entsprechend seiner konkreten Bedürfnisse auswählen kann.

Ähnlich wie in öffentlichen Netzen können bei komplexen TK-Netzgruppen Netzwerkmanagementprodukte eingesetzt werden, die eine umfangreiche Verkehrs- und Nutzungskontrolle ermöglichen.

3.8 DECT

Begriff

DECT steht für **D**igital **E**uropean (**E**nhanced) **C**ordless **T**elecommunication. DECT ist der neueste und modernste Standard für schnurlose Telefone. Er wurde 1985 von der CEPT beschlossen und wird seit 1991, beruhend auf den entsprechenden Standards des ETSI (European Telecommunications Standards Institute), in vielen technical reports erläutert. ETSI hat die Entwicklung von europäischen Telekommunikationsstandards von CEPT übernommen. DECT unterstützt u. a. folgende Merkmale (ausführliche Darstellung im Anhang):

Qualität

- hohe Sprachqualität
- Möglichkeit der Datenübertragung
- flexible Datenratenzuteilung
- vom Mobilteil ausgehende, dynamische Kanalauswahl und unterbrechungsfreier Kanalwechsel (seamless handover)
- Möglichkeit des Telefonierens bei gleichzeitiger Ortsveränderung mit einer Geschwindigkeit von bis zu 20 km/h

Sicherheit

- Abhörsicherheit durch Nutzung von Chiffrieralgorithmen (optional)
- Authentikation der Teilnehmer sowie der Mobil- und (optional) der Basisstationen
- Einrichtung von Zulassungsbereichen

Identitäts- und Informationsmanagement

- Möglichkeit zur kontext- und ortsabhängigen Vergabe mehrerer Identitäten pro Endgerät
- Möglichkeit des Endgerätes zur Unterrichtung der Feststation über seinen Ort und Zustand ohne Bestehen einer Verbindung

Interoperabilität

- Kommunikation zwischen den einzelnen an derselben Basisstation angemeldeten Endgeräten
- Möglichkeit zum Aufbau von Netzen aus mehreren Basisstationen
- Interworking mit dem öffentlichen Telefonnetz (analog und ISDN), GSM und X.25-Netzen
- europaweit einheitliche Frequenzen

Einsatzmöglichkeiten

DECT-Systeme sind vielseitig einsetzbar. Folgende Anwendungsbereiche kommen in Betracht:

- **Einzelapparat**

Ein DECT-System besteht aus einem Basis- und einem Mobilteil. Die Kommunikation zwischen Basis- und Mobilteil erfolgt digital, während das Basisgerät an das öffentliche Telefonnetz je nach Ausführung analog, also über die herkömmliche TAE-Dose, oder digital über einen ISDN-Anschluß, angebunden wird.

- **TK-Anlage**

Bei dieser Einsatzart besteht eine DECT-Anlage aus einem DECT-Basisgerät mit Telefonhörer und/oder mehreren Mobilteilen. Man erhält so eine interne TK-Anlage, da es mindestens zwei Endgeräte (mobil oder

Telefonhörer am Festgerät) gibt und eine interne Kommunikation zwischen ihnen möglich ist ohne Einbeziehung des TK-Netzes, an dem die DECT-Anlage angeschlossen ist.

Werden DECT-Systeme im Geschäftsbereich eingesetzt, so erhält jeder Mitarbeiter „sein“ Mobilteil, das durch einen Code auch so gesichert werden kann, daß nur er damit kommunizieren kann. Die im Geschäftsbereich eingesetzten DECT-Anlagen erlauben es auch in der Regel, jedem Endgerät eine eigene Nummer zuzuweisen. Die Zahl der an einer Basisstation anmeldbaren Endgeräte ist meist auf sechs bis acht beschränkt. Somit kommt ein aus nur einer Basisstation bestehendes DECT-System lediglich für kleine Firmen in Betracht.

Der DECT-Standard erlaubt es jedoch, mehrere Basisstationen zusammenzuschließen (siehe im einzelnen dazu die Anlage). Auf diese Weise können beliebig viele Endgeräte an eine DECT-Anlage angemeldet werden. Außerdem kann dadurch der Aktionsbereich eines Mobilteils erweitert werden, da bei Verlassen einer Zelle, welche durch die Reichweite ihres Basisgerätes bestimmt ist, das Gespräch nahtlos („seamless“) von einer anderen Zelle übernommen werden kann.

- **Ergänzung des GSM-Systems** [s. Anlage]

Sowohl DECT als auch GSM unterstützen die Mobilität beim Telefonieren. Da DECT im Gegensatz zu GSM nur eine kleine Fläche abdeckt, dafür aber eine hohe Teilnehmerdichte erlaubt, bietet sich eine Kopplung mit GSM durch die Verwendung sogenannter Dual-Mode-Geräte an. Diese Geräte funktionieren primär als DECT-Mobilteile, bis der Funkkontakt zur Basisstation abbricht, dann buchen sie sich in das GSM-Netz ein.

- **Drahtlose TK-Netz-Anbindung der einzelnen Teilnehmer (Wireless Local Loop)** [s. Anlage]

Mit Wireless Local Loop soll die „letzte Meile“ zwischen den Endknoten eines TK-Festnetzes und den einzelnen Teilnehmern kostengünstig überbrückt werden. Für den Einsatz von DECT sprechen u. a. die hohe Sprachqualität und Verkehrskapazität sowie der einfache Auf- und Ausbau. Die Realisierung erfolgt durch Ausstattung der Endknoten mit DECT-Basisstationen und auf Seiten der Teilnehmer durch auf die nächste Basisstation gerichtete Antennen mit angeschlossener TAE-Dose (schlichte Leitungsersetzung) oder direkt durch Verwendung der Mobilteile.

- **Telepoint**

Bei der Telepoint-Anwendung (in Deutschland nur im Versuchsstadium) hat der Nutzer die Möglichkeit, sich mit seinem schnurlosen Telefon an öffentlichen Funkfeststationen, z. B. bei Bahnhöfen, einzuwählen. Telepointssysteme beabsichtigen keine Flächendeckung, sondern bilden ein Netz von „Telefonzellen“, wobei zur Vermeidung von Konkurrenz mit dem Mobilfunk nur abgehende Gespräche erlaubt sind.

Aufgrund der stark zunehmenden Verbreitung von Mobilfunksystemen ist der Markt für Telepoints sehr klein geworden. Eine Wiederbelebung könnte der Einsatz von DECT als modernstes und flexibelstes Schnurlossystem anstelle der bisher verwendeten CT-Standards bringen. Dies kommt insbesondere bei der o. a. Integration von GSM und DECT in Betracht, da damit die jederzeitige Erreichbarkeit des Teilnehmers gewährleistet ist, gleichzeitig aber die Möglichkeit, kostengünstig über das Festnetz zu telefonieren, erweitert wird.

Personenbezogene Daten

Welche personenbezogenen Daten bei DECT-Systemen anfallen, hängt im wesentlichen von der Art ihres Einsatzes ab.

Wird lediglich ein **Einzelapparat**, also ein nur aus einem Basis- und einem Mobilteil bestehendes Gerät, eingesetzt, so fallen an der Schnittstelle zum öffentlichen TK-Netz die gleichen personenbezogenen Daten an wie bei einem herkömmlichen, an einer TAE-Dose angeschlossenen, analogen Telefon. Auch bei einer privaten DECT-TK-Anlage ergibt sich hierzu kein Unterschied. Innerhalb der Anlage kann die Anzahl der vertelefontierten Einheiten bzw. die aufgelaufene Gebührensumme je Endgerät gespeichert und angezeigt werden. Da die Endgeräte im allgemeinen nicht bestimmten Personen zugeordnet werden und keine endgerätebezogenen, von außerhalb anwählbaren Rufnummern vergeben werden, fallen auch bei einer privaten DECT-Anlage nicht mehr personenbezogene Daten an als bei einem herkömmlichen Telefon.

Geschäftliche **DECT-TK-Anlagen** mit mitarbeiterbezogenen Mobilteilen und endgerätespezifischen, von auswärts anwählbaren Rufnummern sind hinsichtlich der Leistungsmerkmale und des Anfalls personenbezogener Daten mit ISDN-TK-Anlagen vergleichbar. Daher werden mittlerweile auch kombinierte DECT-ISDN-Anlagen angeboten. Ein Unterschied besteht insoweit, als in einer ISDN-TK-Anlage die Endgeräte in der Regel ortsfest sind, wohingegen bei einer DECT-Anlage festgestellt werden kann, in welcher Zelle sich der Mitarbeiter aufhält. Wird das Verfahren des Anrufausrufs in jeder Zelle gewählt, kann auf die Speicherung der „Aufenthaltszelle“ verzichtet werden (siehe Anlage DECT - Zellenstrukturen).

Bei einer **Kopplung von GSM und DECT** via Dual-Mode-Handy ist maßgeblich über welches Netz gerade kommuniziert wird. Bei DECT ist dann wiederum zu prüfen, ob es sich um eine privates oder um ein geschäftlich eingesetztes System handelt. Die Kombination dieser beiden verschiedenen Systeme hat den Vorteil, daß wegen des immer möglichen Netzwechsels Profilbildungen erschwert werden.

Der **Wireless Local Loop** kann durch DECT entweder mittels direkter Vergabe von Mobilteilen an die Teilnehmer oder durch schlichte Leitungsersetzung realisiert werden.

Erhalten die einzelnen Teilnehmer Mobilteile, mit denen sie direkt über die DECT-Basisstation am zugehörigen Endknoten kommunizieren können, so besteht prinzipiell die Möglichkeit, daß ein Teilnehmer mittels seines Endgerätes Informationen über die anderen, an derselben Basisstation angemeldeten Teilnehmer erhält, z. B. über die angefallenen Gesamtkosten. Man kann aber davon ausgehen, daß die im WLL-Bereich eingesetzten DECT-Anlagen über diese Merkmale ebensowenig verfügen wie über die Möglichkeit zu kostenlosen Interngesprächen. Es bleiben dann noch die bei DECT vorhandenen Lokalisationsmöglichkeiten. Insoweit besteht auch ein Unterschied zu von den Teilnehmern eingesetzten DECT-Anlagen, da die dort entstehenden Lokalisationsinformationen im Bereich des Teilnehmers bleiben und nicht von dem angeschlossenen TK-Netz ausgewertet werden können. Bis auf die Lokalisationsdaten dürften die bei diesem Verfahren anfallenden personenbezogenen Daten trotz unterschiedlicher Technik mit den bei ISDN anfallenden vergleichbar sein. Dies gilt auch für das Verfahren der schlichten Leitungsersetzung, bei der jeder Teilnehmer seine eigene TAE-Dose hat.

Der Einsatz von DECT in **Telepoint**-Anwendungen, insbesondere in Kombination mit GSM ist hinsichtlich der entstehenden personenbezogenen Daten insgesamt ähnlich einem GSM-Netz zu bewerten, mit dem Unterschied, daß die Lokalisierbarkeit beim Einbuchen in einen Telepoint wegen dessen wesentlicher kleinerer Zelle deutlich höher ist als bei einer GSM-Zelle; dies trifft auch im Vergleich zu GSM1800 zu, da DECT eine geringere effektiv abgestrahlte Leistung benutzt. Eine andere Beurteilung ergibt sich, wenn das Einbuchen in die Telepoints anonym erfolgen kann. Dies wird auch beim GSM-Netz diskutiert (siehe Kapitel 4 - Datenminimierung bei Entgeltabrechnungen).

Generell ist zu beachten, daß in allen beschriebenen DECT-Einsatzbereichen ein Lokalisieren des Teilnehmers durch Außenstehende über die Richtungskomponente der gesendeten elektromagnetischen Wellen möglich ist. Unbefugte können Kommunikationsaktivitäten von Teilnehmern und deren Aufenthaltsort beobachten. Wird in Anlagen nicht das Verfahren des Anrufausrufs benutzt, so ist bereits ein Informationsgewinn unter Ausnutzung der Aktivmeldungen der Mobilteile möglich. In diesen Punkten ist somit jede DECT-Anwendung genauso zu bewerten wie GSM.

3.9 Satellitenkommunikation

Dem Einsatz von Satelliten kommt in der Telekommunikation eine ständig wachsende Bedeutung zu. Während Satelliten traditionell vor allem für Zwecke der Fernerkundung, der Verteilung von Radio- und Fernsehprogrammen und zum Herstellen von Telefonverbindungen über große Entfernungen hinweg benutzt wurden, dringen sie jetzt zunehmend auch in Bereiche vor, die bislang durch terrestrische Festnetz- oder Funkanlagen abgedeckt wurden, z. B. Mobiltelefonie und -datenübertragung. Zusätzlich wird das Angebot kontinuierlich um neue Dienste erweitert, die ohne Satelliteneinsatz bisher nicht möglich waren. Dazu gehören gegenwärtig vor allem Flottenmanagement-, Positionsbestimmungs- und Fernortungssysteme. Diese Dienste decken so unterschiedliche Bedürfnisse wie die Ortung gestohlener Fahrzeuge, Rationalisierung im Speditionsgewerbe und die Überwachung von Subventionsmaßnahmen auf EG-/EU-Ebene ab. Die Anzahl der Satellitenbetreiber, insbesondere aber die der Diensteanbieter vergrößert sich nach wie vor ständig.

Satellitenbetreiber

Das kontinuierliche Auftreten neuer Anbieter im Bereich der Satellitenkommunikation führt zu einer großen Unübersichtlichkeit des Angebots. Bei genauer Betrachtung sind die meisten Anbieter von Satellitendiensten jedoch keineswegs selbst Betreiber von Satelliten, sondern sie haben die Übertragungskapazitäten ihrerseits von anderen Unternehmern gemietet. Aufgrund des erheblichen Investitionsbedarfs für die Entwicklung und den Betrieb eines Satelliten sowie vor allem für den Transport in die Orbitposition gibt es nur relativ wenige Organisationen, die selbst Satelliten betreiben. Dabei handelt es sich meist um internationale Konsortien oder um nationale Fernmeldebehörden. Diese vermieten dann Transponderkapazität ihrer Satelliten an andere Unternehmen oder Behörden ("Signatare"), die darauf aufbauend Satellitenkommunikationsdienste am Markt anbieten.

Für die Ermittlung von Informationen zur Behandlung von TK-Daten in der Satellitenkommunikation waren lediglich Grundlagen recherchierbar. Eine Auskunft von den Betreibern über die Verarbeitung von Kontextdaten konnte nicht erreicht werden.

3.10 Internet

Das aktuell viel diskutierte Kommunikationsnetz Internet ist in seiner Ausprägung ein Sonderfall. Bei der Nutzung dieses weltweiten Verbundes von DV-Systemen gibt es eine Zahl von Risiken die keiner Regelung unterliegen (Zwischenspeicherung von Daten, Kookies, Profilerstellung, ...). Jeder Nutzer muß sich dessen bewußt sein und individuell eine mehr oder minder sichere Betriebsform wählen (nur Informationssuche, verschlüsselter Nachrichtenaustausch, Sicherheitssperren, ...)

Im folgenden wird ein Überblick über die Daten gegeben, die im Zusammenhang mit dem Zugang zum Internet auftreten können.

Eigener Internet-Anschluß

In größeren Einrichtungen existiert oftmals ein eigener Internet-Anschluß, z. B. in Universitäten ein WIN-Anschluß (Wissenschafts-Netzanschluß) über das Deutsche Forschungsnetz (DFN). Hier hängen die Rechner des lokalen Netzes „direkt“ am Internet, d. h., sie bilden ein Subnetz des Internets und sind damit Bestandteil des Internet. Jeder Rechner hat eine eigene IP-Adresse. Für die Kommunikation im Internet wird dementsprechend diese IP-Adresse als source address verwendet. Wird ein Rechner nur von einer Person benutzt, ist die feste IP-Adresse dieses Rechners als personenbeziehbares Datum zu sehen. Wird der Rechner von mehreren Personen genutzt (z. B. Workstation-Pools in Universitäten), ist eine eindeutige Zuordnung einer IP-Adresse zu einem Benutzer im Internet nicht mehr möglich.

Nutzung über einen kommerziellen Service-Provider

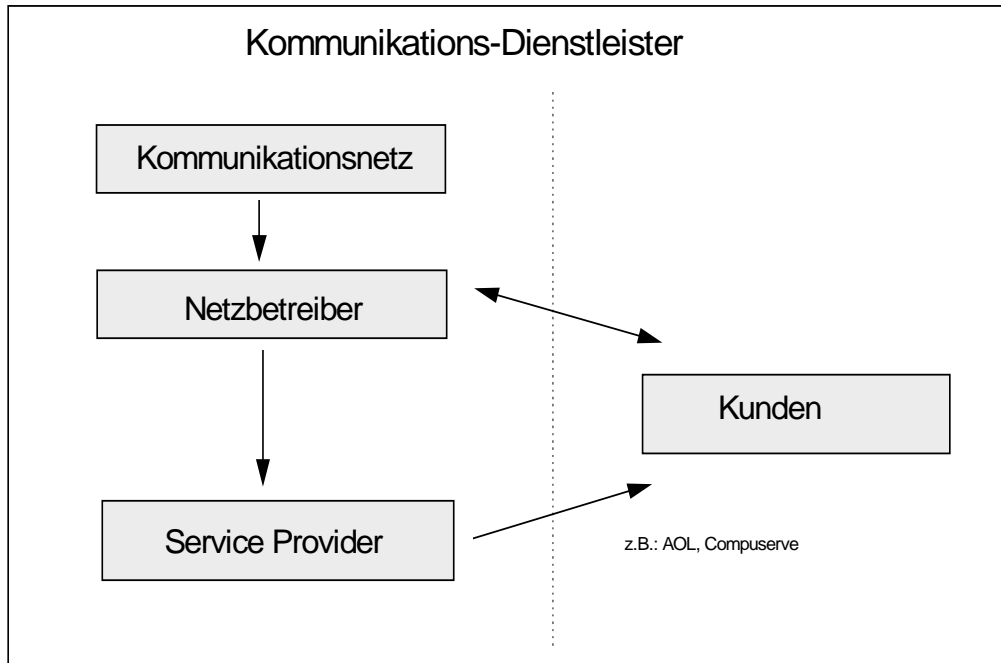
Die zweite Möglichkeit ist die Nutzung über einen Service-Provider. Dies kann und ist für den „normalen“ Nutzer im Normalfall ein kommerzieller Provider, der für seine erbrachte Leistung Geld verlangt. Für diesen Fall treten sowohl Bestands- als auch Abrechnungsdaten auf. Bei der Nutzung des Internet über einen Service-Provider wird dem Benutzer für die Dauer der Verbindung im Normalfall eine IP-Adresse aus einem IP-Adressenpool zugewiesen und ist daher von Verbindung zu Verbindung variabel. Durch die dynamische Zuweisung von IP-Adressen kann für die jeweiligen Nutzer z. B. kein Benutzerprofil durch Dritte auf Basis von IP-Adressen erstellt werden.

Als Bestandsdaten werden der Name, die Adresse, die Kontoverbindung oder Kreditkartennummer gespeichert. Freiwillige Angaben sind die Telefonnummer und der Beruf.

Bei den Abrechnungsdaten muß zwischen verschiedenen Varianten der Service Provider unterschieden werden. Einige Provider bieten für eine monatliche Pauschale die unbegrenzte Nutzung des Internet. Für diesen Fall sollten eigentlich keine Abrechnungsdaten anfallen. (Hier scheint es jedoch Ausnahmen zu geben. Eine Anfrage bei GlobalNet/IBM ergab, daß sie immer protokollieren, wer wann wie lange den Internet-Dienst nutzt. Für den Fall, daß eine bestimmte Stundenzahl im Pauschalbetrag enthalten ist, muß für jeden Benutzer (bzw. Account) protokolliert werden, wie lange er den Internet-Zugang jeweils nutzt (Beginn, Ende). Beim Überschreiten der im Pauschalbetrag enthaltenen Nutzungszeit, werden die Mehrkosten dem Benutzer in Rechnung gestellt, d. h., dem monatlichen Grundbetrag zugeschlagen und vom Konto abgebucht, überwiesen oder über die Kreditkarte abgerechnet. Die Speicherdauer dieser Abrechnungsdaten beträgt z. B. bei

GlobalNet/IBM 1Jahr. Die Aussage mehrerer Service-Provider war, daß die dynamisch zugeordnete IP-Adresse nicht protokolliert wird. Es kann jedoch sein, daß dies bei einigen Providern gemacht wird.

Eine weitere Variante besteht durch Serviceprovider die kein Entgelt für den Internetzugang verlangen, dafür aber das Recht beanspruchen, eine uneingeschränkte Verarbeitung und Nutzung der anfallenden Verbindungsdaten des Kunden zu bekommen (z. B. Germany.net).



Nutzung über einen nicht kommerziellen Provider

Stellt z. B. eine Universität ihren Mitarbeitern und Studenten auch Wähleingänge für Modems oder ISDN zur Verfügung, ist die Universität als Service-Provider zu betrachten, jedoch treten hier im Normalfall keine Abrechnungsdaten auf. Bei dieser Zugangsform werden für die Vergabe der IP-Adressen zwei Varianten verwendet. Im Normalfall wird auch hier dem Benutzer eine IP-Adresse dynamisch zugeordnet. Bei Nutzung von ISDN-Wähleingängen mit Überprüfung der rufenden Nummer werden jedoch auch feste IP-Adressen zugeordnet.

Für ISDN-Wähleingänge wird oftmals durch Überprüfung der übermittelten ISDN-Rufnummer die Zulässigkeit der Nutzung festgestellt. Für diesen Fall sind die berechtigten Rufnummern (und evtl. ihre Inhaber) als Bestandsdaten gespeichert.

Nutzung von „öffentlichen“ Internet-Terminals, z. B. in Internet-Cafes

Nutzung von „öffentlichen“ Internet-Terminals, z. B. in Internet-Cafes. Bei dieser Nutzungsform fallen im Normalfall keine Bestands- und Abrechnungsdaten an.

Der Benutzer zahlt im voraus für eine bestimmte Nutzungszeit, die dann per Systemzeitschaltuhr freigeschaltet wird. Durch den ständigen Wechsel der Nutzer ist eine Zuordnung von IP-Adressen zu Personen nicht möglich.

4 Möglichkeiten der Datenvermeidung und -reduzierung

4.1 Schutz von Sender und Empfänger

Derzeitige Netzstrukturen (Vermittlungsnetze) basieren darauf, Nachrichten zwischen den Teilnehmern an Telekommunikationsdiensten direkt zu vermitteln. Vor Herstellung einer Kommunikationsverbindung sind die Teilnehmerstationen daher zu identifizieren. Durch Einsatz dieser Technik wird das Kommunikationsverhalten leicht beobachtbar und auch kontrollierbar. Je schwächer die Netzbündelung zum Teilnehmer ausgeprägt ist, desto geringer ist der Aufwand, mit dem die Beobachtung vorgenommen werden kann. Bei den Mobilkommunikationsnetzen kommt hinzu, daß die Lokalisierungsinformation schnell wechseln kann, für einen Verbindungsaufbau aber der Aufenthaltsort aktuell bekannt sein muß.

Ein Schutz vor der Preisgabe des Kommunikationsverhaltens sowie des Senders und Empfängers wird dann erreicht, wenn Zeitpunkt, Dauer und Ort der Kommunikation nicht bekannt sind bzw. ermittelt werden können. Es sind deshalb Verfahren und Techniken zum Schutz der Verbindungs- und Lokalisationsdaten einzusetzen. Zu nennen sind die Änderung der physikalischen Netzstruktur durch Verwendung von Verteilnetzen, der Einsatz impliziter Adressierungsarten, die Mix-Technologie sowie in drahtlosen Netzen darüber hinaus das Verhindern der Peilbarkeit und der Teilnehmerortung. Um den Grad des Schutzes von Sender und Empfänger einschätzen zu können, konzentrieren sich die folgenden Bewertungen nach dem Datensparsamkeitsmodell auf Verbindungsdaten und ggf. Verbindungsvorbereitungsdaten.

4.1.1 Verteilung von Nachrichten

Wird insbesondere in teilnehmernahen Netzbereichen ein gleichmäßiges, kommunikationsunabhängiges Nachrichtenaufkommen erzeugt und werden die jeweiligen Nachrichten nicht direkt vermittelt, sondern in den gesamten Netzbereich eingestellt, kann ein Rückschluß auf das Kommunikationsverhalten Einzelner und den Abruf der Nachrichten nicht mehr unmittelbar erfolgen. Verteilnetze (Broadcasting) gestatten allen Teilnehmern, die Informationen aus dem Netz zu nehmen, die für sie bestimmt sind. Damit wird erreicht, daß die Empfänger vom Netz nicht mehr identifiziert werden können.

Im Gegensatz zu expliziter Adressierung, bei der die Adreßinformation zur Wegwahl im Netz verwendet wird, kann in Verteilnetzen jede Teilnehmerstation anhand bestimmter Merkmale (implizite Adresse) erkennen, welche Nachricht an sie gerichtet ist. Bei einer verdeckten Adressierung kann die Adresse nur vom Empfänger ausgewertet werden. Die Möglichkeit der Umsetzung besteht z. B. über Verschlüsselungssysteme, bei denen ein Schlüssel zwischen Kommunikationspartnern ausgetauscht wird und somit Nachrichten und Adressen nur mit Kenntnis des Schlüssels gelesen werden können. Eine andere Möglichkeit ist die Verwendung variabler Adressen, die zwischen den Partnern nach erstmaliger Verbindungsaufnahme vereinbart werden (z. B. durch Generierung mit Pseudozufallsgeneratoren).

Technisch bedeutet der Einsatz von Verteilnetzen eine ganz neue Verkabelungsstruktur in Breitbandtechnik. Die Vervielfachung des Nachrichtenvolumens auf allen Teilnehmerleitungen erfordert eine geeignete Bandbreite, um einen möglichst großen Datenstrom mit vielen Einzelnachrichten multiplexen zu können. Als beste Topologie bietet sich die Ringstruktur mit einem Tokenverfahren an, bei der die Nachrichten bei allen Teilnehmern vorbeilaufen. Aus Leistungs-, Zuverlässigkeits- und Kostengründen lassen sich für sehr viele Teilnehmer reine Verteilnetze bei Individualkommunikation nicht mehr sinnvoll einsetzen. Statt dessen bieten sich Vermittlungs-/Verteilnetze (VmVt-Netze) an, die hierarchisch organisiert sind [Pfit_85]. Solche VmVt-Netze bestehen aus Verteilnetzen im Teilnehmeranschlußbereich, die durch ein Vermittlungsnetz verbunden sind. Die Nachrichten werden dabei nicht an alle, sondern nur an hinreichend viele Teilnehmerstationen verteilt (Multicasting).

Bewertung

Bei Broadcasting für Mediendienste oder Individualkommunikation fallen keine Daten darüber an, welche der Teilnehmer Empfänger der Informationen sind. Es handelt sich also um eine Datenvermeidung bei der Empfängerinformation. Verdeckte Adressen entsprechen benutzerkontrollierten Pseudonymen.

Allgemeine Mediendienste sollten wegen des Schutzes der Empfängerinformation wie bisher über Verteilnetze realisiert werden. Auch bei Individualkommunikation könnte eine derartige Netzstruktur, zumindest in unteren hierarchischen Ebenen, eingesetzt werden, wenn gleichzeitig ein Schutz der Inhalte, z. B. durch Verschlüsselung, und eine nicht direkt auswertbare Adressierung gewährleistet ist.

4.1.2 Bedeutungslose Nachrichten: Dummy Traffic

Unter **Dummy Traffic** versteht man das Einbringen bedeutungsloser Zeichenfolgen in Netze zu kommunikationsarmen Zeiten, um ein gleichbleibendes Kommunikationsverhalten vorzutäuschen und damit ein Ausforschen zu verhindern. Das Einbringen der Zeichenfolge sollte vom Sender erfolgen, sie sollte von realen Nachrichten nicht unterscheidbar sein. Denkbar ist beispielsweise das Senden aller Teilnehmer zu einem festgelegten Zeittakt unabhängig davon, ob bedeutungsvolle Nachrichten verschickt werden sollen oder nicht. Der Schutz des Senders besteht darin, daß für das Netz nicht mehr entscheidbar ist, wann genau und wie viele bedeutungsvolle Nachrichten er sendet.

Das Verfahren ist am wirksamsten, wenn das gesamte Nachrichtenaufkommen über Verteilnetze oder Ringstrukturen abgewickelt wird, um Zuordnungen zu vermeiden. Weiterhin muß die Adressierung verschleierbar sein.

Bewertung

Dummy Traffic ist ein vielfältig einsetzbares Hilfsmittel, das in Kombination mit verschleierter Adressierung eine Identifikation der relevanten Daten nicht erkennen läßt. Durch diese Methode der zusätzlichen Datenproduktion wird der Effekt der Datenvermeidung bzgl. des senderseitigen Kommunikationsverhaltens erreicht. Damit kann diese Methode der zusätzlichen Datenproduktion als eine Art der Datenvermeidung aufgefaßt werden, da Informationen über das senderseitige Kommunikationsverhalten verschleiert werden.

4.1.3 Überlagerndes Senden nach David Chaum: DC-Netz

Die Methode des überlagernden Sendens [Chau_88] gewährleistet in einem beliebigen digitalen Netz, daß das Senden anonym geschieht. Es kann an beliebig vielen Stellen abgehört und manipuliert werden; dennoch ist es einem Angreifer nicht möglich, die gesendeten Nachrichten einer Station zu entschlüsseln. Die Teilnehmerstationen haben paarweise einen Schlüssel miteinander ausgetauscht und diesen Wert vor den anderen geheim gehalten. Auf Basis dieser Beziehung werden über die Nachrichten (sofern die Teilnehmerstation senden will) und Schlüssel bitweise Summen modulo 2 (Überlagerung) gebildet, die zur Identifizierung und Entschlüsselung der im Netz versandten Informationen dienen. Mit einer Erweiterung des überlagernden Empfangens kann das überlagernde Senden auch zum anonymen Empfangen genutzt werden [Pfit_90].

Bewertung

DC-Netze ermöglichen sowohl Sender- als auch Empfängeranonymität. Nach dem Datensparsamkeitsmodell ist das DC-Netz bei der benutzerkontrollierten Pseudonymisierung (wegen der geheimen Schlüssel der Teilnehmerstationen) oder sogar bei der Datenvermeidung (da relevante Daten für das Netz nicht erkennbar sind) einzuordnen. Allerdings sind DC-Netze aufwendig in ihrer Realisierung und nicht für die existierenden schmalbandigen Signalisierungskanäle geeignet.

4.1.4 Mixe

Mixe sind Netzknoten, die dem Schutz der Kommunikationsbeziehung dienen, indem sie die Verkettbarkeit zwischen Sender und Empfänger einer Nachricht verhindern. Dies wird durch das folgende, erstmals von David Chaum entwickelte Verfahren ([Chau_81]) erreicht (übersichtliche Darstellung in [FrJP_97]):

1. Sammlung eingehender Nachrichten
2. Umkodierung der Nachrichten
3. Ausgabe der Nachrichten in veränderter Reihenfolge an den nächsten (Mix-)Netzknoten bis zum Empfänger

Mit der Mix-Technik lassen sich folgende Eigenschaften (wahlweise oder kombiniert) realisieren:

- Unverkettbarkeit zwischen Sender und Empfänger einer Nachricht,
- Pseudonymität des Senders,
- Pseudonymität des Empfängers,
- Anonymität des Senders gegenüber Dritten,
- Anonymität des Empfängers gegenüber Dritten,
- Anonymität des Senders gegenüber dem Empfänger,
- Anonymität des Empfängers gegenüber dem Sender,
- Schutz weiterer Verbindungsdaten, z. B. Signalisierungsbeziehungen, Location Updates / Aufenthaltsinformationen (bei Mobilkommunikation), Beginn, Dauer oder Dienstart der Kommunikation.

Neben technischen Sicherheitsmaßnahmen ist für den Schutz erforderlich, daß ein Angreifer sich keinen Zugriff auf alle auf einem Kommunikationsweg verwendeten Mixe verschaffen kann. Dies wäre z. B. der Fall, wenn alle Mix-Betreiber kooperieren würden, um die Kommunikationsbeziehung von Sender und Empfänger aufzudecken. Mindestens einer der verwendeten Mixe muß also vertrauenswürdig sein. Daher sollten Mixe möglichst unabhängig entworfen und hergestellt werden sowie unabhängige Betreiber haben.

Funktion des Mix-Verfahrens

Um eine Zuordenbarkeit von ein- und ausgehenden Nachrichten zu verhindern, werden die Nachrichten gegebenenfalls auf gleiche Länge gebracht, z. B. in gleich große Abschnitte unterteilt oder aufgefüllt.

Das Umkodieren der Nachrichten erfolgt in der Regel mittels asymmetrischer Kryptographie: Jedem Mix ist ein Schlüsselpaar aus öffentlich bekanntem und dazugehörigem privaten Schlüssel zugeordnet. Die Nachrichten werden mit dem öffentlichen Schlüssel des Mixes verschlüsselt an ihn gesendet. Er entschlüsselt die Nachrichten vor dem Weiterleiten mit seinem privaten Schlüssel. Eine deterministische Umkodierung ist leicht von einem Angreifer auszunutzen, der die ein- und abgehenden Nachrichten beobachtet, indem er eine vom Mix ausgegebene Nachricht erneut mit dem öffentlichen Schlüssel des Mixes verschlüsselt. Dies entspricht dann wieder der Eingangsnachricht. Daher wird eine indeterministische Umkodierung gewählt: Der Nachricht wird ein zufälliger Teil beigefügt, den der Mix nach der Umkodierung entfernt. Hier bietet sich eine längentreue Umkodierung an.

Damit Replay-Angriffe (Wiedereinspielen derselben Nachrichten) keinen Erfolg haben, sind Wiederholungen von identischen Nachrichten zu ignorieren. Dies läßt sich beispielsweise dadurch erreichen, daß vom Mix Zeitstempel für die Nachrichten vergeben werden oder daß bereits gesendete Nachrichten über einen gewissen Zeitraum in einer Datenbank gespeichert werden.

Um die Unverkettbarkeit der ein- und ausgehenden Nachrichten zu erreichen, müssen genügend viele Nachrichten im Mixpuffer vorliegen. Ist dies nicht der Fall, kann der Mix bedeutungslose Dummy-Nachrichten (s. o.) erzeugen, die z. B. beim letzten Mix wieder aussortiert werden. Die Forderung nach genügend vielen verschiedenen Absendern, die sich nicht zu einem Angriff zusammenschließen dürfen, läßt sich technisch auch dann nicht befriedigend lösen, wenn die Absender verifizierbar wären. Doch auch hier bietet die Erzeugung von Dummies Abhilfe.

Für den Puffer des Mixes sind verschiedene Betriebsarten denkbar, z. B. der Batchbetrieb, bei dem alle Nachrichten weiterbearbeitet werden, sobald m Nachrichten im Puffer stehen, der Poolbetrieb, bei dem zufällig eine Nachricht aus dem Puffer zur Weiterbearbeitung ausgewählt wird, sobald die $(m+1)$ -te Nachricht eintrifft, oder auch Mischformen. Daneben kann sich die Steuerung an Latenzzeiten orientieren, z. B. vom Benutzer gewählte Verzögerungen (maximale oder minimale Wartezeiten) oder eine zufällige vom Mix ermittelte Dauer.

Da das Senden beobachtbar bleibt, könnte von den Teilnehmern gefordert werden, daß sie jeweils in einem bestimmten Zeittakt senden müssen und ggf. bedeutungslose Nachrichten erzeugen. Alle Teilnehmer, die zur selben Zeit senden, bilden dann die Anonymitätsgruppe.

Einsatzbereiche für Mixe

Für einige Bereiche der Telekommunikation existieren bereits Konzepte, wie das Mix-Verfahren zum Schutz der Kommunikationsbeziehung eingesetzt werden kann:

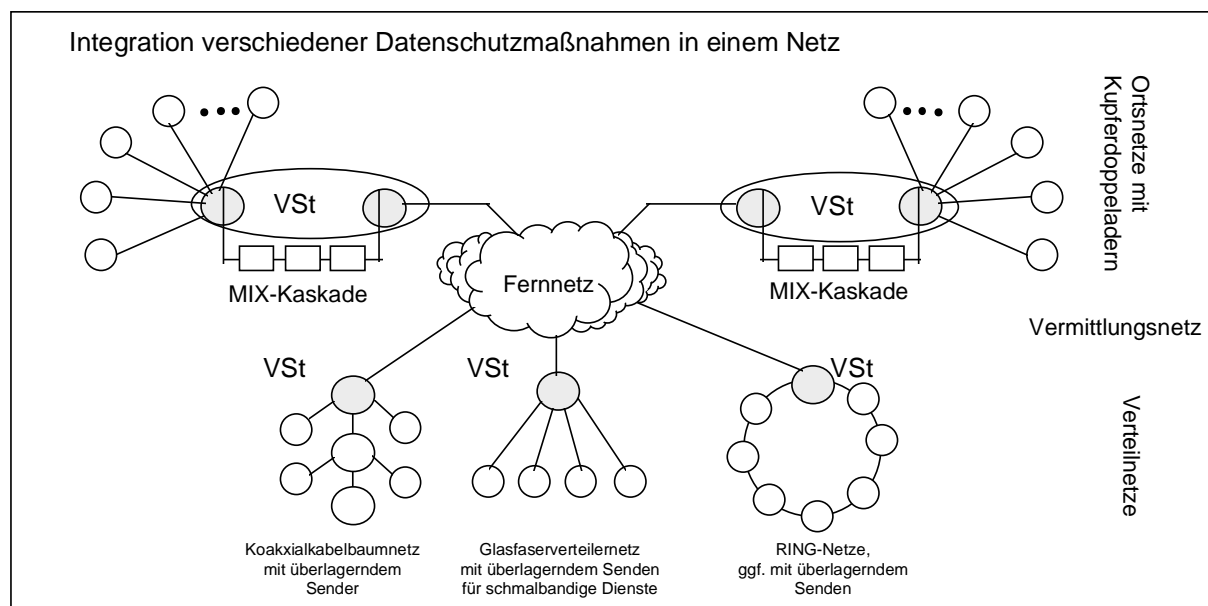
- Telefon-Mixe auf der Basis von ISDN ([PfpW1_89])
- Schutz der Aufenthaltsinformation in Mobilkommunikationsnetzen mit pseudonymer Speicherung von Teilnehmerdaten ([FFJM_97])
- Non-Disclosure Method (NDM) mit unabhängigen „Security Agents“ als Mixe, die vom Benutzer ausgewählt werden können, mit asymmetrischer Umkodierung, z. B. für Mobile IP ([FaKK_97])
- Anonymous- und Pseudonymous-Server im Internet, die auf Anwendungsebene arbeiten ([Cott_95]):
 - Remailer für News-Postings und E-Mail mit Absenderersetzung durch Pseudonyme, die für jeden Nutzer gespeichert werden, ohne eine Möglichkeit der Umkodierung
 - Cypherpunk-Remailer für News-Postings und E-Mail mit Möglichkeit der Umkodierung und Angabe von Latenzzeiten
 - Mixmaster für News-Postings und E-Mail (bestimmtes Format erforderlich) im Poolbetrieb mit Umkodierung und Wiederholungstest auf die Paket-ID
 - Anonymisierungs-Proxy für WWW mit Ersetzung des Absenders durch die Server-Adresse (z. B. <http://www.anonymizer.com>)

Um Echtzeitanforderungen wie z. B. beim Telefonverkehr zu erfüllen, wandelt man das Mix-Verfahren dahingehend ab, daß getaktete Mix-Kanäle mit hybrider Verschlüsselung verwendet werden: Zum Verbindungsaufbau wird eine spezielle Kanalaufbaunachrichtis asymmetrisch verschlüsselt an den Empfänger gesendet, die jedem Mix auf dem Weg einen Schlüssel eines schnellen symmetrischen Kryptosystems übergibt, mit dem die Daten auf diesem Mix-Kanal entschlüsselt werden.

Bewertung

Mixe bieten eine benutzerkontrollierte Pseudonymisierung sowohl für den Sender als auch für den Empfänger. Der Schutz kann sich zusätzlich zu den Verbindungsdaten auch auf die Verbindungsvorbereitungsdaten erstrecken.

Für den Einsatz von Mixen reicht eine Modifikation vorhandener Netze aus; es ist also dafür nicht nötig, vollständig neue Netze zu entwerfen. In vielen Bereichen könnte der Aufbau von Mixen sukzessiv erfolgen. Untersuchungen zeigen, daß die zur Verfügung stehende Bandbreite bestehender Kommunikationsnetze für einen Mix-Betrieb ausreicht ([FJMP_97]). Konzepte für ISDN ([PfpW1_89]), GSM ([FeJP_96]) und bestimmte Internet-Dienste liegen vor, eine Anpassung der Konzepte auf andere Kommunikationsnetze wie ATM und UMTS (Universal Mobile Telekom Systems) ist möglich.



4.1.5 Verhinderung der Peilbarkeit

Elektromagnetische Wellen haben die Eigenschaft, daß aufgrund ihrer Ausbreitung die Sender lokalisiert werden können. Der Aufenthaltsort mobiler Teilnehmer kann somit beim Aussenden von Nachrichten durch Peilung festgestellt und verfolgt werden.

Will man dies verhindern, sind Verfahren einzusetzen, die eine Peilung erschweren. Da eine elektromagnetische Welle nur dann erkennbar ist, wenn sie sich aus dem vorhandenen „weißen Rauschen“ abhebt, kann man sich den Grundsatz der Nachrichtentheorie zunutze machen, daß es zur Erkennung eines digital zu übertragenden Signals nicht auf die Signalform, sondern auf den Energieinhalt ankommt. Wird durch ein geeignetes Modulationsverfahren die Signalleistung so breit verteilt, daß sie sich vom Rauschen nicht mehr abhebt, ist die Abstrahlung von Informationen mit konventionellen Mitteln nicht mehr peilbar. Das Verfahren wird „direkte Spreizung“ genannt [ThFe_96].

Hierbei werden die Daten wie üblich auf den Träger aufmoduliert. Das entstehende Signal wird in einem zweiten Modulationsschritt mit einer Pseudozufallszahlenfolge (PN-Code – **P**seudonoise Code) moduliert. Der PN-Code wird mittels eines PN-Generators aus dem PN-Key von Sender und Empfänger erzeugt. Das entstehende Signal hat eine geringe Leistungsdichte und ähnelt dem „weißen Rauschen“. Der Empfänger multipliziert das empfangene Signal erneut mit dem nachgebildeten PN-Code, wodurch die Spreizung zurückgenommen wird und der Träger in seiner ursprünglichen Form vorliegt. Bei Verwendung von orthogonalen PN-Codes können mehrere Nutzer im selben Spektrum senden. Die Auslastung ist vergleichbar mit den bekannten Multiplexverfahren. Mit konventionellen Mitteln wie Spektrumsanalysatoren sind die direkt gespreizten Signale nicht zu entdecken. Mit einem Radiometer ist dies u. U. möglich. Eine Peilung des Signals ist mit diesem Instrument aber ausgeschlossen.

Bewertung

Sofern zentrale vertrauenswürdige Instanzen eingesetzt werden, kann man lediglich von einer (sonstigen) Pseudonymisierung des Senders und Empfängers nach dem Datensparsamkeitsmodell ausgehen, die sich auch auf die Verbindungsvorbereitungsdaten erstreckt. Es ist jedoch auch möglich, das Verfahren mit benutzerkontrollierten Pseudonymen zu realisieren. Die Ähnlichkeit zum „weißen Rauschen“ trägt dazu bei, daß relevante Informationen nicht mehr erkennbar sind.

Das Verfahren erfordert aufgrund der Spreizung der Nutzsignale eine Bandbreitenerweiterung für die Übertragungskanäle um den Spreizfaktor (100 bis 1000). Damit ist es auf die derzeitige Netzstruktur nicht ohne erheblichen Zusatzaufwand übertragbar, wobei der Aufwand wesentlich davon abhängig ist, an welcher Stelle (in einer ortsfesten Station des Festnetzes oder in der Basisfunkstation) die Entspreizung vorgenommen wird. Bei einer Detektion im Festnetz durch vertrauenswürdige (auch verschiedene dezentrale) Instanzen bedeutet dies, daß die erforderliche Bandbreite auch im Festnetz vorhanden sein muß. Gleichzeitig ist auch das Verfahren der derzeitigen Lokalisation mittels HLR und VLR zu überarbeiten.

4.1.6 Änderung des Aufenthaltsmanagements

Der GSM-Standard erfordert es, in derzeitigen mobilen Netzen Aufenthaltsinformationen zentral in Datenbanken (HLR und VLR) aktuell vorzuhalten. Damit ist die Erstellung von Bewegungsprofilen möglich.

Auslagerung der Aufenthaltsinformationen in vertrauenswürdige Instanzen

Einen Schutz der Aufenthaltsinformationen kann man z. B. dadurch erreichen, daß die Informationen über den Aufenthaltsort in vertrauenswürdige zentrale oder dezentrale Instanzen ausgelagert werden. Dem Netzbetreiber werden von diesen Instanzen für die Teilnehmer zeitgesteuerte Pseudonyme mitgeteilt, mit denen der Aufenthaltsort ermittelt werden kann. Zum Aufbau von Verbindungen ist es bei dieser Struktur zunächst notwendig, bei der vertrauenswürdigen Instanz das aktuelle Pseudonym zu erfragen. In einem zweiten Schritt kann dann hiermit die Netzverbindung hergestellt werden [FJKP_95].

Bewertung

Sender und Empfänger sind mit zeitgesteuerten Pseudonymen ausgestattet, die je nach Ausgestaltung des Verfahrens mehr oder weniger benutzerkontrolliert sein können. Bei diesem Verfahren ist es notwendig, die GSM-Struktur in bezug auf die HLR und VLR zu ändern. Der erforderliche Aufwand des Verfahrens hängt in erster Linie vom Grad der Dezentralisierung ab.

Broadcastverfahren in Anonymitätsgruppen

Eine weitere Möglichkeit, die Aufenthaltsinformation zu verbergen, besteht darin, aus der IMSI mit Hilfe einer allgemein bekannten Hashfunktion eine verkürzte IMSI* zu bilden, die als Gruppenpseudonym dienen kann und im Netz zur Lokalisation verwendet wird. Damit bilden sich Anonymitätsgruppen von Teilnehmern, die hinreichend groß sein müssen und in der GSM-Struktur zu verwalten sind. [FJKPS_95]

Soll ein Verbindungswunsch zu einem mobilen Teilnehmer hergestellt werden, so ist zunächst dem Netz über IMSI* die Gruppe des Empfängers mitzuteilen. Im Broadcastverfahren wird anschließend der gesamten Gruppe die mit dem öffentlichen Schlüssel des Adressaten verschlüsselte IMSI übermittelt. Nur dieser kann dann durch Entschlüsselung mit seinem geheimen Schlüssel feststellen, daß er adressiert wurde, und damit die Nachricht auswerten.

Bewertung

Die Verbindungsdaten werden bei diesem Verfahren nicht geschützt, denn bei Kenntnis der öffentlichen Schlüssel aller in Frage kommenden Teilnehmer kann die gesendete verschlüsselte IMSI leicht abgeglichen werden. Allerdings lassen sich wegen des Broadcastverfahrens innerhalb der Gruppe nicht die Lokalisationsdaten des Empfängers ermitteln.

Dieses Verfahren beruht nicht auf einer Veränderung der GSM-Struktur, erfordert jedoch einen erhöhten Signalisierungsaufwand und eine größere Bandbreite. Nutzt man zur Aufenthaltsermittlung mobiler Teilnehmer hierarchische Netze mit unterschiedlichen Zellradien, kann man die Aufenthaltsinformation dadurch verbergen, daß man die Signalisierung über Netze mit großen Zellradien steuert. Besonders geeignet hierzu wären Satellitennetze (z. B. LEO), die Overlayradien von ca. 2000 km abdecken könnten.

4.2 Datenminimierung bei der Entgeltabrechnung

Im folgenden wird dargestellt, daß es auf der Ebene der Telekommunikationsdienstleistungen technisch möglich ist, den Umfang der zu Abrechnungszwecken gespeicherten Verbindungsdaten erheblich zu reduzieren oder sogar völlig auf deren Speicherung zu verzichten. Ferner kann unter Umständen auch der Umfang der gespeicherten Bestandsdaten reduziert werden.

Da immer mehr Telekommunikationsdienstleistungen mit Hilfe von Chipkarten genutzt und abgerechnet werden und unter dem Oberbegriff **Elektronisches Geld** verschiedene Möglichkeiten für sichere elektronische Zahlungsverfahren entwickelt wurden, mit deren Hilfe auch Telekommunikationsdienstleistungen bezahlt werden können, erfolgt zunächst eine Darstellung wichtiger chipkartengestützter Nutzungs- und Zahlungsformen sowie die Möglichkeiten des elektronischen Geldes, bevor dargelegt wird, wie sich diese Techniken dazu nutzen lassen, den Umfang der gespeicherten Telekommunikations-Verbindungsdaten zu reduzieren oder sogar deren Speicherung gänzlich überflüssig zu machen.

4.2.1 Einsatz von Chipkarten für die Bezahlung von Telekommunikationsdienstleistungen

Die zum Bezahlen von Telekommunikationsdienstleistungen nutzbaren Chipkarten sind entweder mit einem Prepaid- oder mit einem Postpaid-Abrechnungsverfahren verbunden. Bei den **Prepaid-Verfahren** stellt die Chipkarte eine Guthabekarte dar (vergleichbar mit der Telefonkarte), von der bei jeder Nutzung ein entsprechender Betrag abgebucht wird. Im Gegensatz dazu dienen die Chipkarten bei den **Postpaid-Verfahren** in der Regel dazu, den Benutzer gegenüber dem Anbieter der Telekommunikationsdienstleistung sicher zu identifizieren.

Chipkarten in Verbindung mit Prepaid-Zahlung

Bei Chipkarten, die in Verbindung mit einem Prepaid-Abrechnungsverfahren eingesetzt werden, ist zwischen Speicher-Wertkarten, Remote-Access-Karten sowie multifunktionalen Karten zu unterscheiden:

- **Speicher-Wertkarten**

Bei Speicher-Wertkarten wird ein Guthaben in Form von Werteinheiten lokal auf dem in der Karte enthaltenen Chip gespeichert. Bevor mit Hilfe einer solchen Karte eine Telekommunikationsdienstleistung in Anspruch genommen und bezahlt werden kann, muß sich die Karte gegenüber dem Telekommunikationsnetz als gültige Karte ausweisen (authentifizieren). Anschließend kann man die gewünschte Telekommunikationsdienstleistung in Anspruch nehmen. Dabei wird das Guthaben auf der Karte jeweils um die verbrauchten Werteinheiten reduziert. Speicher-Wertkarten können technisch so gestaltet werden, daß das darauf gespeicherte Guthaben beispielsweise mit Hilfe bestimmter Buchungsterminals wiederaufladbar ist. Ein Telekommunikationsunternehmen, das Speicher-Wertkarten zum Bezahlen akzeptiert, kann - technisch gesehen - zusätzlich Schattenkonten führen, in denen es registriert, welcher Guthabenbetrag noch auf den einzelnen ausgegebenen Karten (beispielsweise identifiziert anhand der Kartenummer) verfügbar ist. Derartige Schattenkonten könnten dazu dienen, bestimmte Mißbrauchsarten zu erkennen. Anwendungsbeispiel für eine nicht-wiederaufladbare Speicher-Wertkarte ohne Schattenkontoführung ist die deutsche Telefonkarte.

- **Remote-Access-Karten**

Die vor allem in den USA eingeführten Remote-Access-Karten speichern im Unterschied zu den Speicher-Wertkarten kein Guthaben. Das Guthabekonto (Kartenkonto) des Teilnehmers wird vielmehr zentral vom Telekommunikationsanbieter geführt. Die Chipkarten dienen in erster Linie dazu, den Benutzer gegenüber dem Anbieter der Telekommunikationsdienstleistung sicher zu identifizieren und zu authentifizieren. Dabei tritt die Chipkarte an die Stelle der bei anderen Calling Cards erforderlichen PIN-Eingabe, die leicht abgehört werden kann. Die bei der Telekommunikation zu zahlenden Werteinheiten werden in Echtzeit von einem im voraus auf dem Kartenkonto eingezahlten Guthaben abgebucht. Das Kartenkonto kann durch Einzahlungen wieder "aufgeladen" werden, wobei der Telekommunikationsdienstleister hierfür die Personalien des Karteninhabers nicht kennen muß. Beispiel für eine Remote-Access-Karte ist die T-Card der Telekom zum Telefonieren im Festnetz sowie der Mobilfunkdienst "Telly D1 Xtra" im D1-Mobilfunknetz.

- **Multifunktionale Chipkarten**

Inzwischen gibt es auch im voraus aufgebuchte multifunktionale Kartenzahlungssysteme, etwa die EC-Geldkarte oder die PayCard der Telekom, wobei letztere an Kartentelefonen zum Bezahlen der genutzten Telekommunikationsdienstleistungen eingesetzt werden kann. Derartige multifunktionale Systeme erfordern eine technische und organisatorische Infrastruktur, die die Verrechnung der Werteinheiten (Clearing) zwischen den verschiedenen Organisationen ermöglicht, deren Leistungen mit der Karte bezahlt werden können. Von der konkreten Ausgestaltung dieser Verrechnungsverfahren hängt es ab, ob und wie detailliert die Clearingstellen davon erfahren, wer welche Leistung mit Hilfe einer Karte bezahlt hat.

Chipkarten in Verbindung mit Postpaid-Verfahren

Bei Postpaid-Abrechnungsverfahren, die beispielsweise in Zusammenhang mit Kredit- oder Debitkarten angeboten werden, werden die einzelnen Kommunikationsvorgänge zum Zweck einer späteren Abrechnung personenbezogen zentral gespeichert.

Bewertung des Chipkarteneinsatzes zur Bezahlung von Telekommunikationsdienstleistungen

Aus Sicht des Datenschutzes sind Verfahren, die auf Guthabenbasis arbeiten (Prepaid-Cards) gegenüber den Postpaid-Cards vorzuziehen, da nur die Prepaid-Cards eine anonyme Abrechnung von TK-Dienstleistungen ermöglichen. Dabei ist Systemen mit ausschließlich lokaler Speicherung der Werteinheiten auf der Chipkarte des Teilnehmers der Vorzug vor solchen Verfahren zu geben, bei denen zusätzlich oder ausschließlich eine zentrale Speicherung und Verrechnung der Werteinheiten erfolgt, denn die hierbei geführten Schattenkonten könnten, sofern die Identität des Karteninhabers aufgedeckt würde, zur Bildung persönlicher Kommunikationsprofile genutzt werden. Dieses Risiko ist bei wiederaufladbaren Karten besonders gravierend, da hier die Schattenkonten über einen längeren Zeitraum geführt werden.

Soweit die Chipkarten künftig auch zur Abwicklung intelligenter Authentifizierungsmechanismen genutzt werden, macht dies die bislang zur Authentifizierung der Karte erforderliche Übermittlung der individuellen Kartenummer an das Telekommunikationsdienstunternehmen überflüssig. Hierdurch könnte nicht nur ein abhörsicheres Authentifikationsverfahren realisiert werden, sondern das

Telekommunikationsdienstunternehmen könnte bei diesem Verfahren auch auf die Speicherung der Kartennummern verzichten, die mit entsprechendem Zusatzwissen einzelnen Personen zugeordnet werden könnten.

4.2.2 Elektronisches Geld zur Bezahlung von Telekommunikationsdienstleistungen

In dem Maße, in dem offene elektronische Kommunikationsnetze wie T-Online oder Internet genutzt werden, um Waren oder Dienstleistungen zum Verkauf anzubieten, wächst auch das Interesse an Möglichkeiten des elektronischen Bezahls, das Käufern wie auch Verkäufern eine ausreichende Sicherheit bietet. Dabei können mit dem elektronischen Geld beispielsweise die über Netz bestellten Waren, aber auch Telekommunikationsdienstleistungen bezahlt werden. Mittlerweile wurden verschiedene Varianten elektronischen Geldes entwickelt, die sich unter anderem in folgender Hinsicht unterscheiden:

Bei sog. bargeldähnlichen Verfahren gibt es besonders aufgebaute elektronische Dateien, die wie Bargeld unmittelbar einen Geldwert repräsentieren und durch deren Übertragung bezahlt werden kann. Andere Verfahren, es handelt sich hierbei häufig um besonders gesicherte Formen des Home-Bankings, ermöglichen demgegenüber lediglich die gesicherte Übertragung von Überweisungsaufträgen oder anderen, an die Hausbank gerichteten Aufträgen.

Es gibt, wie bei den Chipkarten, Prepaid-Verfahren, bei denen Werteinheiten in einem ersten Schritt gegenüber der geldausgebenden Stelle (z. B. Bank) bezahlt werden, bevor in einem zweiten Schritt mit dem elektronischen Geld eine Ware oder Dienstleistung bezahlt wird. In anderen Fällen verwendet der Kunde elektronisches Geld, dessen Gegenwert erst dann von ihm an eine Clearingstelle zu entrichten ist, nachdem er das elektronische Geld zum Bezahlen an einen Händler übertragen und dieser es zur Gutschrift des Gegenwerts an die Clearingstelle weitergab.

Bewertung

Aus Sicht des Datenschutzes bieten die bargeldorientierten Prepaid-Verfahren die besten Voraussetzungen für die Realisierung eines sicheren elektronischen Zahlungsverfahrens, das die gleiche Anonymität des Bezahls erlaubt wie das Bezahlen mit Bargeld. Beispiel eines solchen Verfahrens ist E-Cash, das es gestattet, durch den Austausch elektronischer Geldstücke, sog. Cyberbucks, zu bezahlen. Man erhält derartige Cyberbucks auf Anforderung von seiner Bank, die den Gegenwert bar entgegennimmt oder von einem Kundenkonto abbucht. Die Cyberbucks werden anschließend elektronisch auf einen PC des Kunden übertragen und können von ihm wiederum an Händler weitergereicht werden. Die Händler können mit den eingenommenen Cyberbucks ihrerseits Waren oder Dienstleistungen bezahlen.

4.2.3 Möglichkeiten zur Reduzierung oder zur völligen Vermeidung der Speicherung von Verbindungsdaten für Abrechnungszwecke

Sofern bargeldähnliches elektronisches Geld benutzt wird, um Telekommunikationsdienstleistungen abzugelten, eröffnet dies die Möglichkeit, diese Dienstleistung bereits während oder spätestens mit dem Ende der Telekommunikationsverbindung zu bezahlen. Vorstellbar ist, daß der Telekommunikationskunde das Entgelt für jeden neu angebrochenen Zeittakt via elektronischem Geld jeweils in Echtzeit übermittelt. Wird eine neu angebrochene Tarifeinheit nicht umgehend bezahlt, so bricht das Telekommunikationsdienstunternehmen die Verbindung wie beim Münztelefon sofort ab.

Elektronisches Geld kann auch benutzt werden, um auf Speicher-Wertkarten bargeldlos wieder ein Guthaben aufzubuchen, ohne daß man hierfür personenbezogene Angaben preisgeben müßte, beispielsweise die eigene Bankverbindung.

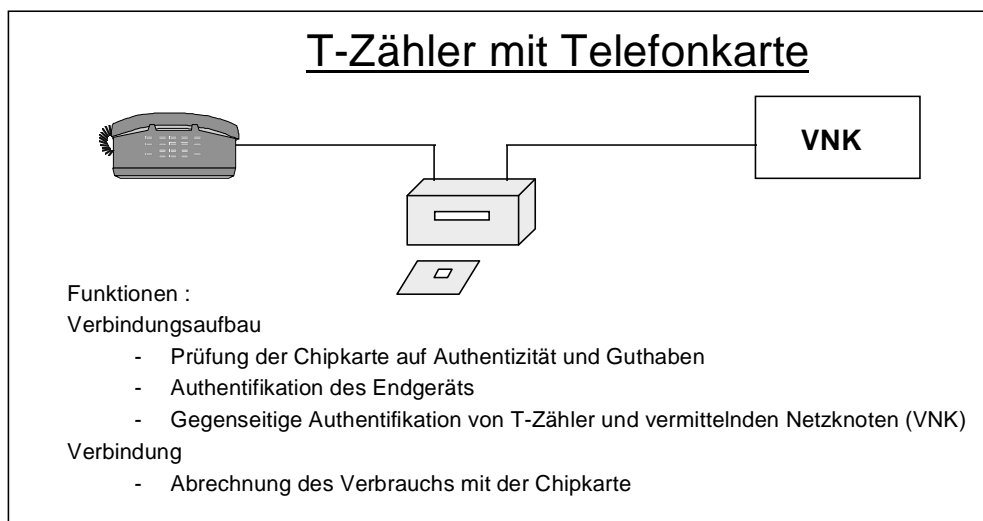
Der Einsatz elektronischen Geldes kann allerdings nur dann zur Datensparsamkeit beitragen, wenn damit anonyme Zahlungsvorgänge möglich sind. Diese Anforderung wird nicht von allen bislang entwickelten Systemen für elektronisches Geld erfüllt.

Bereits aus verschiedenen Anlässen haben die Datenschutzbeauftragten des Bundes und der Länder darauf hingewiesen, daß vielfach auf die Speicherung unter Umständen umfangreicher Datenbestände für Abrechnungszwecke verzichtet werden kann, wenn die Bezahlung mit Hilfe von Speicher-Wertkarten erfolgt

(vgl. z. B. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 22./23.10.1996 zum Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen). Dies gilt auch für das Bezahlen von Telekommunikationsdienstleistungen. Bislang stellt allerdings lediglich die Telefonkarte ein Beispiel für bereits am Markt eingeführte und in größerem Umfang genutzte Speicher-Wertkarten zur Bezahlung von Telekommunikationsdienstleistungen dar. Diese Karten sind nicht wiederaufladbar und können bislang nur an öffentlichen Telefonen genutzt werden. Technisch wäre es aber ebenso möglich, Endgeräte für nicht-öffentliche Anschlüsse anzubieten, die ebenso wie die öffentlichen Telefone in der Lage sind, die anfallenden Telekommunikationsentgelte von einer Chipkarte abzubuchen. Bei der Gestaltung dieser Systeme ist nicht nur darauf zu achten, daß mit ihrer Hilfe zentrale Datenbestände für Abrechnungszwecke vermieden werden können, sondern auch darauf, daß die Abrechnungsmöglichkeiten manipulationssicher sind. Ferner sollten Telekommunikationsverbindungen auf Wunsch des Teilnehmers dokumentiert werden können. Die Verbindungsdaten dürfen hierbei allerdings nur in einem Umfang genutzt werden, daß Persönlichkeitsrechte Dritter, z. B. angerufener Teilnehmer gewahrt bleiben.

Ein solches System könnte wie folgt funktionieren:

Auf der Strecke Endgerät - Anschlußdose - Vermittelnder Netzknoten (VNK) (früher als "Ortsvermittlungsstelle" bezeichnet) wird zwischen dem Endgerät und der Anschlußdose im Bereich des Teilnehmers ein Gerät zur Abrechnung von Telekommunikationsdienstleistungen installiert, im folgenden kurz "T-Zähler" genannt. Denkbar ist auch eine Installation direkt im Endgerät oder erst in der Anschlußdose. Ein solcher T-Zähler enthält einen Mikrocomputer und einen Chipkartenleser. Sobald man von einem über einen T-Zähler angeschlossenen Endgerät, z. B. von einem Telefon oder Telefaxgerät aus eine Verbindung zu einem anderen Teilnehmer aufbauen will, erhält der T-Zähler ein entsprechendes Signal. Er prüft dann zunächst, ob sich eine Speicher-Wertkarte im Lesegerät befindet. Um eine manipulationssichere Abrechnung der in Anspruch genommenen Telekommunikationsdienstleistungen zu ermöglichen, sollten sich T-Zähler und Chipkarte, T-Zähler und Endgerät sowie T-Zähler und VNK jeweils gegenseitig authentifizieren. Anschließend wird, wie bisher, die Verbindung zum gewünschten Telekommunikationsteilnehmer aufgebaut. Zu Beginn der Verbindung sowie mit jedem neuen Zeittakt bucht der T-Zähler das für einen Zeittakt zu zahlende Entgelt vom Guthaben der Speicher-Wertkarte ab. Wann jeweils eine neue Tarifeinheit beginnt, teilt der VNK dem T-Zähler während der laufenden Verbindung mit. Eine solche Übermittlung von Entgeltimpulsen bietet die Telekom ihren Kunden bereits heutzutage auf Wunsch an. Alternativ ist auch eine Ausführung des T-Zählers vorstellbar, bei der dieser anhand einer eingebauten Uhr und den aktuellen Tarifinformationen selbst berechnet, wann ein neuer Zeittakt beginnt. Die hierzu erforderlichen Informationen über neue oder geänderte Tarife sowie die zu verwendenden Taktlängen teilt der VNK hierbei dem T-Zähler jeweils bei Bedarf im Anschluß an die Authentifizierung des T-Zählers gegenüber dem VNK mit. Bei der Übermittlung der Tarifimpulse oder der Tarifinformationen sind technische Maßnahmen (insbesondere Verschlüsselung und elektronische Signatur) vorzusehen, die die Integrität, Authentizität und Zurechenbarkeit der übertragenen Daten sicherstellen. Spätestens nach Abschluß der Verbindung werden beim Telekommunikationsdienstleister alle Verbindungsdaten gelöscht, die dazu dienen, die einzelne Verbindung aufzubauen und aufrecht zu erhalten.



Folgende Voraussetzungen müßten erfüllt sein, soll durch einen Einsatz von Speicher-Wertkarten bei nicht-öffentlichen Telekommunikationsanschlüssen auf die Verbindungsdatenspeicherung für Abrechnungszwecke verzichtet werden:

- Die Telekommunikationsunternehmen müßten neuartige Dienste anbieten, bei denen auf die Speicherung von Verbindungsdaten für die Entgeltberechnung verzichtet wird.
- Es müßten T-Zähler als Einzelgeräte oder Telekommunikationsendgeräte mit Chipkartenleser auf den Markt kommen, die die Funktion des oben beschriebenen T-Zählers übernehmen können. Zur Durchführung der vorgesehenen Authentifikationen müßten die VNK der Telekommunikationsdienstunternehmen technisch entsprechend ergänzt werden.
- Es sollte möglich sein, wiederaufladbare Speicher-Wertkarten zu benutzen. Zum Wiederaufladen einzelner Karten ist eine Infrastruktur mit Aufladestellen erforderlich. Denkbar ist, daß die Karten an Geldautomaten oder öffentlichen Kartentelefonen aufgeladen werden. Ein Beispiel für eine solche wiederaufladbare Speicher-Wertkarte stellt die von der Telekom angebotene "Paycard" dar, mit der man unter anderem auch an öffentlichen Kartentelefonen telefonieren kann. Mit Hilfe einer PIN lassen sich an Kartentelefonen Geldbeträge vom Girokonto auf eine Paycard umbuchen.

Sind alle diese Anforderungen erfüllt, so könnte auch an nicht-öffentlichen Telekommunikationsanschlüssen die bislang übliche Speicherung der Verbindungsdaten zu Abrechnungszwecken entfallen. Sofern der entsprechende Tarif außerdem keinen monatlichen Grundpreis beinhaltet, kann auf die Speicherung von Kundendaten für Abrechnungszwecke ganz verzichtet werden.

Die bislang genannten Möglichkeiten zur Vermeidung der Speicherung von Verbindungsdaten für Abrechnungszwecke wurden am Beispiel der Telekommunikation im Festnetz erläutert. Entsprechende Möglichkeiten bestehen aber auch bei der Mobilkommunikation. In diesem Fall müßte die für jeden Mobilanschluß ausgegebene Mobilfunkkarte zugleich eine wiederaufladbare Speicher-Wertkarte darstellen und das Handy die Funktionen des T-Zählers übernehmen. Daß die Nutzung derartiger Speicher-Wertkarten bei der Mobilkommunikation technisch möglich ist, belegt das Beispiel, daß zum Jahreswechsel 1994/1995 kurzzeitig eine anfänglich mit einem Wert von 100 DM ausgestattete Prepaid-Mobilfunkkarte für das Netz D1 auf den Markt kam, bei der der Diensteanbieter nicht registrierte, an wen er diese Karten ausgegeben hat (vgl. Niederschrift der 725. Sitzung des Bundesrats-Rechtsausschusses vom 18. Juni 1997, S. 53).

4.2.4 Möglichkeiten zur Minimierung von Bestandsdaten

Werden Telekommunikationsdienste angeboten, die keine Speicherung von Verbindungsdaten zu Abrechnungszwecken erfordern, so stellt sich die Frage, ob dies auch zu einer Reduzierung der Kunden-Stammdaten beim Telekommunikationsdienstunternehmen führen kann. Stammdaten dienen zumindest teilweise auch der Abrechnung: Offensichtlich ist dies bei der Bankverbindung. Aber auch die Anschrift dient neben anderen Zwecken - der regelmäßigen postalischen Zustellung der Rechnungen.

Neben der Abrechnung können Stammdaten aber auch folgenden Zwecken dienen:

- **Rufnummernverzeichnisse und Auskunft**
Sofern Kunden in öffentliche Telekommunikationsverzeichnisse (z. B. Telefonbuch) eingetragen werden möchten oder sofern sie damit einverstanden sind, daß ihre Anschlußnummer sowie im Rahmen der Komfortauskunft unter Umständen auch weitere Angaben über eine Auskunft an Dritte weitergegeben werden, erfordert dies die Speicherung entsprechender Stammdaten.
- **Kundeninformation**
Möglicherweise sehen die Telekommunikationsunternehmen außerdem einen Bedarf, eine für einen Anschluß verantwortliche Person individuell schriftlich benachrichtigen zu können, z. B. im Fall einer Tarifänderung oder zur Information über häufig auftretende Störungen.
- **Störungsbeseitigung**
Ein Telekommunikationsunternehmen kann, zumindest bei Festnetzanschlüssen, geltend machen, daß es dauerhaft z. B. Name und Anschrift einer Person benötigt, die ihm im Fall einer Störung Zugang zu den in Privaträumen installierten Netzkomponenten (z. B. Leitungen oder Anschlußdosen) ermöglichen kann.

- **Hoheitliche Aufgaben**
Durch § 90 Abs. 1 TKG werden Telekommunikationsdienstunternehmen, die geschäftsmäßig Telekommunikationsdienste anbieten, verpflichtet, Kundendateien zu führen, in denen Namen und Anschrift der Inhaber von Rufnummern oder Rufnummernkontingenten enthalten sind.

Der Einsatz von Speicher-Wertkarten oder bargeldähnlichem elektronischen Geld zur Vermeidung der Speicherung von Verbindungsdaten für Abrechnungszwecke ermöglicht zunächst nur eine Reduzierung der gespeicherten Stammdaten, insoweit diese ausschließlich für Abrechnungszwecke genutzt wurden, wie dies etwa bei der Bankverbindung der Fall sein dürfte. Soweit Stammdaten neben der Abrechnung auch noch einem oder mehreren anderen Zwecken dienen, ist eine Reduzierung dieser Stammdaten nur in dem Ausmaß möglich, wie sich auch die Stammdatenspeicherung für diese anderen Zwecke reduzieren oder vermeiden läßt. Hierzu ist im einzelnen festzustellen:

Hinsichtlich der für Rufnummernverzeichnisse und Auskunft genutzten Daten haben Kunden heute schon die Wahlmöglichkeit, ob sie ihre Daten für diese Zwecke bereitstellen wollen oder nicht.

Soweit es um Stammdaten geht, die der Kundeninformation dienen, ist vorstellbar, daß ein Kunde auf Speicherung seiner Stammdaten für derartige Zwecke verzichtet. Es müßte dabei jedoch sichergestellt sein, daß dieser Kunde die entsprechenden Informationen auf Wunsch erhalten kann; dies könnte z. B. mit Hilfe eines Telefondienstes erfolgen, der aktuelle Tarifinformationen und sonstige aktuelle Hinweise zum Abruf bereithält. Daten für Zwecke der Störungsbeseitigung dürften allenfalls im Bereich des Festnetzes erforderlich sein.

Hinsichtlich der Vorschrift des § 90 Abs. 1 TKG stellt sich die Frage, ob diese Vorschrift die Telekommunikationsunternehmen auch zur Bereitstellung von Daten über solche Kunden verpflichtet, über die das Unternehmen ansonsten keine personenbezogenen Daten gespeichert hat. Eine solche Auslegung des § 90 Abs. 1 TKG stünde dem Angebot eines anonymen Telekommunikationsdienstes entgegen und widerspräche auch § 89 Abs. 2 Nr. 1 a, wonach Bestandsdaten nur für Telekommunikationszwecke gespeichert werden dürfen.

4.2.5 Datenminimierung bei Entgeltabrechnungen an Nebenstellenanlagen

Die in Nr. 4.2.3 und 4.2.4 dargestellten Möglichkeiten für die Minimierung von Verbindungs- und Bestandsdaten lassen sich aus technischer Sicht auch bei Anschlüssen realisieren, die über eine beispielsweise von einer Firma oder einer Behörde betriebenen Nebenstellenanlage mit dem öffentlichen Telekommunikationsnetz verbunden sind. Auch bei einer eigenen Gebührenverarbeitung kann der Umfang der gespeicherten Verbindungsdaten durch folgende Maßnahmen erheblich reduziert werden:

- Für die Erhebung von Verbindungsdaten in Gebührencomputern ist der Grundsatz anzuwenden, nur die Daten zu speichern, die Basis für eine konkrete Auswertung sind.
- Bereits bei der Übernahme von Verbindungsdaten wird die Erforderlichkeit einer weiteren Speicherung überprüft. Die Daten werden weitestgehend verdichtet und gleichzeitig in der TK-Anlage gelöscht.
- Im Gebührencomputer sind im Regelfall nur noch die Gebühreneinheiten - ggf. fortlaufend addiert - zu speichern und Verbindungsdaten nur soweit wie sie später auch tatsächlich ausgewertet werden.
- Bei der Speicherung von Daten über Dienstgespräche sind insbesondere Prinzipien der zufälligen Stichprobe anzuwenden.
- Den Nutzerinnen und Nutzern von TK-Anlagen ist für die Abrechnung von Privatgesprächen das Wahlrecht einzuräumen auf Einzelnachweise zu verzichten. In diesen Fällen könnte auf die Speicherung der Verbindungsdaten oder zumindest auf deren regelmäßigen Ausdruck verzichtet werden.

4.2.6 Zusammenfassende Bewertung

Das Bezahlen von Telekommunikationsdienstleistungen mit Hilfe bargeldähnlichen elektronischen Geldes kann zur Datenvermeidung beitragen, sofern die Bezahlung jeweils unmittelbar nach Beendigung einer Telekommunikationsverbindung erfolgt. Elektronisches Geld kann auch eine wichtige Rolle spielen, wenn es

um das bargeldlose Wiederaufladen von Speicher-Wertkarten geht, ohne dabei eine Bankverbindung angeben zu müssen.

Die Verwendung von im voraus bezahlten Chipkarten (Speicher-Wertkarten) schafft die technischen Voraussetzungen für Telekommunikationsdienste, bei deren Nutzung keine Verbindungsdaten zu Abrechnungszwecken gespeichert werden müssen.

Darüber hinaus ist auch die Stammdatenspeicherung für Abrechnungszwecke überflüssig z. B. bei Verzicht auf einen Grundpreis oder bei monatlicher Abbuchung über den T-Zähler

Verzichtet der Kunde ferner darauf,

- daß sein Name und seine Rufnummer über eine Auskunft an Dritte weitergegeben werden,
- daß sein Name und seine Rufnummer in öffentlichen Kundenverzeichnissen eingetragen werden und
- daß seine Stammdaten für Zwecke der Kundeninformation verwendet werden,

so besteht im Festnetz unter Umständen lediglich noch ein Bedarf zur Stammdatenspeicherung für die Störungsbeseitigung beim Teilnehmeranschluß. Im Bereich des Mobilfunks ist ein entsprechender Bedarf nicht zu erkennen.

5 Handlungsempfehlung

Telekommunikationsnetze wurden bisher ausschließlich unter Verfügbarkeits-, Performance-, und Sicherheitsaspekten der Betreiber konzipiert. Das Recht der Bürgerinnen und Bürger auf vertrauliche Kommunikation wurde allenfalls in Randbereichen berücksichtigt, meist jedoch als Restriktion diskreditiert. Das Arbeitspapier zeigt auf, daß die Aspekte Datenvermeidung, Pseudonymisierung und Anonymisierung bis heute keine besondere Bedeutung bei der Konzeption und der Ausprägung der TK-Netze besessen haben. Dabei sind die Techniken und Verfahren zur Datenvermeidung und Datenreduzierung bereits längere Zeit bekannt und erforscht. Sie könnten heute in Netz- und Geräteplanungen einbezogen und teilweise kurzfristig mit geringem Aufwand umgesetzt werden.

Die zunehmende Bedeutung der Telekommunikation im täglichen Leben und der gesetzlich normierte Grundsatz der Datenvermeidung zwingen dazu, das Recht der Nutzenden auf unbeobachtbare, gesicherte Telekommunikation stärker in den Mittelpunkt der Entwicklung und Gestaltung von Telekommunikationsnetzen und -diensten zu stellen. Im Endgerätebereich sind die Voraussetzungen für eine breite Einführung von Prepaid Chipkarten sicherlich am leichtesten umzusetzen. Diese Technik ist geeignet, Verbindungs-, Bestands- und Entgeltdaten weitgehend zu vermeiden bzw. zumindest zu reduzieren. Allen Nutzerinnen und Nutzern von TK-Netzen sollte zumindest die Möglichkeit der anonymen Entgeltzahlung wahlweise angeboten werden.

Will man die gesamte Kommunikation zwischen Sender und Empfänger schützen, so wären die derzeitigen Netzstrukturen mehr oder weniger stark zu modifizieren. Im Dialog mit den Herstellern und Betreibern von TK-Netzen sowie den wissenschaftlichen Forschungsgemeinschaften und -instituten sollte die Einbringung datenvermeidender und anonymisierender Technologien in zukünftige Netze weiter erörtert werden. Unter Berücksichtigung des Ziels, die unbeobachtbare, gesicherte Kommunikation zu erreichen, erscheint auch der technische Aufwand und die teilweise noch notwendige Entwicklungsarbeit hierzu gerechtfertigt.

Eine konsequente Umsetzung der Forderungen zur Datenvermeidung und -reduktion scheint im Widerspruch zu bestehenden gesetzlichen Regelungen zu stehen. So werden z. B. nach § 90 Abs. 1 TKG Telekommunikationsdienstunternehmen, die geschäftsmäßig Telekommunikationsdienste anbieten, verpflichtet, Kundendateien zu führen, in denen Namen und Anschrift enthalten sind, um diese den Sicherheitsbehörden, Gerichten, Staatsanwaltschaft und Regulierungsbehörden auf Abruf zur Verfügung zu stellen. Könnte auf Bestandsdaten verzichtet werden, liefe diese Regelung ins Leere. Ebenso wären bei vollständig unbeobachtbarer TK-Nutzung keinerlei Überwachungsmaßnahmen mehr möglich (§ 100 a STPO / § 88 TKG). In diesem Zusammenhang sei daran erinnert, daß in der Mobilkommunikation eine geeignete Überwachungsschnittstelle erst nachträglich gefordert wurde.

Diese Beispiele verdeutlichen, daß es Interessenskonflikte zwischen den Sicherheits- und Überwachungsbedürfnissen des Staates und dem Schutz der persönlichen Daten der einzelnen und damit dem Schutz des Rechts auf informationelle Selbstbestimmung gibt.

Bei Verbesserung der Sicherheits- und Schutzmaßnahmen für die Nutzerinnen und Nutzer von TK-Netzen und Diensten ist zu bedenken, daß Anpassung und Umsetzung im Einklang mit den gesetzlichen Regelungen erfolgen müssen. Erfolge zur Sicherung einer vertraulichen Kommunikation werden deshalb nur durch mehrseitige Betrachtungsweise unter Einbeziehung aller Beteiligten und durch interdisziplinäre Zusammenarbeit möglich sein.

Die Datenschutzbeauftragten des Bundes und der Länder sollten an die Hersteller von Telekommunikationsanlagen und Telekommunikationsanbieter herantreten, um die Realisierbarkeit der aufgezeigten Lösungsansätze zu prüfen. Für das technisch nicht vollständig erfaßbare Umfeld sind Gesellschaft und Gesetzgeber gefordert. Über bestehende Möglichkeiten zur Datenvermeidung und Datenreduzierung sollte die Öffentlichkeit stets aktuell informiert werden.

Literaturverzeichnis

- [Ana_94] Anatol Badach : „ISDN im Einsatz“, Datacom-Verl., Bergheim, Stand 1994
- [BDFK_95] Andreas Bertsch, Herbert Damker, Hannes Federrath, Dogan Kesdogan, Michael Schneider: Erreichbarkeitsmanagement; Praxis der Informationsverarbeitung und Kommunikation (PIK), 18/4 (Oktober 1995), S. 231-234
- [BoGo_92] Egon Bohländer, Walter Gora : „Mobilkommunikation“, Datacom-Verl., Bergheim, Stand 1992
- [Chau_81] David Chaum: „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“, Communications of the ACM 24/2 (1981), 84-88
- [Cott_95] Lance Cottrel: „Mixmaster & Remailer Attacks“, <http://www.obscura.com/~loki/remailer-essay.html>
- [FaKK_97] Andreas Fasbender, Dogan Kesdogan, Olaf Kubitz: „Variable and Scalable Security: Protection of Location Information in Mobile IP“, Arbeitspapier, RWTH Aachen, 1997
- [FeJP_96] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: „Mixes in Mobile Communication Systems: Location Management with Privacy“, R. Anderson: Information Hiding, LNCS 1174, Springer, Berlin 1996, 121-135
- [FJKPS_96] Hannes Federath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: „Mobilkommunikation ohne Bewegungsprofile“, it+it 38/4 (1996)
- [FFJM_97] Hannes Federrath, Elke Franz, Anja Jerichow, Jan Müller, Andreas Pfitzmann: „Ein Vertraulichkeit gewährendes Erreichbarkeitsverfahren (Schutz des Aufenthaltsortes in künftigen Mobilkommunikationssystemen)“, GI-Fachtagung Kommunikation in Verteilten Systemen (KiVS) 97, 17.-22.2.97 in Braunschweig
- [FJMP_97] Hannes Federrath, Anja Jerichow, Jan Müller, Andreas Pfitzmann: „Unbeobachtbarkeit in Kommunikationsnetzen“, eingereicht für VIS '97
- [FrJP_97] Elke Franz, Anja Jerichow, Andreas Pfitzmann: „Systematisierung und Modellierung von Mixen“, eingereicht für VIS '97
- [Lob_94] Hans Lobensommer: „Die Technik der modernen Mobilkommunikation“, Franzis Verl. München, Stand 1994
- [PfPW1_89] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: „Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2·64 + 16)-kbit/s-Teilnehmeranschluß“, DuD 12 (1989), 605-622
- [PfPW_92] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: „Datenschutz garantierende offene Kommunikationsnetze“, GI-Jahrestagung 1992
- [PfPW_91] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: „ISDN-MIXes - Untraceable Communication with Very Small Bandwidth Overhead“, Proc. Kommunikation in Verteilten Systemen (KiVS) 91, IFB 267, Springer, Berlin 1991, 451-463
- [RaPM_96] Kai Rannenber, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit; it+ti 38/4 (1996) 7-10.

- [RDLM 95] Kai Rannenberg, Herbert Damker, Werner Langenheder, Günter Müller: Mehrseitige Sicherheit als integrale Eigenschaft von Kommunikationstechnik; In: Kubicek, Müller, Neumann, Raubold, Roßnagel: "Jahrbuch Telekommunikation & Gesellschaft", 1995, R.v.Decker's Verlag, Heidelberg, 1995, S. 254 - 260
- [Schu_96] Heinz Schulte: Telekommunikation: Dienste und Netze wirtschaftlich planen, einsetzen und organisieren; Interest Verl., Augsburg; Stand: Oktober 1996; Kapitel 9/11.2.3
- [ThFe_95] Jürgen Thees, Hannes Federath: „Methoden zum Schutz von Verkehrsdaten in Funknetzen“, Proc. Vis 95, 181-191

Anlage: Technische Beschreibungen und Beispiel

1 ATM

Funktion des ATM-Verfahrens

Das ATM-Verfahren basiert darauf, daß Datenpakete (Zellen) von konstanter Länge in einem festen Zellenraster - asynchron zum Netztakt - übertragen werden. Jede Zelle hat eine feste Größe von 53 Bytes. Im Zell-Header (5 Bytes lang) stehen die Steuerinformationen für die Wegesuche der Zellen durch das ATM-Netz, die restlichen 48 Bytes enthalten die Nutzdaten. Die zur Verfügung stehende Bandbreite einer Anschlußleitung kann für verschiedene Verbindungen gleichzeitig genutzt werden.

Das ATM-Netz besteht aus ATM-Vermittlungsstellen, Anschluß- und Verbindungsleitungen, angeschlossenen Endeinrichtungen sowie Vorfeldeinrichtungen, die Verkehrsströme von Endeinrichtungen, Privatnetzen oder anderen ATM-Vermittlungsstellen zusammenfassen, verteilen oder umleiten (ATM-Multiplexer, ATM-Konzentratoren und ATM-Cross-Connects).

Das ATM-Forum (<http://www.atmforum.com>) ist eine weltweite Organisation zur Förderung von ATM in der Industrie und im Anwenderbereich. Die ca. 750 Mitglieder setzen sich zusammen aus Herstellern und Betreibern von Kommunikationstechnik, Computerfirmen, staatlichen Organisationen, Forschungsinstitutionen und Anwendern. Schwerpunkte der Arbeit sind die Standardisierung von ATM und die Festlegung von Richtlinien für sowohl öffentliche als auch private ATM-Netze.

Das ATM-Verfahren arbeitet verbindungsorientiert:

- Zunächst erfolgt eine einmalige Wegesuche, denn alle Zellen einer Verbindung nehmen unter Einhaltung ihrer Reihenfolge den gleichen Weg durch das ATM-Netz. Vor der eigentlichen Nutzdatenübertragung findet zu diesem Zweck zwischen den Endeinrichtungen und der ATM-Vermittlungsstelle ein gesonderter Datenaustausch statt.
- Anschließend wird die Verbindung aufgebaut. Dabei werden in den ATM-Vermittlungsstellen Verbindungstabellen angelegt, die die Informationen VCI (Virtual Channel Identifier, identifiziert den virtuellen Kanal) und VPI (Virtual Path Identifier, faßt mehrere virtuelle Kanäle mit gleichem Übertragungsweg zusammen) enthalten.
- Dann werden die Daten in ATM-Zellen übermittelt. In jeder ATM-Vermittlungsstelle wird der virtuelle Kanal (VCI), der für beide Richtungen (abgehend und ankommend) gleich ist, neu vergeben. Die Header der ATM-Zellen werden in Abhängigkeit der Verbindungstabellen erzeugt und dienen der Wegesuche der Zellen durch das ATM-Netz. Die Zellen werden in der Vermittlungsstelle zwischengepuffert, bis sie an die nächste Station geschickt sind.
- Schließlich wird die Verbindung wieder abgebaut, die Verbindungstabellen werden gelöscht.

Die Zellen sind in den ATM-Knoten also kurzzeitig (Größenordnung bei Knoten der Deutschen Telekom: 100 bis höchstens 250 Mikrosekunden) zwischengespeichert. Während der gesamten Verbindung enthalten Verbindungstabellen in den Vermittlungsstellen die Informationen über den Weg. Für Abrechnungszwecke werden hieraus Informationen gewonnen die zur Erstellung der Entgeltdaten dienen.

2 Zellulare Mobilfunknetze

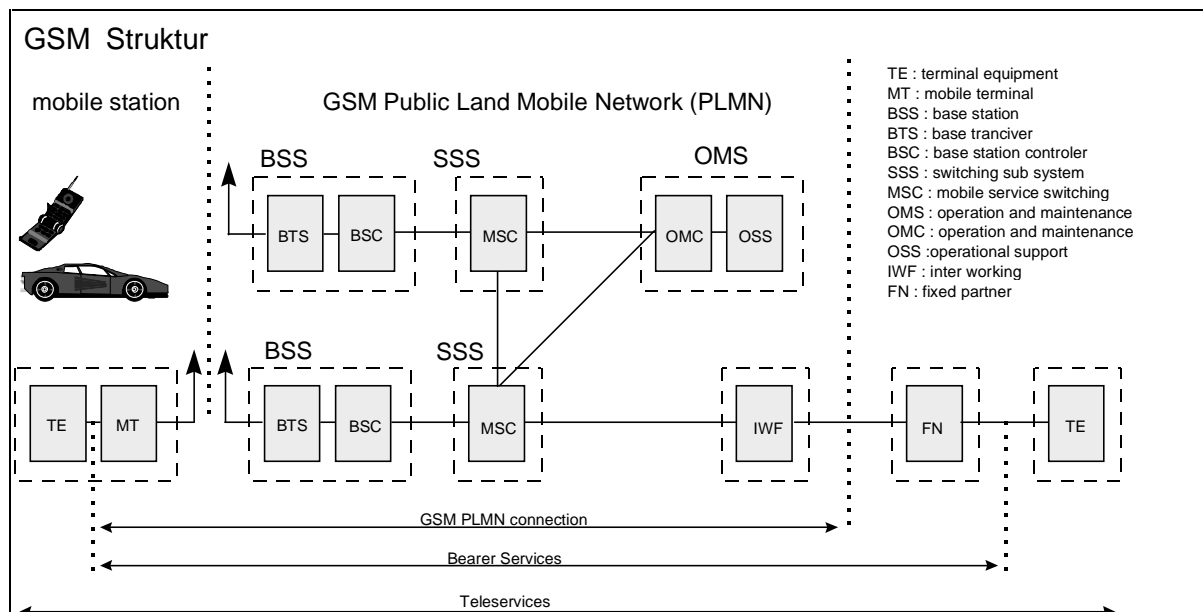
Die GSM-Systemstruktur ist in drei Teilsysteme (Subsysteme) eingeteilt, die wiederum aus mehreren Netzelementen bestehen.

Die Teilsysteme sind:

BSS (Basestation Sub-System) der funktechnische Teil

SSS (Switching Sub-System) der vermittlungstechnische Teil

OMS (Operating and Maintenance System) das Betriebs und Wartungssystem



Die Netze **D1 / D2 Netze** arbeiten im 900-MHz-Frequenzbereich. Beide Netze sind Bestandteil eines europäischen Mobilfunknetzes.

Das **E-plus Netz** richtet sich nach den Vorgaben des DCS1800-Standards (DCS = Digital Cellular System), welcher mittlerweile in GSM1800 umbenannt wurde. Er unterscheidet sich von GSM im wesentlichen dadurch, daß die Funkübertragungen im 1800 MHz Bereich erfolgen und eine geringere Reichweite haben. Die Systemstruktur, die Bitübertragungsraten, die Sprachcodierung und die Verschlüsselungen gleichen dem GSM-Standard.

Struktur der Mobilfunknetze C, D1, D2, E-plus

Die **Mobilstation** wird durch das eigentliche Funktelefon dargestellt. Es ist als Autotelefon, als tragbares Gerät oder als Handgerät (Handy) ausgeführt. Die Verbindung zum ortsfesten GSM-System bildet die Luftschnittstelle in Form einer Funkverbindung zu einer der Basisstationen (BS).

Die **Basisstationen** setzen sich aus dem **funktechnischen Teil, der BTS (= Base Transceiver Station)**, und dem **steuerungstechnischen Teil, dem BSC (= Base Station Controller)** zusammen. Sie ergeben zusammen das **BSS (Basestation Sub-System)**.

In den vermittlungstechnischen Zentralen des GSM-Systems, den **MSCs (= Mobile Switching Center)** werden folgende Funktionen abgewickelt:

- Ermittlung mobiler Teilnehmer
- Verbindung zum öffentlichen Telefon-Festnetz
- Bereitstellung der Supplementary Services (Zusatzdienstleistungen), wie Rufumleitung, Konferenzschaltung usw.
- Vorhalten von Datenbanken die zur Durchführung der Basisdienste erforderlich sind:
 - HLR = Home Location Register
 - VLR = Visitor Location Register
 - EIR = Equipment Identity Register
 - AC = Authentication Center

Die Gesamtheit der Elemente bildet das **SSS (Switching Sub-System)**.

Heimatdatei HLR (Home Location Register)

Datei zum Speichern aller teilnehmerspezifischen Daten, wie:

- Teilnehmeridentität (IMSI = International Mobile Subscriber Identification),
- Zugangsberechtigungen des Teilnehmers (MSISDN = Mobile Station International ISDN Number),
- dem Teilnehmer zugeordnete Dienste,
- Zuordnung des aktuellen Aufenthaltsorts zum Teilnehmer.

Geräte kennzeichnungsdatei EIR (Equipment Identity Register)

Endgerätedatei, in der Listen über Endgeräte gespeichert sind, denen der Netzzugang verwehrt wird, z. B. gestohlen gemeldete Geräte. Diese Listen werden beim Einbuchen eines Gerätes mit der übertragenen Gerätenummer verglichen.

Chipkarte SIM (Subscriber Identity Modul)

Die Karten sind zum Großteil mit einem Prozessor und Speicher ausgestattet. Auf ihnen werden die vom Betreiber des Heimatnetzes eingegebene Teilnehmernummer und die Teilnehmeridentität (IMSI) hinterlegt.

Mit Hilfe der Betriebszentrale dem **OMC (= Operation and Maintenance Center)**

können die Funktionen des Netzes überwacht und Fehler erkannt werden, um Reparatur- und Wartungsmaßnahmen zu veranlassen.

Das **OSS (= Operational Support System)** stellt den administrativen Teil des GSM-Netzes dar und wickelt die Verwaltung der Teilnehmer und der von ihnen beanspruchten Dienstleistungen ab. Es bildet die Datennachverarbeitung.

Beide Komponenten zusammen bilden das **OMS (Operating and Maintenance System)** das Betriebs und Wartungssystem.

Für den vermittlungstechnischen Ablauf werden zwei spezifische Techniken benutzt:

Roaming:

Ständige Verfolgung von mobilen Teilnehmern und automatisches Suchen bei Ruf des mobilen Teilnehmers. Der Anrufer muß nicht wissen, wo sich der gewünschte Teilnehmer aufhält. Die Standortmeldungen erfolgen aktiv durch das Teilnehmerendgerät.

Handover:

Automatisches Weiterreichen einer Funkverbindung von einer Zelle (zu einem Sender/Empfänger gehörendes Gebiet) in die nächste. Der Teilnehmer kann sich während eines Gesprächs durch verschiedene Zellen bewegen.

Struktur des Mobilfunknetzes Modacom

Die wichtigsten Netzelemente sind:

Basisstation BS (Base Station)

In der Basisstation sind alle funktechnischen Einrichtungen untergebracht, die erforderlich sind, um eine Funkverbindung zwischen den mobilen und den Basisstationen herzustellen.

Funkkonzentrator ACC (Area Communication Controller)

Die Funkvermittlungen (ACC) sind im Modacom-Netz, wie auch bei anderen zellularen Systemen, dezentral aufgebaut. Mit diesem Netzelement wird der Datenverkehr in einem Funkvermittlungsbereich gesteuert. Der ACC bildet die Schnittstelle zwischen dem Datex-P Netz und den Basisstationen. An einem ACC können bis zu 64 Basisstationen (Zellen) angeschlossen werden. Der ACC besteht aus zwei Einheiten, dem **Radio Network Controller (RNC)** und dem **Radio Network Gateway (RNG)**. Die ACC's sind untereinander über das Datex-P Netz verbunden.

Die Aufgaben des **RNC** sind die Protokollkonvertierung von X.25 nach RD-LAP und umgekehrt die Weiterleitung abgehender Daten an die entsprechende Basisstation sowie das Roamingmanagement, wenn

Funkteilnehmer in den Bereich eines anderen ACC wechseln. Der RNC ist zur Betriebssicherheit redundant ausgelegt.

Das **RNG** ist die Verbindung zwischen dem Modacom-Netz und dem Datex-P Netz. Im RNG werden die Daten vom RNC zum Datex-P Netz weitervermittelt und umgekehrt. Im RNG wird das Teilnehmermanagement durchgeführt. Wie in anderen zellularen Systemen, so sind auch bei Modacom Heimatdateien (HLR) und Besucherdateien (VLR) vorhanden, in denen alle relevanten Teilnehmerdaten gespeichert sind. Das RNG registriert alle Verkehrsdaten, die für die Betriebsführung, Betriebsstatistik und die Gebührenabrechnung an die Teilnehmer wichtig sind und überträgt sie zum NMC.

Betriebs- und Service Center NMC (Network Management Center)

Das NMC ist die Kommandozentrale für das Modacom System. Es ist mit allen ACC's über das Datex-P Netz verbunden. Im NMC laufen alle Verkehrsdaten zur Nachbearbeitung und Auswertung zusammen. Es ist der zentrale Bedienplatz für Diagnose, Störungsbearbeitung und Betriebskoordination.

Die Verarbeitung der Gebührendaten kann sowohl dezentral bei den ACC erfolgen, als auch zentral im NMC durchgeführt werden.

3 DECT

Grundlegende Systemmerkmale von DECT

Modulation:	Die Modulation erfolgt mittels GMSK (Gaussian Minimum Shift Keying) mit der sich über die Luftschnittstelle eine Datenübertragungsgeschwindigkeit von 1152 kbit/s pro Trägerfrequenz ergibt.																								
Sprachcodierung:	Die Sprache wird mittels ADPCM (Adaptive Differential Pulse Code Modulation) codiert. ADPCM ist ein spezielles Verfahren zur Digitalisierung und Mehrkanalübertragung analoger Quellsignale, insbesondere von Telefonsignalen. Die Verfahrensschritte sind: Abtastung, Quantisierung und Codierung. Bei der Nutzdatenrate von 32 kbit/s pro Kanal ergibt sich eine gute Sprachqualität. Die Geschwindigkeit der parallel dazu übertragenen Signalisierungsdaten beträgt 4800 bit/s.																								
Kanalzugriff:	Es wird das TDMA-Verfahren (Time Division Multiple Access) verwendet, d. h. die einzelnen Verbindungen nutzen einen Kanal jeweils mit erhöhter Datenübertragungsgeschwindigkeit, aber nur für einen Bruchteil der Zeit. Zwischen 1880 und 1900 MHz stehen 10 Trägerfrequenzen mit einem Kanalabstand von 1,728 MHz zur Verfügung, wobei jeder Träger in 24 Zeitschlitze (Slots) eingeteilt wird. Ein Rahmen (Frame) mit 24 Slots wiederholt sich periodisch alle 10 ms. Insgesamt ergibt dies 120 Duplexkanäle.																								
Paketaufbau:	Nutz- und Signalisierungsdaten werden parallel übertragen. In einem Slot wird ein Datenpaket mit 420 Bit übertragen, welches sich folgendermaßen zusammensetzt: <table> <tr> <td>1. Synchronisation:</td> <td>32 Bit</td> <td></td> </tr> <tr> <td>2. Signalisierung:</td> <td>64 Bit</td> <td></td> </tr> <tr> <td> a.) Header</td> <td></td> <td>8 Bit</td> </tr> <tr> <td> b.) Signalisierungsdaten</td> <td></td> <td>40 Bit</td> </tr> <tr> <td> c.) Sicherung</td> <td></td> <td>16 Bit</td> </tr> <tr> <td>3. Nachrichteninhalte:</td> <td>324 Bit</td> <td></td> </tr> <tr> <td> a.) Nutzdaten</td> <td></td> <td>320 Bit</td> </tr> <tr> <td> b.) Interferenzerkennung</td> <td></td> <td>4 Bit</td> </tr> </table> <p>Die Nutzdaten können in Gruppen zu je 80 Bit aufgeteilt werden. Davon werden dann 64 Bit zur Datenübertragung und 16 Bit zur Fehlerkorrektur (Sicherung) verwendet. Der Schutz der Signalisierungsdaten erfolgt mittels CRC (Cyclic Redundancy Check).</p> <p>Die Anzahl der in einem Slot (416,7 µs) übertragenen Bits beträgt 480. Die Differenz von 60 Bit zum Umfang des Datenpaketes dient der Einhaltung einer Schutzzeit von 52,1 µs zum nächsten Datenpaket.</p>	1. Synchronisation:	32 Bit		2. Signalisierung:	64 Bit		a.) Header		8 Bit	b.) Signalisierungsdaten		40 Bit	c.) Sicherung		16 Bit	3. Nachrichteninhalte:	324 Bit		a.) Nutzdaten		320 Bit	b.) Interferenzerkennung		4 Bit
1. Synchronisation:	32 Bit																								
2. Signalisierung:	64 Bit																								
a.) Header		8 Bit																							
b.) Signalisierungsdaten		40 Bit																							
c.) Sicherung		16 Bit																							
3. Nachrichteninhalte:	324 Bit																								
a.) Nutzdaten		320 Bit																							
b.) Interferenzerkennung		4 Bit																							
Reichweite:	Bei der Sendeleistung von 250 mW ergibt sich eine Reichweite von bis zu 50 m in Gebäuden und bis zu 300 m im Freien. Mittels Richtantennen lassen sich bis zu 5																								

km überbrücken. Dies ist für stationäre Systeme, insbesondere WLL (Wireless Local Loop) interessant.

Kanaltypen:

Es gibt vier Kanaltypen:

Typ	Datenrate	Nutzdatenfeld	Fehlererkennung	Fehlerkorrektur	Verzögerung
1	32 kbit/s	ungeschützt	bedingt	nein	fest/minimal
2	32 kbit/s	ungeschützt	bedingt	nein	fest/normal
3	25,6 kbit/s	geschützt	ja	nein	fest
4	< 25,6 kbit/s	geschützt	ja	ja	variabel

Kanalkopplung:

Mehrere Kanäle können parallel - auch über mehrere Basisstationen - belegt und somit Übertragungsgeschwindigkeiten von $n * 32 \text{ kbit/s}$ (bzw. $n * 25,6 \text{ kbit/s}$) erzielt werden.

Asymmetrische Übertragung:

Die Duplexverbindungen können aufgebrochen werden. Somit können für Hin- und Rückrichtung verschiedene Typen und unterschiedliche Geschwindigkeiten gewählt werden.

Zellenstrukturen

Ein-Zellen-System:

Es können mehrere Mobilstationen angemeldet werden. Die Teilnehmer haben die Möglichkeit, kostenlos interne Gespräche zu führen. Gleichzeitig kann über eine nicht belegte Mobilstation auf die Amtsleitung zugegriffen werden.

Mehr-Zellen-Systeme:

Mehrere Basisstationen sind über einen Controller miteinander verbunden. Der Controller ist auch für den Anschluß an andere Netze (z. B. ISDN) zuständig. Man ist im gesamten funktechnisch abgedeckten Bereich erreichbar. Die Mobilstationen halten selbständig Kontakt zu der stärksten Basisstation in ihrer Reichweite.

Schnurlose

Zur Erweiterung des Systems können auch sog. Wireless Base Stations Basisstationen: (WBS), auch Relais oder Repeater genannt, eingesetzt werden. Diese senden die empfangenen Pakete in einem anderen Zeitschlitz (Slot) an die nächste Basisstation weiter. Für jedes über eine WBC geführtes Gespräch müssen somit insgesamt vier Zeitschlitze belegt werden.

Kanalwahlverfahren:

Die Mobilstation hat mittels DCS (Dynamic Channel Selection - Dynamisches Kanalwahlverfahren) die Möglichkeit, aus allen zur Verfügung stehenden 120 Kanälen den nicht belegten mit der geringsten Störung auszuwählen. Dazu werden die Kanäle ständig abgehört und der empfangene Pegel für jeden Kanal gespeichert. Dies geschieht sogar während eines Gesprächs. Die Basisstation paßt sich der von der Mobilstation gewählten Frequenz und dem gewählten Slot an. Daher ist keine Frequenzplanung für die Basisstationen erforderlich.

Bakensignale:

Jede Basisstation sendet immer auf mindestens einem Kanal. Dabei werden stets auch die Systeminformation und die Identifikation der Basisstation ausgestrahlt. Dies ermöglicht jedem Endgerät, allein durch Abhören die in seiner Reichweite befindlichen Basisstationen zu identifizieren. Wenn das Endgerät ein gewünschtes System erkannt hat, hört es alle 160 ms irgendeinen aktiven Kanal der stärksten erreichbaren Basisstation auf einen möglichen Funkruf des Systems ab.

Verbindungsaufbau:

Wünscht die Mobilstation eine Verbindung zum System, baut sie mittels des o. g. Kanalwahlverfahrens DCS einen Kanal auf. Der Verbindungswunsch wird sowohl durch abgehende Anrufe als auch durch die Bereitschaft, einen eingehenden Anruf anzunehmen, ausgelöst. Eingehende Anrufe werden mittels des o. g. Funkrufs von der Basisstation signalisiert.

In Mehr-Zellen-Systemen gibt es zwei prinzipielle Möglichkeiten der Weiterleitung eingehender Anrufe an das jeweilige Endgerät.

1. Ausruf des Anrufs in jeder Zelle

Das jeweilige Endgerät stellt dann die Verbindung zu der Basisstation in der aktuellen Funkzelle her.

2. Ausruf des Anrufs in der Zelle der gewünschten Mobilstation

Dies funktioniert mittels Speicherung der Angabe, in welcher Zelle sich jede Mobilstation befindet, in der Datenbank des Controllers.

Die Hersteller können das eine oder das andere Verfahren wählen.

Handover-Arten:	Intracell-Handover meint den Wechsel auf einen anderen Kanal derselben Basisstation. Dabei wird neben dem Zeitschlitz meist auch die Frequenz gewechselt, um eine bessere Übertragungsqualität zu erreichen. Bei einem Intercell-Handover wird nicht nur der Kanal, sondern auch die Basisstation gewechselt.
Seamless Handover:	Bei einem Wechsel des Kanals wird eine bestehende Verbindung nicht unterbrochen. Um dies zu erreichen, werden von einer Mobilstation kurzzeitig zwei Kanäle belegt. Die Mobilstation gibt den ersten Kanal erst dann frei, wenn die zweite Verbindung steht. Aber der Aufbau der zweiten Verbindung ist auch bei einem Abbruch der ersten möglich, ohne daß die logische Übertragung endet. Im Gegensatz zu den meisten anderen Systemen, z. B. GSM, wird der Handover von der Mobil- und nicht von der Basisstation eingeleitet (MCHO - Mobile Controlled Handover). Die Mobilstation sucht dazu ständig die 11 nicht genutzten Slot-Paare ab, um eine bessere Verbindung zur selben oder einer anderen Basisstation zu finden. Vorteil dieses Verfahrens ist ein sehr schneller und daher vom Benutzer praktisch nicht wahrnehmbarer Kanalwechsel (bei DECT dauert ein Handover 0,1 ms, bei GSM etwa 1 ms).

Interoperabilität

im DECT-System:	Basisstationen unterschiedlicher Firmen können zusammenarbeiten. Die an einer Basisstation angemeldeten Mobilstationen können von einem anderen Hersteller stammen als die Basisstation. Es ist beispielsweise möglich, in einem Zwei-Zellen-System die Basisstation für die eine Zelle von der Firma A, die für die andere von der Firma B zu nehmen sowie mit einer Mobilstation der Firma C über die Basisstation der ersten Zelle ein Gespräch zu führen und sich dabei ohne Unterbrechung mittels seamless handover in den Bereich der zweiten Zelle zu bewegen.
mit anderen Netzen:	Bisher sind im DECT-Standard Anschlüsse an bzw. Integration in folgende Netze vorgesehen: analoges öffentliches Telefonnetz mit Telefax-Gruppe 3, ISDN mit Telefax-Gruppe 4, X.25 und GSM. Zur Realisierung bedarf es einer Schnittstelle, die die Signalisierung umsetzt, die Sprache umkodiert und die Datenpakete umformatiert.
Standards:	Die einschlägigen ETSI-Standards sind CI (Common Interface) mit PAP (Public Access Profile) sowie GAP (Generic Access Profile).
DECT - GSM:	Da sowohl DECT als auch GSM die Mobilität beim Telefonieren unterstützen, jedoch unterschiedliche Zielsetzungen haben, ergänzen sich beide Systeme gut und bietet sich eine Kopplung an. Typische Eigenschaften im Vergleich: <ul style="list-style-type: none"> - DECT deckt kleine Fläche mit hoher Teilnehmerdichte ab, - GSM ist nahezu flächendeckend bei geringer Teilnehmerdichte, - DECT ist bis 20 km/h, GSM bis 250 km/h einsetzbar, - DECT ist im Gegensatz zu GSM schnell und leicht erweiterbar. Mittels Dual-Mode-Geräte können die Vorteile beider Systeme verbunden werden. Solange Funkkontakt zu einer DECT-Basisstation besteht, wird diese Verbindung gewählt, ansonsten bucht das Gerät automatisch in ein GSM-Netz ein.
DECT im WLL:	Wireless Local Loop ist eine Möglichkeit, die relativ teure Verkabelung vor allem der letzten 300 m zwischen dem drahtgebundenen Netz und der Wohnung des Teilnehmers einzusparen, indem man diesen per Funk an das Netz anschließt. Die Kopplung von DECT mit drahtgebundenen Netzen ist hierfür aus folgenden Gründen gut geeignet: <ul style="list-style-type: none"> - hohe Sprachqualität, - hohe Verkehrskapazität mit bis zu 10000 Erlang/qkm, - Unterstützung des Telefaxdienstes, - implementierbare Vorkehrungen für Abhörsicherheit, - einfache und schnelle Installation, - keine Frequenzplanung erforderlich, - problemloser Ausbau durch Hinzufügung weiterer Basisstationen.

Für die Realisierung der Verbindung gibt es zwei Möglichkeiten:

- schlichte Ersetzung der Leitung zwischen OVSt und Teilnehmeranschlußdose, beispielsweise durch Montage einer auf die nächste Basisstation gerichteten Antenne auf dem Dach des Teilnehmers unter Beibehaltung der Anschlußdose,
- Neighbourhood Access: Jeder Teilnehmer hat als Endgerät eine Mobilstation, die auf die nächste Basisstation der OVSt zugreift.

Weitere Systemmerkmale

Sicherheitsaspekte:	<ul style="list-style-type: none"> - Einrichtung von Zulassungsbereichen - Authentikation des Teilnehmers - Authentikation der Mobilstation - Authentikation der Basisstation (optional) - optionale Nutzung von Chiffrier-Algorithmen für Nutz- und Signalisierungsdaten
Identitätsmanagement:	Jedes Endgerät und jedes System kann verschiedene kontext- und ortsabhängige Identitäten haben. Prozeduren der Netzwerkschicht reservieren und aktivieren diese Identitäten falls erforderlich.
Kontextinformationen:	Das Endgerät kann dem System mitteilen, an welchem Ort und in welchem Zustand es sich befindet, unabhängig von dem Bestehen einer Verbindung. Eine Erweiterung des Protokolls ermöglicht es der Mobilstation, einer Basisstation eines anderen DECT-Systems während einer Verbindung Ort und Status zu übermitteln. Dies erlaubt ein Handover zwischen verschiedenen Systemen.

Die DECT-Luftschnittstelle unterstützt mobile Teilnehmer, die sich mit bis zu 20 km/h durch den Versorgungsbereich bewegen.

4 Satellitenkommunikation

Zu den für die Bundesrepublik wichtigsten kommerziellen Betreibern von Satelliten gehören

INTELSAT	(International Telecommunications Satellite Organisation), eine internationale Organisation mit mehr als 100 Mitgliedsländern, die in 172 Ländern Kommunikationsdienste ihrer INTELSAT-Satelliten anbietet,
INMARSAT	(International Maritime Satellite Organisation), eine 1975 gegründete internationale Organisation mit gegenwärtig ca. 70 Mitgliedern (Stand: April 1994), die sich zunächst vornehmlich mit dem Aufbau von Kommunikationsverbindungen zu Schiffen beschäftigte, ihr Geschäftsfeld aber mittlerweile auch auf Kommunikationsverbindungen zu Flugzeugen und mobilen Landfahrzeugen ausgedehnt hat,
EUTELSAT	(European Telecommunications Satellite Organization), die 1977 von 26 europäischen Fernmeldeverwaltungen zur Verbesserung der innereuropäischen Satellitenverbindungen gegründet wurde und heute 38 Mitglieder hat. Neben TV-Übertragung, Telefon- und Datenübertragungsdiensten wird auch das Flottenmanagementsystem EUTELTRACS über EUTELSAT-Satelliten betrieben,
Deutsche Telekom AG	(ehemals Deutsche Bundespost TELEKOM), die im Augenblick drei DFS-Kopernikus-Satelliten unterhält, welche zur Übertragung von TV-Programmen, für Fernmeldeverbindungen (vor der Vereinigung der beiden deutschen Staaten insbesondere solche zwischen der BRD und West-Berlin) und Datenübertragungsdienste genutzt werden.

Im folgenden wird der Schwerpunkt auf die Satellitentelefonie und -datenübertragung gelegt. Die Nutzung von Satelliten für Dienste, wie z. B. Flottenmanagement, Fernerkundung, Positionsbestimmung (GPS) oder Fernortung werden nicht betrachtet, da hier die datenschutzrechtliche Problematik innerhalb des Dienstes selbst zu sehen ist und nicht in der Nutzung der Satelliten zur Kommunikation.

Satellitentechnik

Die in der Satellitentechnologie verwendete Technik hängt vom Einsatzzweck, der Orbitalbahn und der Ausstattung des Satelliten ab. Generell werden zwei Frequenzbänder verwendet, der Uplink zu dem Satelliten und der Downlink von dem Satelliten. Um den Aufwand im Satelliten gering zu halten, wird der Downlink im niedrigeren Frequenzband ausgeführt. Da sich das Signal zweidimensional ausbreitet, kann auf einer Frequenz ein Kanal mit horizontaler Amplitude und ein Kanal mit vertikaler Amplitude betrieben werden. Das Nutzsignal wird meist als Frequenzmodulation aufmoduliert, für Steuerungssignale wird die Phasenmodulation verwandt. Das Trägersignal wird nicht übertragen.

Bei Satelliten in einer geostationären Umlaufbahn findet die Telekommunikation oft über eine Erde - Satellit - Erde Festverbindung statt. Bei Satelliten auf einer niedrigen Umlaufbahn kommen andere Techniken, wie z. B. Tracking Data Relay oder Packet Radio zum Einsatz. Sie können aufgrund ihrer zeitweisen Nähe zur Bodenstation große Datenmengen von schwachen Sendern übertragen, die sie dann zu einem höher im Orbit stehenden Satelliten weitergeben. Dieser besorgt dann den Downlink zur Erde. Bei dem Packet Radio Verfahren werden kleine Datenmengen von dem Sender zum Satelliten übertragen. Dieser speichert sie auf seinem Flug um die Erde, bis der Empfänger in Reichweite kommt. Dort sendet er sie an den Empfänger.

5 TCP/IP als Grundlage zum Internet

Die TCP/IP Protokollfamilie

Die Protokolle der TCP/IP-Protokollfamilie sind in der Lage, die Kommunikation zwischen¹ verschiedenen physikalischen Netzen zu bewältigen. Sie eignen sich damit als Transportmedium für Anwendungen, die über mehrere physikalische Netze hinweg Daten transportieren müssen.

Die TCP/IP-Protokollfamilie im OSI – Referenzmodell (genähert)

	OSI – Modell	Ebenen	Protokolle	
7	Anwendungsschicht	Anwenderebene		
6	Darstellungsschicht			
5	Kommunikationssteuerungsschicht			
4	Transportschicht	Internetebene	TCP	UDP
3	Vermittlungsschicht		IP	ICMP
2	Sicherungsschicht	Netzebene		
1	Bitübertragungsschicht			

Die TCP/IP-Protokolle übernehmen die Aufgaben der Transportschicht und der Vermittlungsschicht. Die Transportschicht übernimmt die Steuerung des Datentransports vom Sender zum Empfänger. So gewährleistet das TCP-Protokoll die Vollständigkeit, die richtige Reihenfolge und die Fehlerfreiheit der empfangenen Daten. Für den Transport über die Vermittlungsschicht werden die zu transportierenden Daten in einzelne Datenpakete (Datagramme) aufgeteilt. Diese sind im IP Protokoll definiert.

¹ Lat. Inter

In der Vermittlungsschicht wird der Weg festgelegt, den die Datenpakete nehmen müssen, um zum Ziel zu gelangen. Die Wegwahl wird von Routern anhand der IP-Zieladresse der Datagramme vorgenommen. Die Router entscheiden durch eine Tabelle, welche Station die Datagramme als nächstes anlaufen müssen, um zum Ziel zu gelangen.

Die Protokollspezifikation der TCP/IP-Protokollfamilie ist offen. Die Protokolle sind unabhängig von der eingesetzten Rechner- oder Netzhardware, dem eingesetzten Betriebssystem und dem im physikalischen Netz eingesetzten Protokoll.

Die Protokolle der Vermittlungsschicht

Das wichtigste Protokoll der Vermittlungsschicht ist das **Internet Protocol IP**. Mit ihm können Daten in Datagrammen transportiert werden. Ein Datagramm besteht aus einem Kopf (Header) mit Kontroll- und Adreßinformationen. Diese Informationen werden benötigt, damit das Datagramm seinen Weg zum Empfänger findet. Im Rumpf des Datagramms befinden sich die Nutzdaten, die von den Protokollen der Transportschicht weiterverarbeitet werden.

Der Aufbau eines IP Datagramms:

Bit	0	4	8	12	16	20	24	28	31
Wort 1	Version	IHL	Serviceart		Gesamtlänge				
2	Identifikation				Flags	Fragment Offset			
3	Time to Live		Protokollnummer		Header - Prüfsumme				
4	Quelladresse								
5	Zieladresse								
6	Optionen						Füllbits		
	Nutzdaten								

- Mit der **Version** wird die Version des IP Protokolls gekennzeichnet. Zur Zeit wird das IP Protokoll Version 4 verwendet. Aufgrund zunehmender Knappheit im Adreßraum wird in den nächsten 10 Jahren ein Umstieg auf die Version 6 vorbereitet.
- Mit der **Internet Header Length** wird die Länge der Kopfdaten festgelegt.
- Die **Service-Art** zeigt die relative Bedeutung dieses Datagramms in den Punkten Verzögerung, Durchsatz und Verlässlichkeit.
- Mit der **Gesamtlänge** wird die Länge des Datagramms festgelegt.²
- Das **Identifikation**-Feld enthält einen Identifizierungswert, der dem Empfänger bei der Zusammensetzung des Datagramms hilft.
- Mit den **Flags** wird gesetzt, ob das Datagramm fragmentiert werden darf und ob dieses Fragment das letzte Fragment ist.

² Ist ein Datagramm länger als die maximal mögliche Paketlänge auf dem Transportweg, so wird das Datagramm in Fragmente zerlegt, die am Ziel wieder zusammengesetzt werden müssen.

- Der **Fragment Offset** gibt die Position des Datagrammfragments in dem ursprünglichen Datagramm an ³.
- Das **Time-to-Live** Feld zeigt die verbleibende Lebenszeit des Datagramms in Sekunden an. Es wird mittlerweile aber als Hop Count eingesetzt, d. h. bei jeder durchlaufenden Station wird sein Wert um mindestens 1 verringert. Mit dem Time-to-Live-Feld wird verhindert, daß ein Datagramm endlos im Kreis läuft.
- Die **Protokollnummer** kennzeichnet das in der darüberliegenden Transportebene verwendete Protokoll. (TCP = 6, UDP = 17)
- Mit der **Header-Prüfsumme** können Übertragungsfehler in der Kopfinformation entdeckt werden. Sie errechnet sich aus dem Rest der $((\sum \text{Headerdaten}) / 2^{16})$.
- Die **Quelladresse** kennzeichnet den Rechner, von dem das Paket stammt.
- Die **Zieladresse** bestimmt den Empfänger des Paketes. Ihre Notation gleicht der der Quelladresse.
- Mit den **Optionen** können weitere Parameter bestimmt werden. So können über ein Security-Feld Sicherheitseinstufungen und spezielle Behandlungsanweisungen festlegen. Mit dem Source Routing kann der Weg zum Ziel definitiv festgelegt werden, d. h., das IP-Paket und nicht der Router entscheidet, welcher Weg zum Ziel eingeschlagen wird⁴. Weitere Optionen bestehen in der Messung des zurückgelegten Weges und der verbrauchten Zeit.
- Mit den **Füllbits** wird die Kopfinformation auf die Länge eines vollen Langwortes gebracht.
- Die **Nutzdaten** sind die zu transportierenden Daten des Protokolls aus der Transportebene.

Eine **Internetadresse** besteht aus 4 Oktetten⁵. Sie wird in Dotted - Dezimalnotation geschrieben. Eine Internetadresse ist z. B. 194.64.160.72. Eine IP-Adresse hat sowohl eine Identifizierungs- als auch eine wegweisende Funktion. Um einen Rechner eindeutig identifizieren zu können muß er eine weltweit eindeutige Adresse besitzen. Als Wegweiser dient die Netzadresse, die in der Rechneradresse enthalten ist. Der gesamte Adreßraum ist in folgende Bereiche aufgeteilt:

	Netzadresse	Rechneradresse	Netzmaske	Anzahl	Bereich
A	1 Oktett	3 Oktette	255.000.000.000	127	001. - 127.
B	2 Oktette	2 Oktette	255.255.000.000	~ 16.000	129. - 191.
C	3 Oktette	1 Oktett	255.255.255.000	~ 2 Mio	192. - 223.
D	4 Oktette	Multicasting		268 Mio.	224. - 239.
E	Reserviert	Reserviert			240. - 255.

Die Netzmaske gibt an, welcher Teil der IP-Adresse zum Netz und welcher Teil zum Rechner gehört. Die Adreßverteilung innerhalb eines Netzes sieht folgendermaßen aus:

194.64.160.0	Netzadresse	
194.64.160.1 - 194.64.160.254	254 mögliche Rechner und Routeradressen	Adressraum für die verschiedenen Rechner in diesem Netz
194.64.160.255	Broadcast Adresse	Für Nachrichten an alle Rechner im Netz

³ Als 64 Bit Offset.

⁴ Diese Option kann zu Sicherheitsrisiken bei der Verwendung interner Adressen führen.

⁵ Ein Oktett sind 8 Bit. Der Wertebereich geht von 000 bis 255.

Die unterste Adresse in einem Netz ist immer die Netzadresse.

Das **Internet Control Message Protocol ICMP** ist ein spezielles Steuerprotokoll, mit dem Fehler gemeldet werden und Wegwahl sowie zeitliches Verhalten in einem Netzwerk untersucht werden können.

Fehlermeldung	Ergebnismeldung
Empfänger nicht erreichbar (Netz, Host, Protokoll, Fragmentierung)	Echo vom Ziel
Quelldatenstrom unterdrücken, Empfänger ist ausgelastet.	Zeitstempel hin und zurück
Andere Wegwahl für (Netz, Host, Netz & Service, Host & Service)	Information Anfrage / Antwort
Zeitlimit überschritten (beim Transport, beim Zusammensetzen der Fragmente)	Adreßmaske Anfrage / Antwort

Die Protokolle der Transportschicht

Das **Transmission Control Protocol TCP** ist ein verbindungsorientiertes Protokoll, für die Ende-zu-Ende Kommunikation. Mit dem TCP Protokoll kann zwischen zwei Rechnern eine Transportverbindung aufgebaut werden.

Der Verbindungsaufbau geschieht durch einen 3-Wege Handshake. Der Sender schickt zuerst seine Initialisierte Sequenz Nummer **SYN**. Der Empfänger bestätigt diese **ACK** und schickt seinerseits seine Synchronisierungsnummer **SYN**. Von nun an beginnt der beiderseitig bestätigte Datenaustausch.

Der Empfänger hat dem Sender beim Leitungsaufbau ein Empfangsfenster mitgegeben. Dieses entspricht der Größe des freien Speichers, die der Empfänger im Moment besitzt. Der Datenfluß wird dadurch gesteuert. Der Sender sendet nur so viele Daten, wie der Empfänger empfangen kann. Dann wartet er neue Empfangsbestätigungen mit neuen Empfangsfenstern ab.

Der Empfänger kontrolliert die empfangenen Datenpakete anhand der Prüfsumme, sendet Bestätigungen oder fordert das Datensegment noch einmal neu an. Sind alle Daten übertragen oder ist der Verbindungsaufbau fehlgeschlagen, so sendet der Sender das **FIN**-Signal. Auch nach einer bestimmten Ruhezeit wird die Verbindung abgebaut.

Der Aufbau des TCP-Protokolls:

Bit	0	4	8	12	16	20	24	28	31
Wort 1	Quellport				Zielpport				
2	Sequenznummer								
3	Acknowlegmentnummer								
4	Data Offset	Reserviert	Kontrollbits		Empfangsfenster				
5	Prüfsumme				Dringlichkeitszeiger				
6	Optionen				Füllbits				
3	Nutzdaten								

- Der **Quellport** gibt den Port des anfragenden Rechners an. Die Portnummer ist ein freier Quellport, so daß mehrere Verbindungen zu dem gleichen Zielrechner unterscheidbar sind.
- Der **Zielport** gibt den nachgefragten Dienst des Zielrechners an. Eine Portnummer < 1024 kennzeichnet im Regelfall einen Standarddienst.
- Die **Sequenznummer** gibt einem Datensegment eine Sequenznummer. Die Sequenznummer beginnt mit der **ISN** Initialisierten Sequenznummer und wird für jedes versandte Segment um eins erhöht.
- Die **Acknowledgementnummer** ist die Sequenznummer des Datensegmentes, deren korrekten Empfang der Sender als nächstes vom Empfänger bestätigt haben möchte.
Diese Funktion ist nur aktiv wenn das **ACK** Kontroll Bit gesetzt ist.
- Der **Data Offset** zeigt an, wo die TCP-Kopfinformationen aufhören und die Nutzdaten beginnen.
- Die **Kontrollbits** beinhalten Steuerungsbits

URG	Dringlichkeit ist signifikant	RST	Reset der Verbindung
ACK	Empfangsbestätigung ist signifikant.	SYN	Synchronisierungsbit. Wird nur im ersten TCP Paket gesendet.
PSH	Push-Funktion	FIN	Das Endebit. Wird nur im letzten TCP-Paket gesendet.

- Das **Empfangsfenster** zeigt die Größe des freien Empfangspuffers, den der Empfänger bei der letzten bestätigten Sequenz aufwies.
- Die **Prüfsumme** ist das Komplement der Summe aller Daten.

Vor dem Versand wird ein Pseudoheader erstellt, der die Quell und die Zieladresse an das IP Protokoll übergibt.

Bit	0	4	8	12	16	20	24	28	31
Wort 1	Quelladresse								
2	Zieladresse								
3	zero	Protokoll			UDP Länge				

- Der **Dringlichkeitszeiger** zeigt auf die Sequenz hinter den wichtigen Daten, wenn das **URG** Flag aktiviert ist.
- Die **Optionen** im TCP Protokoll.

0	Ende der Optionen
1	Keine Operation
2	Maximale Segmentgröße (32 Bit)

- Die **Nutzdaten** beinhalten den kompletten Datensatz des Dienstes.

Das **User Datagram Protocol** UDP ist ein verbindungsloses simples Protokoll ohne Sicherheitsvorkehrungen. Es ist hauptsächlich für den Einsatz in lokalen Netzen geeignet, da es keinen besonderen Verwaltungsaufwand erfordert. Im Internet wird es nur für einen, allerdings unverzichtbaren, Dienst, dem **Domain Name System** **DNS** verwandt.

Der Aufbau eines UDP-Datagramms:

Bit	0	4	8	12	16	20	24	28	31
Wort 1	Quell Port				Ziel Port				
2	Gesamtlänge				Prüfsumme				
3	Nutzdaten								

- Der **Quellport** gibt den Port des anfragenden Rechners an. Die Portnummer ist ein freier Quellport, so daß mehrere Verbindungen zu dem gleichen Zielrechner unterscheidbar sind.
- Der **Zielport** gibt den nachgefragten Dienst des Zielrechners an. Eine Portnummer < 1024 kennzeichnet im Regelfall einen Standarddienst.
- Die **Gesamtlänge** ist die Länge des Datagramms mit Kopf.
- Die **Prüfsumme** ist das Komplement der Summe aller Daten.

Vor dem Versand wird ein Pseudoheader erstellt, der die Quell- und die Zieladresse an das IP Protokoll übergibt.

Bit	0	4	8	12	16	20	24	28	31
Wort 1	Quelladresse								
2	Zieladresse								
3	zero	Protokoll			UDP-Länge				

Die Normierung der Internet Protokolle

Die technischen Grundlagen für das Internet werden in den **RFCs**⁶ beschrieben und nach Erscheinen nummeriert. Die Beschreibung erfolgt in gut verständlichem Englisch ohne besondere Gestaltung. Grundlage eines RFC muß eine funktionierende Implementation eines Programms sein. Diese wird zum allgemeinen Verständnis in ihrem Aufbau und ihrer Funktionsweise dort kurz beschrieben. Die Standardisierung erfolgt durch allgemeine Nutzung. Die RFCs sind kostenfrei im Internet verfügbar.

RFC	Jahr	Inhalt	Seiten
RFC-791	9 / 1981	IP Internet Protocol specification v04	45
RFC-792	9 / 1981	ICMP Internet Control Message Protocol specification	21
RFC-793	9 / 1981	TCP Transmission Control Protocol specification	85
RFC-768	8 / 1980	UDP User Datagram Protocol spezifikation	3

⁶ Request for Comments. (Aufruf zur Abgabe von Kommentaren.)

6 **Schutz von Nachrichteninhalten**

Verschlüsselung / Kryptierung

Mit Hilfe von unterschiedlichen Verschlüsselungssystemen ist es möglich, die Inhalte einer beliebigen Kommunikationsverbindung gegen unbefugte Kenntnisnahme zu schützen. Es werden Schlüsselpaare generiert und zwischen den Kommunikationspartnern ausgetauscht. Bei der Erstellung und Verwaltung dieser Verschlüsselungssysteme unterscheidet man zwischen symmetrischen und asymmetrischen Verfahren.

Die **symmetrischen Verfahren** beruhen darauf, daß beide Partner einen gemeinsamen, geheimen Schlüssel kennen, der sowohl zur Ver- als auch zur Entschlüsselung dient. Damit wird ein Schlüssel nicht einem bestimmten Teilnehmer, sondern einer bestimmten Kommunikationsbeziehung zugeordnet. Um eine Kommunikationsbeziehung gesichert beginnen zu können, müssen sich beide Partner zuvor auf einen gemeinsamen Schlüssel einigen. Bei offenen Netzen muß dies über das Netz selber erfolgen können, da man nicht davon ausgehen kann, daß die Partner vorher bereits in einem direkten Kontakt gestanden haben.

Das bekannteste symmetrische Verschlüsselungsverfahren ist DES (data encryption standard) das von der NBS (der amerikanischen Normungsbehörde für den öffentlichen Bereich) definiert wurde.

Bei den **asymmetrischen Verfahren** wird, statt einen einzigen Schlüssels zum Ver- und Entschlüsseln zu verwenden, diese Funktion auf zwei zusammengehörige Schlüssel „c“ und „d“ verteilt. Der Schlüssel „d“ soll nur zum Entschlüsseln (dechiffrieren) dienen und muß natürlich geheimgehalten werden. Aus diesem Grund bekommt er auch die Bezeichnung „privater Schlüssel“. Der Schlüssel „c“ hingegen soll nur das Verschlüsseln (chiffrieren), nicht aber das Entschlüsseln ermöglichen, darum wird er als „öffentlicher Schlüssel bezeichnet und kann bekanntgegeben werden. Als Bedingung muß jedoch sichergestellt sein, daß man keine Möglichkeit hat einen unbekanntes „privaten Schlüssel“ aus einem zugehörigen „öffentlichen Schlüssel“ abzuleiten.

Durch ein asymmetrischen Verfahren entsteht die Möglichkeit, einen Schlüssel oder genauer ein Schlüsselpaar (c, d) einem Benutzer und nicht nur einer Kommunikationsbeziehung zuzuordnen, der sich zudem diesen Schlüssel selbst generieren kann. Möchte jemand mit diesem Benutzer gesichert kommunizieren, so muß er sich lediglich dessen öffentlichen Chiffrierschlüssel „c“ besorgen. Dies kann entweder durch eine offene Anfrage an den gewünschten Benutzer geschehen oder unter Verwendung zentraler gegen Manipulation gesicherter Register (Trust Center) erfolgen.

Das bekannteste asymmetrische Verfahren wurde von 1978 von Rivest, Shamir und Adleman veröffentlicht und trägt die Bezeichnung RSA-Verfahren.

7 **Anwendung des Datenmodells für Wähl- und Festverbindungen im digitalen Festnetz**

Das Telekommunikations-Datenmodell wird im folgenden auf bestimmte Dienstleistungen im digitalen Festnetz angewandt. Dabei wird unterschieden zwischen Wählverbindungen (z. B. ANIS, ISDN) und fest geschalteten Verbindungen. Es ist jedoch unbeachtlich, ob mittels dieser Anschlußarten telefoniert oder eine andere Form von Daten ausgetauscht wird.

Bestandsdaten

personenbezogen

Zu den gespeicherten Daten gehören in jedem Falle Name, Vorname und Anschrift, ferner Angaben über die vom Vertrag erfaßten Leistungsmerkmale.

Die Bestandsdaten werden personenbezogen gespeichert. Insbesondere das jetzt übliche Rechnungslegungsverfahren wirkt hier als Beschränkung. Soll dieses Verfahren im wesentlichen beibehalten werden, so ist höchstens eine schwache Pseudonymisierung erreichbar. Dafür wäre eine Treuhandstelle für den Rechnungsversand und die Reklamationsbearbeitung notwendig.

Verkehrsdaten

Wählverbindungen: + anonymisiert/personenbezogen

Festverbindungen: personenbezogen

Zu Zwecken des Netzmonitorings werden Daten über die Auslastung von Ressourcen und über die Qualität der Datenübertragung gespeichert. Auf diese Weise kann der Netzbetreiber erkennen, welche Übertragungswege oder -einrichtungen überlastet oder gestört sind.

Bei Festverbindungen kann man diese Aufzeichnungen prinzipiell immer einem Kunden zuordnen, da die entsprechenden Ressourcen (z. B. Übertragungsleitungen) in einem bestimmten Zeitraum exklusiv zugeteilt werden.

Entgeltdaten

personenbezogen

Die Rechnung wird immer auf eine Person ausgestellt. Der Personenbezug entfällt nur dann ausnahmsweise, wenn eine juristische Person als Kunde auftritt und die aufgeführten Beträge keiner bestimmbar Person (z. B. einem Angestellten einer GmbH) zugeordnet werden können.

Verbindungsdaten

Wählverbindungen: personenbezogen

Festverbindungen: vermieden

Die Verbindungsdaten werden bei Wählverbindungen unter der Anschlußnummer erfaßt, die spätestens im Zuge der Rechnungslegung mit den Bestandsdaten zusammengeführt werden.

Bei Festverbindungen werden Verbindungsdaten nicht verarbeitet; sie sind wegen der pauschalen Tarifierung und der festen Ressourcenzuweisung auch nicht notwendig.

Verbindungsvorbereitungsdaten

Wählverbindungen: personenbezogen

Festverbindungen: vermieden

Bei Wählverbindungen fallen bei den meisten Kunden nur Daten über erfolglose Verbindungsversuche an. Sind die entsprechenden Leistungsmerkmale aktiviert, so werden jedoch auch Daten über Rufumleitungen etc. gespeichert. Auch mittels eines Anrufbeantworters werden Verbindungsvorbereitungsdaten verarbeitet. Dies ist von Bedeutung, wenn diese Funktion durch Baugruppen des Netzes realisiert wird.

Bei Festverbindungen entstehen keine Verbindungsvorbereitungsdaten.

Wählverbindungen

	Datenvermeidung	benutzerkontrollierte Pseudonymisierung	Anonymisierung	sonstige Pseudonymisierung	Vertraulichkeitssicherung
statischer Kontext: Bestandsdaten					X
Verkehrsdaten			+		X
Entgeltdaten					X
Verbindungsdaten					X
Verbindungsvorbereitungsdaten					X

Festverbindungen

	Datenvermeidung	benutzerkontrollierte Pseudonymisierung	Anonymisierung	sonstige Pseudonymisierung	Vertraulichkeitssicherung
statischer Kontext: Bestandsdaten					X
Verkehrsdaten					X
Entgeltdaten					X
Verbindungsdaten	X				
Verbindungsvorbereitungsdaten	X				