Authentikation als Grundlage der Skalierung von Sicherheit in der Kommunikationstechnik[1]

Reiner Sailer
sailer@ind.uni-stuttgart.de

Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart
Prof. Dr.-Ing. Dr. h.c. P.J. Kühn

Kurzfassung

Moderne Kommunikationsnetze ermöglichen zunehmend flexible, nutzerkonfigurierbare Dienste. Durch die Anwendung der Kommunikationstechnik zur Verarbeitung sensitiver Daten sind die Anforderungen an die Sicherheit gestiegen, welche oftmals bei der Einführung neuer Systeme und Dienste noch nicht konkretisiert sind und deshalb nur unzureichend Berücksichtigung finden. Die zunehmende Auswertung personenbezogener Daten, die zur Realisierung von Diensten im Kommunikationsnetz verarbeitet werden, macht auch diese Daten schützenswert. Die Qualität eines Dienstes wird deshalb in Zukunft auch an seiner Möglichkeit gemessen werden, individuelle Sicherheitsanforderungen effizient zu realisieren oder mindestens zu unterstützen. Die vorliegende Arbeit stellt ein Konzept vor, welches durch Betrachtung verschiedener Kriterien eine wirtschaftliche und effiziente Sicherung von Kommunikationssystemen ermöglicht. Die Verfahren zur sicheren Identifikation von Kommunikationspartnern (Authentikation) und die Verteilung von geheimen Schlüsseln zur Sicherung der übermittelten Daten werden aufgrund ihrer Bedeutung detailliert behandelt. Eine Integration vorgeschlagener Sicherungsmechanismen auf Protokollebene wird am Beispiel der Dienstanforderung im Schmalband-ISDN skizziert.

1 Einführung

Moderne öffentliche Kommunikationsnetze bieten dem Nutzer eine Fülle von Diensten an, mit deren Hilfe Informationen über beliebige Entfernungen übertragen werden können. Telekommunikationsdienste werden zunehmend flexibel und lassen sich auf Wunsch nutzerspezifisch konfigurieren. Beispiele sind das Einrichten zeit- und ursprungsabhängiger Rufumleitungen beim Telefondienst. Aspekte der Datensicherheit und des Datenschutzes standen jedoch bei der Definition der Qualitätsparameter nicht im Vordergrund und sind im Augenblick nicht genügend berücksichtigt.

Gemeinsam genutzte öffentliche Netze sind sehr effizient bezüglich der Ausnutzung ihrer Ressourcen (Economy of Scale, Bündelungsgewinn). Die gemeinsame Nutzung von Netzressourcen impliziert jedoch, daß die Daten verschiedener Nutzer, die sich gegenseitig nicht vertrauen, gemeinsam verarbeitet werden. Kommt es bei dieser Verarbeitung zu Fehlern, so ist nicht mehr gewährleistet, daß die übermittelten Informationen nur für den erwarteten Empfänger zugänglich sind. Dabei spielt es keine Rolle, ob der Fehler beim Nutzer liegt oder Fehler in der hochkomplexen Netzfunktionalität vorliegen.

Durch die absehbare Entwicklung, immer mehr und flexiblere Dienste innerhalb eines Netzes zu realisieren (z.B. im Intelligenten Netz [1]), wird ohne entsprechende Sicherungsmöglichkeiten den Nutzern auf lange Sicht zunehmend die Kontrolle über die durch das Kommunikationsnetz vermittelten bzw. im Kommunikationsnetz verarbeiteten Daten entzogen.

Durch die zunehmende Menge persönlicher Informationen, mit denen diese flexiblen Dienste nutzerspezifisch konfiguriert werden können, entstehen auch datenschutzrechtliche Probleme,

[1]Besonderer Dank gilt der Gottlieb Daimler- und Karl Benz-Stiftung in Ladenburg und deren Mitarbeitern und Förderern für ihre freundliche Unterstützung und die finanzielle Förderung dieser Arbeit.

die nicht einfach zu lösen sein werden, die Akzeptanz der Dienste aber wesentlich beeinflussen können. Illustriert wird die Entwicklung des Bewußtseins der Kunden auch am Beispiel des vieldiskutierten Video-On-Demand. Da hier für jeden Film getrennt abgerechnet wird, können aus den Abrechnungsdaten Interessendaten der Kunden abgeleitet werden. Deshalb werden dort mit Nachdruck anonyme Zahlungsmöglichkeiten (z.B. Debitkarten) verlangt, die eine Erfassung abgerufener Filme (zu Abrechnungszwecken) umgehen.

Besonders augenscheinlich wird das Sammeln von Kommunikationsdaten und das Extrahieren von Interessendaten von Teilnehmern im Zusammenhang mit neuen Marktstrategien, die im Internet zunehmend Verbreitung finden. Diese Strategien zielen auf die Sammlung möglichst vieler Daten über Teilnehmer ab (Kreditwürdigkeit anhand der Kreditkartenart, Interessen, Wohngebiet, Telefonnummern, Anschriften) und verwenden sie für Marktstudien und Werbeaktionen.

Im Bereich der öffentlichen Kommunikationsnetze sind kommerziell erhältliche CD-ROMs zu nennen, deren Erzeuger finanziellen Gewinn daraus ziehen, daß sie persönliche Daten von Millionen von Teilnehmern der Bundesrepublik elektronisch verarbeitbar mit entsprechenden Anwendungsprogrammen zur Verfügung stellen. Vorstellbar für die Zukunft sind auch das Einbeziehen der Kommunikationshäufigkeit, der Nutzung von Mehrwertdiensten und der Ableitung von Interessen der einzelnen Teilnehmer der Bundesrepublik bzw. deren berufliche Orientierung, um diese gezielt mit - gegebenenfalls von diesen Personen unerwünschtem - Werbematerial zu überhäufen. Eine Verknüpfung mit Informationen aus dem Internet und anderen Informationsquellen kann die Problematik zusätzlich verschärfen. Auch die Integrität der zugänglichen Informationen kann nicht geprüft werden. So kann das Unterschieben falscher Information zur Benachteiligung von Personen führen.

Weiterhin wird die Kommunikationstechnik in immer stärkerem Maße in sensitiven Bereichen (z.B. im Gesundheitswesen) eingesetzt, in denen ein Kontrollverlust über Informationen bei der Nutzung öffentlicher Netze verhindert werden muß.

Dies alles zeigt, daß ehemals bedenkenlos bereitgestellte persönliche Angaben aufgrund ihrer zunehmenden Verfügbarkeit in digitalisierter Form (z.B. durch Nutzung von Kommunikationsdiensten) und der resultierenden einfachen Verarbeitbarkeit zu einem Kontrollverlust für die betroffenen Personen führen können. Elektronisch erfaßte Daten wurden beispielsweise in den USA zur Kontrolle des Einkommens von Sozialleistungsempfängern verwendet [2].

Der zunehmende Kontrollverlust über sensitive Informationen zusammen mit der zunehmenden Abhängigkeit der (Informations-) Gesellschaft von den Telekommunikationsdiensten und der daraus resultierenden Verletzlichkeit durch Fehlfunktion der Netze [3] macht die „Nachrüstung“ der Telekommunikationsnetze mit Mechanismen erforderlich, die die steigenden Sicherheitsanforderungen der Nutzer und auch der Netzbetreiber bzw. Dienstanbieter garantieren können.

1.1 Möglichkeiten der Kompensation des Kontrollverlustes

Sicherheit beschreibt die Erfüllung der an ein System gestellten Sicherheitsanforderungen. Wir unterscheiden zwischen den Anforderungen:

- *Vertraulichkeit* von Informationsträgern (Schutz gegen unautorisierte Kenntnisnahme),
- *Integrität* von Daten (Schutz gegen unautorisierte, unerkannte Veränderung) und
- *Verfügbarkeit* von Daten und Diensten.

Diese Sicherheitsanforderungen werden im allgemeinen mit schützenswerten Objekten verknüpft. Eine solche Verknüpfung wird im folgenden *Schutzziel* genannt.

Eine Möglichkeit, den Zugriff auf schützenswerte Informationen auch in nicht kontrollierbaren Bereichen zu sichern, stellt die Verschlüsselung dar. Eine Verschlüsselung bildet die interpre-

tierbaren Daten mit Hilfe einer umkehrbaren Abbildung auf nicht interpretierbare Daten ab. Diese Abbildung kann nur unter Kenntnis eines „Geheimnisses“ umgekehrt werden.

Zwar ist der Zugriff auf die nichtinterpretierbaren Daten weiterhin nicht kontrollierbar, doch können Angreifer „lediglich“ die Verfügbarkeit der übertragenen Daten stören. Sie können nicht mehr unautorisiert Informationen erlangen (Störung der Vertraulichkeit) oder die zu übermittelnde Information durch Manipulation der Informationsträger unbemerkt verändern (Störung der Integrität).

Wesentliche Bedeutung für die Effizienz von Sicherheitsfunktionen - d.h. die wirtschaftliche Erfüllung aller Sicherheitsanforderungen - hat die *Allokation* dieser Funktionen. Die Allokation bestimmt die Stellen innerhalb eines Kommunikationssystems, an denen Sicherheitsfunktionen realisiert werden. Für die Lokalisierung von Sicherheitsfunktionen bieten sich aus Teilnehmersicht drei Möglichkeiten:

- innerhalb des teilnehmerkontrollierten Bereiches
- innerhalb des Netzes (kontrolliert durch den Netzbetreiber bzw. Dienstanbieter)
- ausgelagert in vertrauenswürdige Organisationen (unabhängig kontrolliert, zertifiziert)

Sicherheitsmechanismen können nur in vertrauenswürdigen, d.h. als sicher angenommenen Umgebungen realisiert werden, da sonst die Implementierung der Mechanismen nicht manipulationssicher wäre. Deshalb ist es wichtig, inwieweit ein solches Vertrauen bezüglich der Garantie verschiedener Schutzziele gegeben ist bzw. gewonnen werden kann.

Ähnlich wie beim Postdienst, der in Zusammenarbeit mit den Kunden Inhalte durch Briefumschläge schützt, ist auch in Kommunikationsnetzen ein sogenannter Grundschutz vorstellbar, der für alle Kommunikationsvorgänge automatisch Anwendung findet. Im Postdienst steigt dadurch der Aufwand potentieller Angreifer, Briefe mit interessantem Inhalt zu identifizieren. Ähnlich kann eine allgemein angewendete, jedoch nur bis zu einem bestimmten Maße vertrauenswürdige Grundsicherheit innerhalb des Netzes erheblich zum Vertrauensgewinn beitragen, indem an kritischen Stellen der Aufwand für Angriffe erhöht wird.

Das Maß an Vertrauen in den Netzbetreiber bzw. Dienstanbieter und die Sicherheitsanforderungen an einen Kommunikationsdienst bestimmen, ob zusätzlich individuelle Sicherheitsmaßnahmen ergriffen werden müssen. Solche Sicherungsmaßnahmen können eine Verschlüsselung in den Endgeräten oder die beglaubigte Aufzeichnung der in Anspruch genommenen abrechnungspflichtigen Leistungen des Netzbetreibers bzw. Dienstanbieters darstellen.

Die ungenügende Beachtung der Aspekte des Datenschutzes und der Datensicherheit bei der Planung und Entwicklung vieler heute im Betrieb befindlicher Kommunikationssysteme schafft harte Randbedingungen für eine sicherheitstechnische Nachrüstung der Kommunikationsinfrastruktur im Teilnehmer- und Netzbereich. Die durch diese Nachrüstung zu erwartenden hohen Kosten erzwingen eine effiziente Realisierung von Schutzzielen. Es ist genau zu überlegen, welche Sicherheitsmechanismen notwendig sind und wo diese effizient lokalisiert werden können.

Der vorliegende Beitrag beschäftigt sich mit Sicherheitsaspekten bei der Inanspruchnahme von Telekommunikations-Dienstleistungen an der Schnittstelle zwischen Teilnehmerbereich und Netzbereich. Es werden Ausprägungen und Integrationsmöglichkeiten von Sicherheitsfunktionen zur Realisierung zukünftig erwarteter Sicherheitsanforderungen an einem konkreten Beispiel besprochen.

1.2 Szenario der zukünftigen Dienstnutzung und Sicherheitsanforderungen

Die Anforderungen an die Unterstützung der Mobilität von Teilnehmern werden zukünftig auch im Festnetzbereich steigen (Universal Personal Telecommunications [4]). Mobile Teilnehmer werden private oder öffentliche Endgeräte an öffentlichen oder gemeinsam genutzten Anschlüssen bargeldlos nutzen. Dazu müssen bei der Dienstanforderung die in Anspruch

genommenen Leistungen sicher dem jeweiligen Nutzer zugeordnet werden können. Außerdem muß der Zugriff auf mehrwertige Dienste auf der Basis von Teilnehmeridentitäten kontrollierbar sein. Nutzer- und nutzungsspezifische Tarife setzen dabei eine eindeutige Identifikation der Dienstnehmer beispielsweise als Grundlage einer flexiblen und korrekten Zuordnung der Gebühren (Accounting) voraus.

Bei der Realisierung von Diensten und entsprechender Infrastruktur zur Unterstützung der Teilnehmermobilität müssen Aspekte des Datenschutzes und der Datensicherheit in ausreichendem Maße mitberücksichtigt werden.

Im weiteren Verlauf der Arbeit werden vor allem Möglichkeiten zur gegenseitigen Identifikation von Dienstnutzer und Dienstanbieter und zum Schutz von übermittelten Anwendungs- bzw. Kommunikationsdaten untersucht. Dabei spielt die Integrationsfähigkeit von Mechanismen an der Schnittstelle von Teilnehmer- und Netzbereich zur Realisierung individueller Sicherheitsanforderungen in bestehenden Kommunikationsnetzen eine wichtige Rolle.

Bild 1 zeigt die zugrundeliegende Konfiguration. Das Sicherheitsmodul (SM) vertritt den Teilnehmer gegenüber dem Endgerät und dem Kommunikationsnetz bei der Realisierung und Anwendung von Sicherheitsfunktionen.

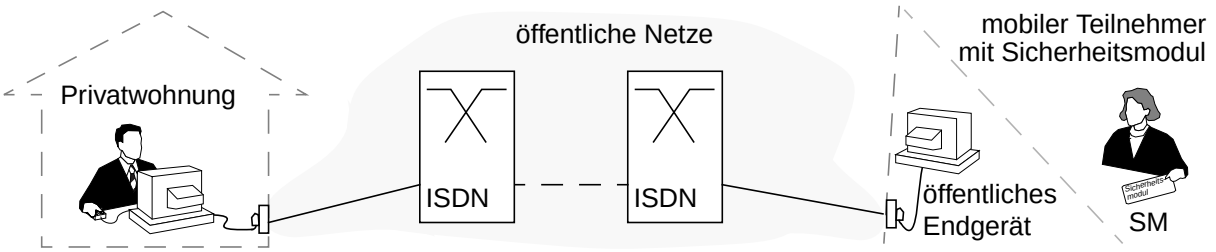

Bild 1: *Aufgliederung des Telekommunikationsnetzes in Bereiche*

Abschnitt 2 führt zunächst in allgemeine Konzepte zur Realisierung verschiedener Sicherheitsanforderungen ein. Abschnitt 3 bespricht Mechanismen zur Authentikation, welche als Grundlage dienen für das in Abschnitt 4 dargestellte Protokoll zur Sicherung der Teilnehmer-Netz-Schnittstelle im ISDN.

2 Bildung von Bereichen zur Integration von Sicherheitsfunktionen

Zur effizienten Sicherung von Kommunikationsnetzen werden diese zunächst in Bereiche aufgegliedert, die separat gesichert werden können. Für eine effiziente Sicherung bietet sich die Aufteilung des Netzes nach folgenden Kriterien an [5]:

- Zuständigkeit und Verantwortlichkeit für Management, Administration und Organisation,
- technische und organisatorische Gegebenheiten und
- geltende Sicherheitsanforderungen bzw. vorgegebene Schutzziele.

Durch die Abbildung der Systemkonfiguration auf hinsichtlich der genannten Kriterien unterscheidbare Bereiche können die einzubringenden Sicherheitsmechanismen an die jeweiligen *Gegebenheiten* und resultierende *Angriffsmöglichkeiten* angepaßt werden.

Sicherheitsmechanismen können wirkungsvoll nur in Bereichen realisiert werden, deren Verantwortlichen Vertrauen entgegengebracht wird, da Sicherheitsmechanismen auch verwaltet, aktuelle Software-Versionen installiert, Zugriffsrechte gesetzt, Schlüssel installiert und aktualisiert und Überwachungsergebnisse (z. B. Protokoll-Dateien, siehe [6]) interpretiert werden müssen.

Die verschiedenen Bereiche müssen gegeneinander abgegrenzt und Bereichsübergänge müssen abgesichert werden. Die Zugriffskontrolle für Dienste und Daten sowie die Anpassung

der Sicherheitsanforderungen zwischen Teilnehmerbereich und Netzbereich stellen Beispiele für Funktionen an Bereichsgrenzen dar.

Die dargestellte Konfiguration aus Bild 1 unterscheidet bezüglich der Verantwortlichkeiten und der Vertrauenswürdigkeit lokalisierter Sicherheitsmechanismen die Bereiche Privatwohnung, öffentliche Netze, öffentliches Endgerät und mobiler Teilnehmer bzw. SM.

Zwei wichtige Mechanismen, die dem Bereichskonzept zugrundeliegen, sind die *Separation* und die *Mediation* [7].

- *Separation* zielt auf die gegenseitige Abgrenzung von Informationsträgern (Nutzdaten und Steuerdaten) ab, die verschiedenen Sicherheitsanforderungen unterliegen. In Bild 1 kann innerhalb des Kommunikationsnetzes zwischen der Teilnehmeranschlußleitung und dem Zwischenamtsbereich unterschieden werden. Unter der Annahme, daß Angriffe an der zugänglichen Teilnehmeranschlußleitung eher erwartet werden, können die Informationsträger in diesem Teilbereich durch kryptographische Verschlüsselung zusätzlich gesichert werden. Durch diese Aufteilung entsteht eine *Skalierbarkeit* der zusätzlich notwendigen Sicherheitsmechanismen abhängig von zugrundeliegenden Schutzzielen und Annahmen über Bedrohungen, welche in den jeweiligen Teilbereichen relevant sind.
- *Mediation* realisiert die Vermittlung zwischen verschiedenen Bereichen und sichert so die innerhalb der aneinandergrenzenden Bereiche vorgegebenen Schutzziele an den Bereichsgrenzen ab. Alle Informationsträger, welche einen Bereich verlassen oder in einen Bereich Eingang finden sollen, müssen durch das Mediationsverfahren geprüft werden. Im obigen Beispiel sorgt die Mediation dafür, daß Daten vor ihrer Übertragung über die Teilnehmeranschlußleitung im Teilnehmerbereich bzw. in der Vermittlungsstelle verschlüsselt werden.

2.1 Separationskonzept

Die Separation kann verschiedene Ausprägungen erfahren. Prinzipiell sind die physikalische, temporäre, logische und kryptographische Separation unterscheidbar.

Durch Separation können sowohl Informationsträger (Nutz- und Steuerdaten) als auch Funktionen (Telekommunikationsdienste, kryptographische Funktionen) geschützt werden. Die verschiedenen Ausprägungen der Separation werden nachfolgend anhand des Szenarios aus Bild 1 an Beispielen veranschaulicht.

Physikalische Separation: Eine physikalische Separation kann zur Sicherung von besonders schützenswerten Daten genutzt werden. Sie wird dadurch realisiert, daß z.B. geheime kryptographische Schlüssel auf separate Sicherheitsmodule verteilt werden und dort ausforschungssicher nur für die zugehörigen Teilnehmer nutzbar sind. Sicherheitsmodule realisieren meist auch die durch diese geheimen Schlüssel parametrisierten Funktionen (z.B. Signaturdienst), da die geheimen Schlüssel den vertrauenswürdigen Bereich nicht verlassen sollen [8].

An der Schnittstelle des Sicherheitsmoduls zum Menschen ist eine Identitätsprüfung bzw. Zugriffskontrolle aufbauend auf biometrischen Verfahren in naher Zukunft denkbar. Der Schutz des Menschen vor der Nutzung gefälschter Module kann durch Echtheitsmerkmale realisiert werden. Eine physikalische Separation der Module selbst durch ihren Besitzer kann zusätzlich vor Diebstahl oder Unterschieben gefälschter Sicherheitsmodule schützen.

Temporäre Separation: Die temporäre Separation kann durch die Personalisierung des Endgerätes mit Hilfe eines Sicherheitsmoduls durch den jeweiligen Nutzer erfolgen. Damit diese Separation vertrauenswürdig ist, können die Endgeräte unabhängig kontrolliert werden und ein gültiges Zertifikat gegenüber dem Teilnehmer (z.B. durch eine Plakette) oder gegenüber dessen SM (in Form elektronisch signierter Nachweise) nachweisen. Sie müssen nach der Nutzung in einen definierten Grundzustand übergehen (z.B. durch Löschen des Wahlwiederholspeichers bei Telefonen), so daß keine Information über vorherige Nutzer durch nachfolgende Nutzer ableitbar ist.

Logische Separation: Zugriffskontrollverfahren für Informationen und Dienste realisieren eine logische Separation. Aufbauend auf der Identität einer Instanz wird der Zugriffsschutz auf Informationsträger oder Dienste mit Hilfe sogenannter Zugriffskontroll-Listen (Access Control List) realisiert [9]. Diese Zugriffskontroll-Listen können in Form von Tabellen realisiert werden, die für Gruppen oder Einzelne die zugelassenen Zugriffsarten auf Ressourcen (z.B. durch Dienst-Profile, Schreib- bzw. Lese-Rechte für Daten) beschreiben. Jeder Zugriff auf logisch separierte Ressourcen muß durch einen Monitor überwacht werden. Dieser Monitor entscheidet auf der Grundlage der Zugriffskontroll-Listen, ob ein Zugriff zugelassen oder abgewiesen wird.

Kryptographische Separation: Die kryptographische Separation realisiert eine Separation der Verständlichkeitsmenge der Informationsträger von autorisierten Zugreifern bezüglich der Verständlichkeitsmenge unautorisierter Zugreifer dadurch, daß sie die Interpretierbarkeit von Daten bzw. die Nutzung von Diensten an die Kenntnis eines nur autorisierten Zugreifern bekannten Geheimnisses knüpft. Die kryptographische Separation der Informationsträger wird hier auf die (physikalische) Separation der geheimen kryptographischen Schlüssel bzw. die (logische oder physikalische) Separation der diese Schlüssel schützenden SM abgebildet.

In Kommunikationsnetzen können folgende Separations-Mechanismen zur Abgrenzung von Daten verschiedener Verbindungen unterschieden werden:

- *Physikalische Separation* durch räumlich begrenzte Ausdehnung des Übertragungsmediums (Funkzelle, Übertragungsleitung) und physikalischen Zugangsschutz der Vermittlungsstellen.
- *Logische Separation* durch Modulationsverfahren (Frequenzmultiplex, Zeitmultiplex, Wellenlängenmultiplex) oder logische Kanalnummern und Adressen auf den Übertragungsstrecken bzw. getrennte Speicherbereiche bei der parallelen Verarbeitung verschiedener Verbindungen innerhalb einer Vermittlungsstelle.
- *Temporäre Separation* durch getrennte Übermittlung der Daten zeitlich nicht überlappend aktiver Verbindungen.

Die temporäre und die logische Separation sind nur innerhalb vertrauenswürdiger Bereiche realisierbar, da ihre Wirksamkeit auf der Implementierung des jeweiligen Zugriffverfahrens beruht. Die physikalische Separation der durch Kommunikationsdienste übertragenen oder verarbeiteten Informationsträger einzelner Verbindungen widerspricht den Zielen der gemeinsamen Nutzung von Netzressourcen (Bündelungsgewinn). Für den Schutz von Informationen in nicht kontrollierbaren Kommunikationsnetzen wird deshalb die kryptographische Separation vorgeschlagen. Durch *kryptographische Separation* kann zusätzlich realisiert werden:

- die Abgrenzung von Daten verschiedener Verbindungen (Anwendungsdaten etc.) während der gemeinsamen Verarbeitung in der Vermittlungsstelle – z.B. zum Schutz gegen Fehlfunktion des Netzes oder falsche Zieladressen – und
- der Schutz von Daten gegen Angreifer an nicht kontrollierbaren Übertragungsstrecken bzw. innerhalb von Netzknoten.

Bei kryptographisch separierten Verbindungen kann ein Fehlrouten die Vertraulichkeit und Integrität der zugehörigen Daten nicht stören, da das „neue“ Ziel die falsch gerouteten Daten nicht interpretieren oder unbemerkt ändern und wiedereinspielen kann. Eine entsprechende kryptographische Separation kann beispielsweise in den Endgeräten oder in Zusatzgeräten im Teilnehmerbereich [10] realisiert werden. In [11] werden anschaulich negative Auswirkungen beschrieben, welche durch das Verwählen bei der Nutzung eines Telefax-Dienstes entstehen können.

2.2 Mediationskonzept

Die Mediation hat die Aufgabe, Sicherheitsanforderungen verschiedener Bereiche an den Übergängen dieser Bereiche zu sichern. Ein Mediator sichert also den Übergang von einem Bereich in einen angrenzenden Bereich. Die Vermittlung zwischen Mediatoren muß deshalb in einer Umgebung realisiert werden, die für alle Bereiche vertrauenswürdig ist, deren Sicherheitsanforderungen an den Bereichsgrenzen umgesetzt werden müssen. Falls diese Bereiche keinen gemeinsamen Vertrauensbereich besitzen, dann muß die vermittelnde Funktionalität in einen neu zu schaffenden gemeinsamen Vertrauensbereich ausgelagert werden.

Ein Vertrauensbereich stellt einen abgeschlossenen Bereich dar, der bezüglich der geltenden Sicherheitsanforderungen als vertrauenswürdig angenommen wird. Es werden in diesem Bereich keine Angreifer oder Angriffsmöglichkeiten angenommen. Durch welche technischen, rechtlichen oder organisatorischen Maßnahmen diese Vertrauenswürdigkeit einer Instanz – bzw. eines durch sie verantworteten Bereiches – gegenüber anderen Instanzen gewonnen werden kann und welche Voraussetzungen dafür gegeben sein müssen, wird in [12] näher betrachtet.

Eine Instanz, die einen solchen ausgelagerten gemeinsamen Vertrauensbereich realisiert, wird im folgenden Vertraute Instanz (VI) genannt.

Das Prinzip der VI als Vermittler zwischen Mediatoren verschiedener Bereiche wird am Beispiel der sicheren Zuordenbarkeit der Inanspruchnahme von Dienstleistungen im Umfeld der Telekommunikation erläutert (Accounting, Rechteprüfung). Es dient als Grundlage für das in Abschnitt 4 vorgestellte Protokoll zur Sicherung dieser Schnittstelle.

Bei den verantwortlichen Instanzen handelt es sich um den Teilnehmer, der einen Dienst anfordert und um den Netzbetreiber der den Dienst abrechnet bzw. um den Dienstanbieter, der die Berechtigung prüft (siehe Bild 2). Der Teilnehmer fordert, daß nur jene Dienste abgerechnet werden, die auch vom ihm in Anspruch genommen werden. Der Dienstanbieter und der Netzbetreiber fordern, daß alle genutzten Dienste abgerechnet und den Teilnehmern korrekt zugeordnet werden. Zur Befriedigung dieser Anforderungen müssen alle genutzten Dienste eindeutig dem richtigen Teilnehmer zugeordnet werden können.

Durch die Mobilität von Teilnehmern kann die Zuordnung von Dienstanforderungen nicht an ortsfeste Netzanschlüsse gebunden werden und somit nicht vom Netzbetreiber zweifelsfrei anhand der Anschlußlage einer Teilnehmeranschlußleitung bestimmt werden. Ein entsprechender Mediator für den Netzbereich (M^N) schützt Netzbetreiber und Dienstanbieter vor unautorisierter Dienstnutzung von außerhalb des Netzbereiches und muß die Zuordenbarkeit der anfallenden Gebühren nachweisbar gestalten.

Durch die absehbare Vielfalt an Dienstanbietern und entsprechend unterschiedlichen Tarifen muß der Teilnehmer die Möglichkeit besitzen, den Dienstanbieter bzw. den in Anspruch genommenen Dienst eindeutig – und eventuell auch nachweisbar – zu identifizieren. Ein Mediator für den Teilnehmerbereich (M^T) muß dazu die Identität des Dienstanbieter bzw. des genutzten Dienstes vor der Dienstnutzung prüfen.

Abschnitt 3 führt in ein international standardisiertes kryptographisches Verfahren ein, welches von den Mediatoren zur Identitätsprüfung genutzt werden kann. Das vorgestellte Verfahren hat den Vorteil, daß eine Instanz ihre Identität nachweisen kann, ohne daß der Prüfer die dabei erhaltenen Informationen nutzen könnte, um diese geprüfte Instanz gegenüber anderen Instanzen zu imitieren. Dies ist in unserem Beispiel notwendig, da der prüfenden Instanz nicht uneingeschränkt vertraut werden soll. Die prüfende Instanz muß über den Inhaber der zu prüfenden Identität keinerlei weitere Kenntnis besitzen. Damit ist das Verfahren auch für die Nutzung von Fremdnetzen über Zugangsnetze anwendbar. Dieses spielt gerade bei mobilen Teilnehmern und bei der Diversität von Netzbetreibern eine wichtige Rolle.

Die Mediatoren M^T und M^N (siehe Bild 2) fordern bei Bedarf die zur Prüfung einer Identität notwendige Prüfinformation bei einer VI an. Die entsprechende Funktionalität zur Verwaltung dieser Prüfinformation kann deshalb durch eine von Teilnehmer und Netzbetreiber bzw. Dienstanbieter unabhängige, vertrauenswürdige Instanz realisiert werden. Diese VI muß bei jeder Dienstanforderung den Mediatoren zugänglich sein. Eine effiziente Realisierungsmöglichkeit bietet deshalb ihre Einbeziehung in die Signalisierung zur Dienstanforderung. Diese Möglichkeit wird in Abschnitt 4 näher untersucht.

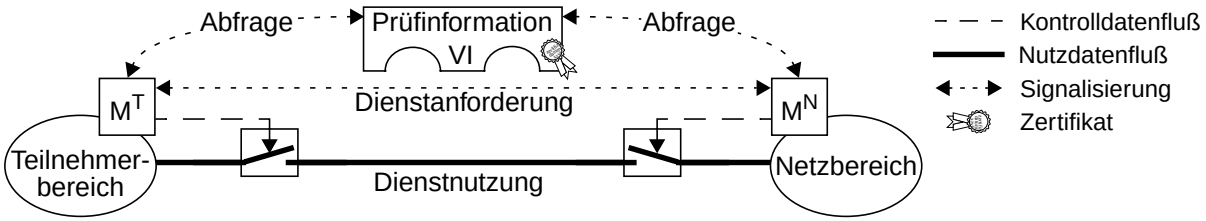

Bild 2: *Vertraute Instanzen als Vermittler zwischen Bereichen*

Weitere Aufgaben einer VI können auch im Schutz von Daten liegen, die gegenwärtig im Kommunikationsnetz verarbeitet werden und deren Verbleib für den Teilnehmer dadurch nicht kontrollierbar ist. Damit verschiedene Kommunikationsereignisse nicht aufgrund der Identität eines Teilnehmers miteinander in Beziehung gesetzt werden können – woraus zusätzliche Informationen über Teilnehmer ableitbar wären –, ist es denkbar, daß für jede Dienstnutzung temporäre Identitäten (Pseudonyme) vergeben werden. Die Auflösung der Pseudonyme muß durch die VI zur Weitergabe der Gebühren an den Teilnehmer und zur Bestimmung von Berechtigungen möglich sein. Das Netz würde bei entsprechender Realisierung die Gebühren der VI zuordnen, welche diese Gebühren nach Auflösung der Pseudonyme an die entsprechenden Verursacher weitergibt. Die Bekanntgabe der Berechtigungen der jeweiligen Teilnehmer durch die VI genügt im Netz für die Prüfung der Dienstanforderung. Auf diese erweiterten Möglichkeiten zur Vermeidung persönlicher Daten im Netz durch die Einbeziehung von Vertrauten Instanzen wird im weiteren nicht näher eingegangen.

3 Authentikation im Anwendungsfeld Telekommunikation

Authentikation beschreibt den Vorgang der „sicheren“ Identifikation von Objekten oder Instanzen. In der Kommunikationstechnik dient die Authentikation vor allem im Vorfeld einer Zugriffskontrolle (Access Control) zur Klärung der Identität der zugriffsfordernden Instanz.

Die Bindung einer Identität an eine Instanz kann prinzipiell durch ein eindeutiges biometrisches Merkmal (z.B. einen bestimmten Fingerabdruck), durch Besitz eines Sicherheitsmoduls, durch Wissen um ein Geheimnis oder eine Kombination von Wissen und Besitz realisiert werden. Innerhalb von Kommunikationssystemen bietet sich der Identitätsnachweis durch Besitz oder Wissen an. An der Schnittstelle des Menschen zur Technik sind biometrische Verfahren eher geeignet. Bild 3 zeigt, wie die Authentikation zweier Teilnehmer A und B als Dienst nach dem Vorbild des OSI-Referenzmodelles dargestellt und realisiert werden kann.

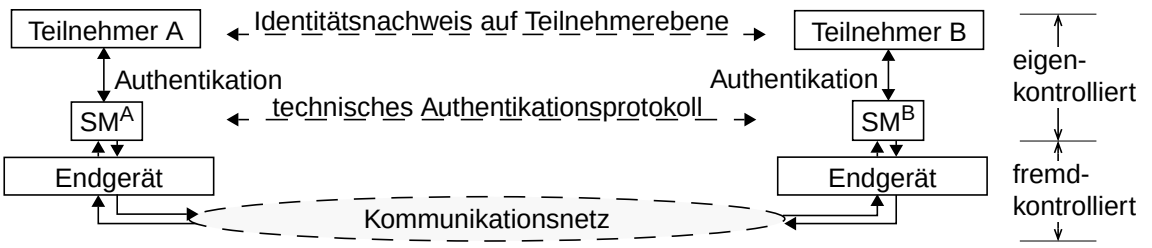

Bild 3: *Kommunikationsmodell der Authentikation zwischen zwei Teilnehmern*

Zunächst authentisiert sich der Teilnehmer gegenüber seinem Sicherheitsmodul. Dadurch wird das Sicherheitsmodul bei Verlust gegen unbefugte Nutzung gesichert. Für diese Authentikation sind biometrische Verfahren besonders geeignet [13], da bei Paßwörtern etc. menschliche Gedächtnisschwächen und die Anwendung der Verfahren in öffentlichen Gebäuden zu Sicherheitslücken – z.B. durch „Schultergucker“ – führen können.

Bei zugriffskontrollierten Endgeräten muß vor der Nutzung des Endgerätes zur Bestimmung der Identität des Teilnehmers eine Authentikation des diesen Teilnehmer vertretenden Sicherheitsmoduls gegenüber dem Endgerät stattfinden. In diesem Bereich existieren verschiedene Authentikationsprotokolle, von denen einige in [14] dargestellt sind. Umgekehrt muß das Endgerät einen Beweis seiner Vertrauenswürdigkeit gegenüber dem Sicherheitsmodul liefern, um den Teilnehmer vor „gefälschten Endgeräten“ zu schützen. Dieses kann durch Zertifikate (begrenzter Gültigkeitsdauer) von unabhängigen Kontrollinstanzen unterstützt werden.

Die Authentikation auf Teilnehmerebene kann nun durch die technischen Vertreter der Teilnehmer (hier: SM^A, SM^B) auf eine Authentikation auf technischer Ebene abgebildet werden.

Da nicht alle während der späteren Kommunikation schützenswerten Daten zur Sicherung durch das Sicherheitsmodul geleitet werden können, wird einem zertifizierten Endgerät aus Aufwandsgründen meist vertraut werden müssen. Ein während des Authentikationsvorganges zwischen den Sicherheitsmodulen ausgehandelter Kommunikationsschlüssel wird an das Endgerät weitergegeben, welches die Sicherung der übertragenen Daten und damit deren Authentisierung übernimmt. Da zwischen der Informationsquelle (Teilnehmer) und der Sicherheitsfunktion (Verschlüsselungsmodul im Endgerät) ein unkontrollierter Bereich liegt, sind die übertragenen Daten höchstens so sicher wie dieser Bereich.

Als Beispiel für den Protokollablauf einer Authentikation wird im folgenden ein Basisverfahren vorgestellt, welches den Identitätsnachweis auf der Grundlage des Wissens eines geheimen Schlüssels realisiert. Anschließend wird die Sicherheit des vorgestellten Authentikationsverfahrens in Bezug auf seine Robustheit gegen vorstellbare Angriffsversuche untersucht.

3.1 Basis-Protokoll für eine kryptographische Authentikation

Das vorgestellte Protokoll basiert auf der X.509-Empfehlung der ITU-T [15],[16] und damit auf einem asymmetrischen Signatursystem [17], bei dem jeder Identität ein geheimer (privater Schlüssel) zur Unterschrift und ein öffentlich bekannter Schlüssel zur Prüfung der Echtheit dieser Unterschrift durch jedermann zugeordnet ist.

Die die Authentikation initiierende Instanz A schickt eine signierte Nachricht N1 zur Partnerinstanz B (Bild 4). Instanz B beweist ihre Identität durch das Signieren der in N1 enthaltenen Zufallszahl r^A in N2 mit ihrem geheimen Schlüssel. Zusätzlich fordert sie von A, die in N2 enthaltene Zufallszahl r^B zu signieren. Instanz A beweist ihre Identität gegenüber B dadurch, daß sie diese Zufallszahl in N3 mit dem nur ihr bekannten geheimen Signaturschlüssel signiert und an B übermittelt.

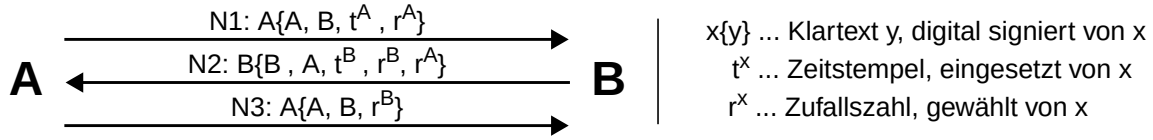

Bild 4: *Technisches Authentikationsprotokoll basierend auf ITU-T X.509*

Das Enthaltensein der Zufallszahlen in den signierten Nachrichten verhindert, daß ein Angreifer einen Authentikationsvorgang zwischen A und B abhört und die dabei gewonnenen signierten Nachrichten dazu nutzt, sich fälschlicherweise für A oder B auszugeben. Die Zeitstempel t^x beschränken die Gültigkeitsdauer von Nachrichten und ermöglichen so, daß sich die

verwendeten Zufallszahlen verschiedener signierter Nachrichten – im Bezug auf die Sicherheit des Verfahrens gegen das Wiedereinspielen abgehörter Nachrichten – nur innerhalb des Gültigkeitszeitraumes unterscheiden müssen. Dieses Verfahren vereinfacht die Wahl einer „neuen“ Zufallszahl aus Sicht des Senders, da innerhalb verschiedener Gültigkeitszeiträume gleiche Zufallszahlen nicht zu wiederverwendbaren Nachrichten führen.

Zur Realisierung des Verfahrens wird ein (asymmetrisches) Signatursystem benötigt. Die an der Authentikation teilnehmenden Instanzen müssen zur Prüfung der Signaturen über den öffentlichen Schlüssel der zu authentisierenden Partnerinstanz verfügen.

Dieser öffentliche Schlüssel muß authentisch sein, d.h. tatsächlich zu der Identität gehören, deren Signatur mit dem öffentlichen Schlüssel geprüft wird. Die Verwaltung dieser öffentlichen Schlüssel kann von sogenannten Verzeichnisdiensten übernommen werden. Diese liefern auf Anfrage den zu einer Identität gehörigen gültigen öffentlichen Schlüssel. Diese Verzeichnisdienste können auch die Sperrung von Schlüsseln realisieren, deren zugehörige geheime Schlüssel bekannt geworden sind (kompromittierte Schlüssel). Die Vertrauenswürdigkeit der Authentikation hängt direkt von der Authentizität der öffentlichen Schlüssel ab und damit von der Vertrauenswürdigkeit des Verzeichnisdienstes, der i.a. über das Kommunikationsnetz angesprochen wird. Interessante Ansätze und Gestaltungsalternativen für vertrauenswürdige Verzeichnisdienste werden in [18] besprochen. Die VI in Bild 2 kann beispielsweise einen solchen Verzeichnisdienst realisieren.

Prinzipiell könnte der Identitätsnachweis auch mit Hilfe symmetrischer Verschlüsselungsverfahren realisiert werden. Die mit symmetrischen Verschlüsselungssystemen erzeugten Signaturen werden auch Message Authentication Codes (MAC) genannt. Zur Bildung des MAC können geheime Schlüssel – welche ausschließlich den zu authentisierenden Instanzen bekannt sind – in die Berechnung eines Hash-Wertes über die zu signierende Nachricht einbezogen werden [19]. Dieses Verfahren erscheint in offenen Systemen insbesondere bei der spontanen Kommunikation mit vorher nicht bekannten Kommunikationspartnern unpraktikabel beziehungsweise setzt zur Installation gemeinsamer geheimer Schlüssel seinerseits ein asymmetrisches Verschlüsselungssystem voraus. Die Urheberschaft von Nachrichten kann mit symmetrischen Verfahren nicht nachgewiesen werden. Außerdem darf der geheime Schlüssel nicht außerhalb des Vertrauensbereiches der zu authentisierenden Instanzen vorliegen. Deshalb können sich Instanzen, die sich nicht gegenseitig vertrauen, mit diesen Verfahren nur über den Umweg einer Authentikation gegenüber einer gemeinsamen VI indirekt authentisieren.

3.2 „Angriffsmodell“ für die Authentikation

Gelingt einem Angreifer ein erfolgreicher Angriff auf das Authentikationsverfahren, so kann er sich fälschlicherweise als Inhaber einer Identität ausgeben und erbt die zu dieser Identität gehörigen Rechte.

Die Sicherheit des vorgestellten Authentikationsverfahrens ist abhängig von der Korrektheit der Implementierung des verwendeten Verfahrens [20] und der Sicherungsmechanismen des zugrundeliegenden Protokolles. Das Signatursystem muß u.a. robust sein gegen die allgemein bekannten Angriffsversuche zur Erlangung des geheimen Schlüssels [21], der dem Verschlüsselungssystem zugrundeliegt. Durch die Wahl geeigneter Schlüssel und eine sorgfältige Implementierung in sicherer Umgebung können viele dieser Angriffe so erschwert werden, daß sie i.a. als nicht mehr relevant einzustufen sind. Gegenwärtig empfehlenswerte minimale Schlüssellängen werden in [22] und [23] diskutiert.

Das Protokoll zur Authentikation muß u.a. resistent sein gegen das Wiedereinspielen abgehörter signierter Nachrichten aus parallel ablaufenden oder zeitlich zurückliegenden Authentikationsvorgängen. Außerdem müssen die zum Zwecke der Authentikation zwischen den Partnern ausgetauschten Nachrichten (N1 bis N3 in Bild 4) während der Übertragung vor Veränderung geschützt werden. Die Authentizität des zur Prüfung der signierten Nachrichten benutzten

öffentlichen Schlüssels muß gewährleistet sein, um eine sogenannte Maskerade (Vorspiegeln einer falschen Identität) durch Einführen falscher Schlüssel zur Signaturprüfung zu verhindern.

Bei geeigneter Implementierung des Signatursystems – Implementierung der Funktionen, Schlüsselwahl und -aufbewahrung – verbleiben folgende relevante Angriffsmöglichkeiten, welche durch Mechanismen des Authentikationsprotokolles kompensiert werden müssen:

(a) Impersonation durch Angabe einer falschen Identität,
(b) Einführen falscher öffentlicher Schlüssel,
(c) Stehlen geheimer Schlüssel,
(d) Ändern des Chiffrats,
(e) Ändern des Klartextes und
(f) Wiedereinspielen abgehörter Nachrichten.

Den Angriffen (a), (d), (e) und (f) kann durch die Verwendung sicherer Signatursysteme, durch Zeitstempel von synchronisierten Uhren, Zufallszahlen, Prüfsummen oder einfache Redundanz entgegengewirkt werden [24],[25],[26].

Die Angriffe (b) und (c) können nur durch eine entsprechende Sicherungsinfrastruktur [18] kompensiert werden. Dabei kann sich u.U. das häufige Wechseln von Schlüsseln zur Kompensation von Angriff (c) bei ungenügender Realisierung der Sicherungsinfrastruktur negativ auf die Robustheit gegen Angriff (b) auswirken, da die Konsistenz des Schlüsselverzeichnisses aufwendiger und damit fehleranfälliger werden kann. Der sogenannte „Man-in-the-Middle“ Angriff, bei dem sich der Angreifer in die Kommunikation der zu authentisierenden Kommunikationspartner einschleust und den jeweils anderen Partner „spielt“, ist durch vertrauenswürdige Zertifikate und gute Signatursysteme ebenfalls ausgeschlossen.

Die Verfügbarkeit zertifizierter öffentlicher Schlüssel und ihre authentische Verteilung sowie die sichere Aufbewahrung und korrekte Anwendung der geheimen Schlüssel sind deshalb Voraussetzung für ein sicheres Authentikationsverfahren.

4 Unterstützung von Separation und Mediation durch Authentikation in offenen Telekommunikationssystemen

Dieser Abschnitt zeigt die Anwendung der bisherigen Ergebnisse anhand von Protokollen, die an der Schnittstelle zwischen Teilnehmer- und Netzbereich zur Realisierung der folgenden Sicherheitsanforderungen integriert werden können:

(A) Authentikation zwischen Teilnehmer und Dienst (Berechtigungsprüfung, etc.)
(B) Sicherung der übermittelten Nutzdaten auf der Teilnehmeranschlußleitung
(C) Authentikation der Kommunikationspartner (indirekt unter Mitwirkung des Netzes)

Abschnitt 4.1 bespricht ein Protokoll zur Realisierung dieser Forderungen unter der Voraussetzung, daß die Kommunikations- und Nutzdaten innerhalb der Netze sicher sind, d.h. daß dem Netzbetreiber und Dienstanbieter bezüglich der Sicherheit der übermittelten Daten innerhalb des Netzes vertraut wird. Der Schwerpunkt der Betrachtungen liegt auf dem Aufbau und Inhalt der Nachrichten, welche zur Realisierung der Forderungen zwischen Teilnehmer und Netz ausgetauscht werden müssen. Abschnitt 4.2 skizziert die Integration dieser Nachrichten in die Teilnehmersignalisierung im Schmalband-ISDN (N-ISDN).

4.1 Integration von Sicherheit unter Mitwirkung des Netzbetreibers

Dieser Abschnitt stellt ein Protokoll vor, mit dem die Anforderungen (A) bis (C) unter Mitwirkung des Netzbetreibers realisiert werden können. Das Protokoll basiert auf dem Authentikationsprotokoll aus Bild 4.

Bild 5 zeigt ein Protokoll, das die genannten Anforderungen unterstützt. Die Nachrichtenteile S^{ix} enthalten die für die Authentikation notwendigen Parameter der *Nachricht i* aus Bild 4 zur

Authentikation von *Teilnehmer x* und *Vermittlungsstelle* V^x. Zusätzlich beinhalten die signierten Nachrichten weitere Parameter zur Realisierung der Forderungen (B) und (C), welche durch ihre Bindung an die Authentikation ebenfalls authentisch sind.

In die Authentikationsvorgänge zwischen Teilnehmer und Teilnehmervermittlungsstellen wird zur Installation eines gemeinsamen geheimen Schlüssels (Sitzungsschlüssel, SKey) das sogenannte Diffie-Hellman-Verfahren eingebettet [27]. Mit diesem Sitzungsschlüssel kann anschließend die Kommunikation zwischen Endgerät und Vermittlungsstelle verschlüsselt werden (Forderung B). Jeder Kommunikationspartner wählt bei diesem Verfahren einen Schlüsselteil $Skey^x$. Die Berechnung des Sitzungsschlüssels aus den Schlüsselteilen ist nur den Kommunikationspartnern möglich, die einen der Schlüsselteile erzeugt haben. Deshalb müssen die Schlüsselteile während der Übertragung nicht geheim gehalten werden. Schwächen des Diffi-Hellman-Verfahrens [28] werden durch die zugrundeliegende Authentikation kompensiert.

Das in Bild 5 dargestellte Authentikationsprotokoll realisiert auch für mobile Teilnehmer weitgehende Sicherheit unter Einbeziehung des Netzbetreibers. Dieser kann aufgrund der bekannten Identität des rufenden Teilnehmers die Zuordnung der Gebühren selbst vornehmen. Die Vertraute Instanz dient lediglich als Verzeichnisdienst für öffentliche Schlüssel (Protokollnachrichten 2 und 3) und muß bei entsprechenden Caching-Verfahren innerhalb der Vermittlungsstelle nicht bei jeder Dienstanforderung zwischengeschaltet werden (siehe auch Bild 2).

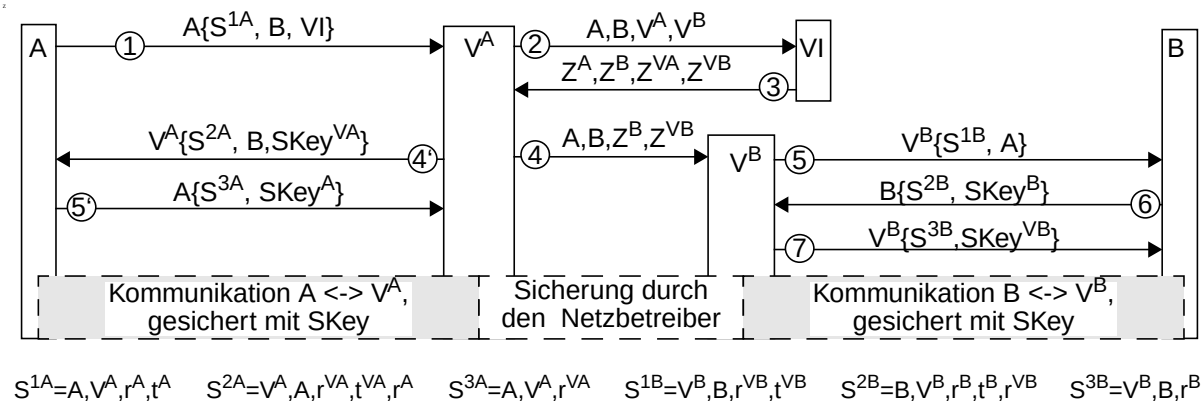

Bild 5: *Sicherung der Teilnehmer-Netz-Schnittstelle unter Einbeziehung des Netzes*

Die Caching-Strategie muß natürlich ausgleichen zwischen möglichst geringer zusätzlicher Netzlast durch Abfragen bei der Vertrauten Instanz und der Aktualität der Zertifikate. Das Sperren ungültiger öffentlicher Schlüssel kann bei der Nutzung zwischengespeicherter Zertifikate nicht berücksichtigt werden. Die Zertifikate Z^B und Z^{VB} für die gerufene Seite werden von der Vermittlungsstelle V^A des rufenden Teilnehmers zur Zielvermittlungsstelle V^B übertragen, um weitere Abfragen einzusparen. Ebenso werden die Identitäten A und B der Teilnehmer übermittelt. Falls das Netz die Verbindung nur dann durchschaltet, wenn die Authentikation der Teilnehmer A und B erfolgreich verläuft, dann ist auch Forderung (C) erfüllt.

4.2 Integration des Protokolles in die ISDN-Teilnehmersignalisierung

Die Implementierung der Protokolle im ISDN-Teilnehmerbereich erfordert zunächst die Kodierung der Nachrichten (1) bis (7) aus Bild 5. Die Anwendung, welche die Nachrichten generiert bzw. prüft, soll an dieser Stelle nicht näher beschrieben werden. Die in Tabelle 1 angegebenen Längen von Nachrichtenelementen sind als Richtwerte gedacht und sollen als Ausgangspunkt für die Bewertung der Integrationsfähigkeit des Protokolles in bestehende Signalisierprotokolle im Teilnehmerbereich dienen.

Aus dieser Kodierung folgt, daß die Nachrichtenlängen kleiner als 1536 Bits (= 192 Oktetts) sind. Die Signatur kann also bei Verschlüsselung mit 1536 Bit-Schlüsseln[1] mit einem asymmetrischen Verschlüsselungssystem in einem Block erfolgen. Die Signaturprüfung kann dadurch erfolgen, daß die Nachrichten mit dem öffentlichen Schlüssel des angeblichen Senders entschlüsselt werden und in der entschlüsselten Nachricht die enthaltene Identität des Senders mit der zum öffentlichen Schlüssel gehörigen Identität verglichen wird. Die Redundanz zur Bestimmung der Authentizität einer Nachricht besteht hier aus der Nachrichtenstruktur und dem Inhalt bestimmter Felder, welche bei der Prüfung mit dem falschen öffentlichen Schlüssel mit größter Wahrscheinlichkeit nicht mit den erwarteten Werten übereinstimmen werden.

Identitäten (A,B,V^A,V^B,VI)	8 Oktetts (16 Ziffern, 2^{64} Identitäten)
Zeitstempel (t^A,t^B,t^{VA},t^{VB})	8 Oktetts (Y,M,D,H,M,S,Timezone)
Zufallszahlen (r^A,r^B,r^{VA},r^{VB})	4 Oktetts
Schlüsselhälften nach Diffie-Hellman ($SKey^X$)	128 Oktetts (Modulo 1024bit)

Tabelle 1: *Mögliche Längenkodierung der Nachrichtenelemente des Protokolles*

Bei den in die bestehende Teilnehmersignalisierung im ISDN zu integrierenden Nachrichten kann eine Länge von 1536 Bits angenommen werden. Zur effizienten Entschlüsselung beim Empfänger ist es sinnvoll, die Identität des Signaturerzeugers unverschlüsselt voranzustellen.

Bild 6 zeigt die Signalisierung eines erfolgreichen Verbindungsaufbaus im ISDN [29],[30]. Die beim Verbindungsaufbau ausgetauschten Signale werden um die Nachrichten aus Bild 5 erweitert. Dazu werden sogenannte Facility-Informationselemente (FAC) verwendet, die auch für die Aktivierung von Dienstmerkmalen verwendet werden. Die Integration des Nachrichtenaustausches erfordert nur eine zusätzliche Facility-Nachricht zur Übertragung der Nachricht (5‘) aus Bild 5. Die weiteren Facility-Informationselemente können in reguläre Signalisiernachrichten des Verbindungsaufbaus integriert werden.

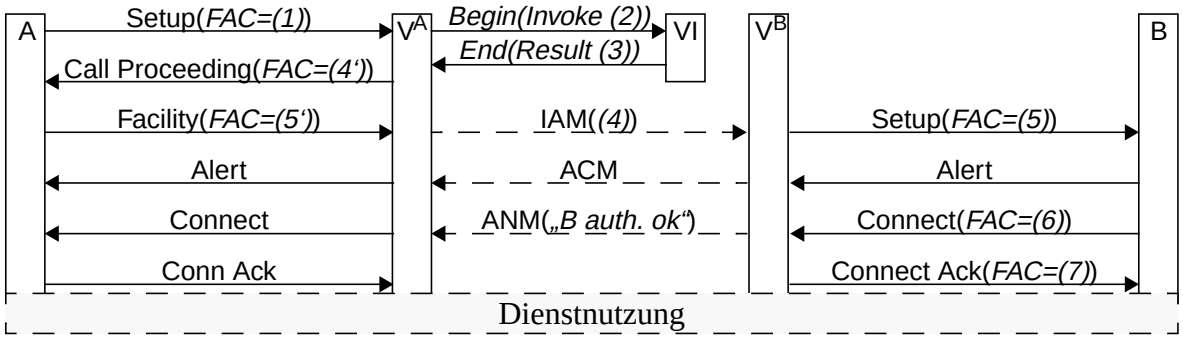

Bild 6: *Integration der Nachrichten in die Verbindungssignalisierung im (N-) ISDN*

Zur Abfrage gültiger Zertifikate der öffentlichen Schlüssel wird das Transaction Capability Application Service Element verwendet, welches im Zwischenamtsbereich für die verbindungsunabhängige Signalisierung zur Verfügung steht. Da die Signalisierung eine gesicherte Übertragung bietet (bezüglich Verlust von Nachrichten und Übertragungsfehlern) und die Zertifikate sowieso signiert sind, wird diese Abfrage der VI nicht speziell gesichert. Die Teilnehmer können die Zertifikate der Vermittlungsstellen bei Bedarf z.B. über ein Dienstmerkmal anfordern.

[1]Das öffentliche Signatursystem ist universell verwendbar und sollte größtmögliche Sicherheit bieten. Das Diffie-Hellman-Verfahren braucht nicht sicherer zu sein, als die anschließende Verschlüsselung bzw. die vom Netz im Zwischenamtsbereich gebotene Sicherheit. Die Schlüssellängen sind aus [23], S. 162, Tab. 7.6 abgeleitet.

Die maximale Nachrichtenlänge der dargestellten Signalisiernachrichten innerhalb der Teilnehmersignalisierung beträgt im (N-) ISDN 260 Oktetts. Die Länge der zur Zeit verwendeten Nachrichten beim normalen Verbindungsaufbau liegt meist deutlich unter 50 Oktetts, so daß die zusätzlichen Daten integrierbar sind, ohne eine Segmentierung erforderlich zu machen.

Falls eine Authentikation erfolglos verläuft, sollte dies dem A-Teilnehmer angezeigt und die Dienstanforderung abgebrochen werden. Da die Identität des rufenden Teilnehmers mit der Durchschaltung des Rufes zum gerufenen Teilnehmer feststeht, kann dem B-Teilnehmer – falls vom A-Teilnehmer gewünscht – die geprüfte Identität von A angezeigt werden (Forderung C).

Bewertung des Verfahrens:

Die Teilnehmer sind vor dem Durchschalten einer Verbindung authentisiert, da deren Authentikation mit der Weiterleitung der Connect-Nachricht abgeschlossen ist. Die Authentikation des rufenden Teilnehmers ist schon vor der Einleitung des Verbindungsaufbaus abgeschlossen. Der gerufene Teilnehmer wird bei gemeinsam genutzten Endgeräten sein Sicherheitsmodul erst nach der Dienstanzeige (Klingelsignal beim Telefon) in das Endgerät einführen, so daß Nachricht 6 in Bild 6 frühestens mit der Connect-Nachricht übertragen werden kann.

Zur Sicherung der Datenaustauschphase wird während des Verbindungsaufbaus ein gemeinsamer Schlüssel zwischen Endgerät und Vermittlungsstelle installiert, während innerhalb der Netze die Sicherung der Daten dem Netzbetreiber übertragen wird. Deshalb muß dieser für beide Teilnehmer vertrauenswürdig sein. Aufgrund bekannter rechtlicher Anforderungen an den Netzbetreiber sind die übertragenen Informationen mit diesem Verfahren nicht gegen Zugriffe in- und ausländischer staatlicher Dienste geschützt.

5 Zusammenfassung und Ausblick

Das vorgestellte Konzept zur Bereichsbildung zeigt einen Weg zur wirtschaftlichen Integration von Sicherheitsmechanismen auf. Es bezieht gegebene Sicherheitsanforderungen, Verantwortlichkeiten und technische Randbedingungen ein und ermöglicht dadurch effiziente Sicherheitsmechanismen. Separation und Mediation bilden die Basis für die Einordnung von Sicherheitsmechanismen und fördern das Verständnis für deren Wirkung. Die Bedeutung gemeinsamer Vertrauter Instanzen und Möglichkeiten für deren Einbindung in die Dienstanforderung im ISDN wurden an einem Beispiel erläutert.

Vertrauenswürdige Verzeichnisdienste spielen im Umfeld der spontanen, sicheren Kommunikation in offenen Systemen eine zentrale Rolle. Deshalb wird für die Nutzung von Kommunikationsdiensten in privaten und öffentlichen Bereichen wegweisend sein, wie die Vertrauenswürdigkeit verschiedener Interessengruppen gewonnen werden kann. Aus technischer Sicht sind hier vor allem die Zertifikation zu nennen [31], der im Rahmen der Zuverlässigkeit und der unabhängigen Kontrolle als Basis für die Vertrauenswürdigkeit von Technik eine zentrale Rolle zukommt. Die Implementierung von Verzeichnisdiensten kann im Intelligenten Netz durch zertifizierte Dienste unabhängiger Netzbetreiber realisiert werden.

Das vorgestellte Protokoll zur Sicherung der Teilnehmer-Netz-Schnittstelle wurde bezüglich der Länge von Nachrichten auf seine Integrationsfähigkeit in die Teilnehmersignalisierung im Schmalband-ISDN geprüft. Untersuchungen von Zeitverzögerungen, die durch die Generierung und Prüfung der zusätzlichen Nachrichtenteile (Signaturerzeugung, Signaturprüfung) innerhalb des Protokollablaufs entstehen, müssen im Rahmen einer Simulation durchgeführt werden. Die Vorteile einer Auslagerung der gesamten Authentikation und damit zusammenhängender Netzfunktionen in Vertraute Instanzen muß in Zusammenhang mit den neuen Möglichkeiten, welche das Intelligente Netz bieten wird, untersucht werden.

Literatur

[1] *T. Magedanz, R. Popescu-Zeletin:* „Intelligent Networks - Basic Technology, Standards and Evolution“, International Thomson Computer Press, 1996

[2] *J. Shattuck:* „Computer Matching Is A Serious Threat to Individual Rights“, Comm. ACM, Vol. 27, No. 6, June, 1984, pp. 538-541

[3] *A. Roßnagel, P. Wedde, V. Hammer, U. Pordesch:* „Die Verletzlichkeit der Informationsgesellschaft“, 2. Auflage, Westdeutscher Verlag GmbH, Opladen, 1990

[4] *G. Arndt, R. Lueder:* „Bewegungsfreiheit in allen Netzen“, Siemens telcom report *16*, 2/1993, pp. 67-69

[5] *R. Sailer, P. J. Kühn:* „Ein Domain-Konzept zur systematischen und wirtschaftlichen Integration von Sicherheit in Kommunikationsnetze“, it+ti Informationstechnik und Technische Informatik, Heft 4, 1996

[6] *B. Richter, M. Sobirey, H. König:* „Auditbasierte Netzüberwachung“, *PIK*, 19, 1996, Heft 1, pp. 24-32

[7] *J. Rushby, B. Randell:* „A Distributed Secure System“, IEEE Computer, July, 1983, pp. 55-67

[8] *A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner:* „Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule“, Proc. Verläßliche Informationssysteme (VIS‘ 95), Vieweg, 1995

[9] *R. Sandhu, P. Samarati:* „Access Control: Principles and Practice“, IEEE Comm. Magazine, 9/1994, pp. 40ff

[10] *N. Pohlmann:* „Schutz von LANs und LAN-Kopplung über öffentliche Netze“, *DATACOM*, 6, 1995, pp. 50ff

[11] *M. Warwick:* „Feeling Insecure?“, Communications International, January 1996, pp. 37

[12] *W. Langenheder, U. Pordesch:* „Sicherheit und Vertrauen in der Kommunikationstechnik - Soziologische Ansätze und Methoden“, it+ti Informationstechnik und Technische Informatik, Schwerpunktheft 4, 1996

[13] *B. Miller:* „Vital signs of identity“, IEEE Spectrum, February 1994, pp. 22-30

[14] *H.-P. Königs*: „Cryptographic Identification Methods for Smart Cards in the Process of Standardization“, IEEE Communications Magazine, June 1991, pp. 42-48

[15] „Data Networks And Open System Communications, Directory, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework“, ITU-T Recommendation X.509, 1993

[16] *C. I‘Anson, C. Mitchell:* „Security Defects in CCITT Recommendation X.509 - The Directory Authentication Framework“, ACM Computer Communication Review, Vol. 20, No. 2, April, 1990, pp. 30-34

[17] *R. L. Rivest, A. Shamir, L. Adleman*: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“, Comm. ACM, Volume 21, No. 2, February 1978, pp. 120-126

[18] *V. Hammer (Hrsg.), M. J. Schneider, A. Roßnagel, J. Bizer, C. Kumbruck, U. Pordesch:* „Sicherheitsinfrastrukturen - Gestaltungsvorschläge für Technik, Organisation und Recht“, Springer Verlag, 1995

[19] *G. Tsudik:* „Message Authentication with One-Way Hash Functions“, *ACM Computer Communication Review*, Vol. 22, No. 5, October, 1992, pp. 29-38

[20] *J. H. Moore:* „Protocol Failures in Cryptosystems“, *Proc. IEEE*, Vol. 76, No. 5, May, 1988, pp. 594-602

[21] *A. Beutelspacher, J. Schwenk, K. - D. Wolfenstetter:* „Moderne Verfahren der Kryptographie“, Vieweg, 1995

[22] *M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thomson, M. Wiener:* „Minimal Key Lengths For Symmetric Ciphers To Provide Adequate Commercial Security“, ftp://ftp.research.att.com/dist/mab/keylength.ps, January, 1996

[23] *B. Schneier:* „Applied Cryptography“, 2nd ed., John Wiley & Sons, Inc., 1996

[24] *M. Abadi, R. Needham:* „Prudent Engineering Practice for Cryptographic Protocols“, Digital, Systems Research Center, Research Report No. 125, Palo Alto, California, June 1994

[25] *B. C. Neuman, S. G. Stubblebine:* „A Note on the Use of Timestamps as Nonces“, ACM Operating Systems Review, Vol. 27, No. 2, April, 1993, pp. 10-14

[26] *T. Y. C. Woo, S. S. Lam:* „A Lesson on Authentication Protocol Design“, ACM Operating Systems Review, Vol. 28, No. 3, July 1994, pp. 24-37

[27] *W. Diffie, M. E. Hellman*: „New Directions in Cryptography“, IEEE Transactions On Information Theory, Volume 22, No. 6, November 1976, pp. 644-654

[28] *R. L. Rivest, A. Shamir:* „How to Expose an Eavesdropper“, *Comm. ACM*, Vol. 27, No. 4, 1984, pp. 393-395

[29] *G. Bandow, H. Gottschalk, D. Gehrmann, W. Hlavac, H. Koch, W. Müller, D. Schwetje:* „Zeichengabesysteme - Eine neue Generation für ISDN und intelligente Netze“, L.T.U. - Vertriebsgesellschaft mbH, Bremen, 2. Auflage, 1995

[30] „Digital Subscriber Signalling System No. 1 (DSS1), Network Layer, User-Network Management“, ITU-T Recommendations Q.930-Q.940, Geneva, 1989

[31] *K. Rannenberg:* „Evaluationskriterien zur IT-Sicherheit - Entwicklungen und Perspektiven in der Normung und außerhalb“, Verläßliche IT-Systeme, GI-Fachtagung, Vieweg, April 1995