6

Integration von Authentikations-verfahren in Kommunikationsnetze unter Verwendung separat sicherbarer Bereiche[1]

R. Sailer, P. J. Kühn[2]

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 Dieser Beitrag erweitert den im Tagungsband der KIVS ‘97 unter dem Titel „Authentikation als Grundlage für die Skalierung von Sicherheit in der Kommunikationstechnik“ erschienenen Beitrag um wesentliche Aspekte der Implementierung.

2 Universität Stuttgart, Institut für Nachrichtenvermittlung und Datenverarbeitung, Email: {sailer,kuehn}@ind.uni-stuttgart.de

6.1 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. Ein entsprechendes Beispiel stellt das Einrichten zeit- und ursprungsabhängiger Rufumleitungen beim Telefondienst dar. 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 [MaPo_96]), 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, 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 ist auch das Einbeziehen der Kommunikationshäufigkeit und der Nutzung von Mehrwertdiensten sowie die Ableitung von Interessen der einzelnen Teilnehmer bzw. Informationen über deren berufliche Orientierung, um diese anschließend 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 [Shat_84].

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 [RoWe_90] macht die „Nachrüstung“ der Telekommunikationsnetze mit Mechanismen erforderlich, die die steigenden Sicherheitsanforderungen der Nutzer und auch der Netzbetreiber bzw. Dienstanbieter befriedigen können.

6.2 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),
- *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 interpretierbaren 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 der Netze 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 oder Protokollierung 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.

Zukünftiges Dienstnutzungs-Szenario

Die Anforderungen an die Unterstützung der Mobilität von Teilnehmern werden zukünftig auch im Festnetzbereich steigen (Universal Personal Telecommunications [ArLu_93]). 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. Abb. 6.1 zeigt die zugrundeliegende Konfiguration. Das Sicherheitsmodul (SM) vertritt den Teilnehmer gegenüber dem Endgerät und dem Kommunikationsnetz bei der Realisierung und Anwendung von Sicherheitsfunktionen.

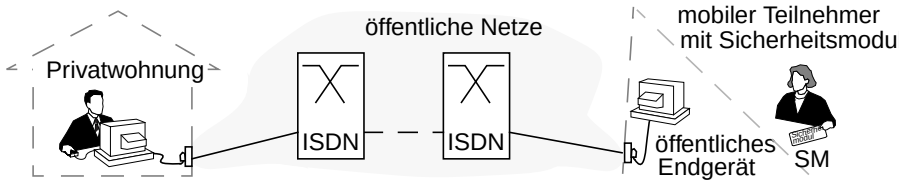


Abbildung 6.1: Aufgliederung des Telekommunikationsnetzes in Bereiche

Abschnitt 6.3 führt zunächst in allgemeine Konzepte zur Realisierung verschiedener Sicherheitsanforderungen ein. Abschnitt 6.4 bespricht Mechanismen zur Authentikation, welche als Grundlage dienen für das in Abschnitt 6.5 dargestellte Protokoll zur Sicherung der Teilnehmer-Netz- Schnittstelle im ISDN.

6.3 Bildung von separat sicherbaren Bereichen

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 [SaKu_96]:

- Zuständigkeit 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, Zugriffs-

rechte gesetzt, Schlüssel installiert und aktualisiert und Überwachungsergebnisse (z. B. Protokoll-Dateien, siehe [RiSo_96]) 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 Abb. 6.1 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* [RuRa_83].

- *Separation* zielt auf die gegenseitige Abgrenzung von Informationsträgern (Nutzdaten und Steuerdaten) ab, die verschiedenen Sicherheitsanforderungen unterliegen bzw. unterschiedlichen Bereichen zugeordnet sind. In Abb. 6.1 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.

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 Abb. 6.1 an Beispielen veranschaulicht.

Physikalische Separation: Eine physikalische Separation kann zur Sicherung von besonders schützenswerten Daten genutzt werden. Sie wird realisiert, indem 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 [PfPf_95].

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 [SaSa_94]. 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 sind gegenwärtig folgende Separations-Mechanismen zur Abgrenzung von Daten verschiedener Verbindungen bzw. Nutzer unterscheidbar:

- *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 Bearbeitung verschiedener Verbindungen innerhalb einer Vermittlungsstelle.
- *Temporäre Separation* ist dann gegeben, wenn Daten verschiedener Verbindungen zeitlich versetzt übermittelt werden.

Die temporäre und die logische Separation sind nur innerhalb vertrauenswürdiger Bereiche realisierbar, da ihre Wirksamkeit auf der Implementierung des jeweiligen Zugriffsverfahrens 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 (Nutzdaten) 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 [Pohl_95] realisiert werden. In [Warw_96] werden anschaulich negative Auswir-

kungen beschrieben, welche durch das Verwählen bei der Nutzung eines Telefax-Dienstes entstehen können.

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 verschiedenen Bereichen muß deshalb in einer Umgebung realisiert werden, die für alle beteiligten 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 dabei 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 [LaPo_96] näher untersucht.

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 6.5 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 Abb. 6.2). Der Teilnehmer fordert, daß nur jene Dienste abgerechnet werden, die auch von 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 Netzbe-

reich (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 Dienstanbieters bzw. des genutzten Dienstes vor der Dienstnutzung prüfen.

Abschnitt 6.4 führt in ein international standardisiertes kryptographisches Authentikationsverfahren 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 anwendbar. Dieses spielt gerade bei mobilen Teilnehmern und bei der Diversität von nicht flächendeckend vertretenen Netzbetreibern eine wichtige Rolle.

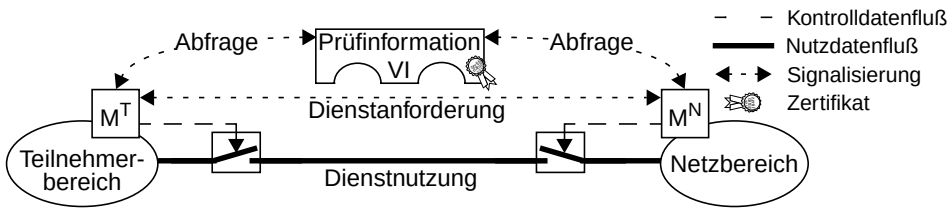


Abbildung 6.2: Vertraute Instanzen als Vermittler zwischen Bereichen

Die Mediatoren M^T und M^N (siehe Abb. 6.2) 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 6.5 näher untersucht.

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 kann im Rahmen dieses Beitrages nicht näher eingegangen werden.

6.4 Authentikation in der 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.

Abb. 6.3 zeigt, wie die Authentikation zweier Teilnehmer A und B als Dienst nach dem Vorbild des OSI-Referenzmodelles dargestellt und realisiert werden kann.

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 [Mill_94], 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 [Koen_91] 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.

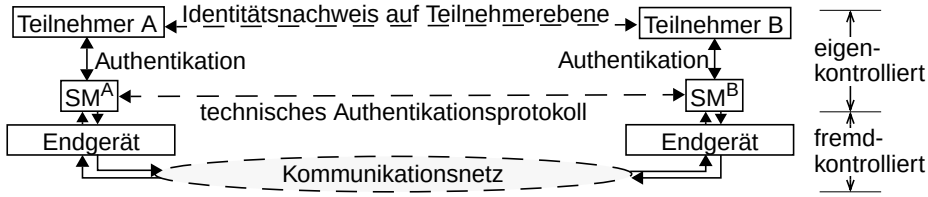


Abbildung 6.3: Kommunikationsmodell für die Authentikation zwischen zwei Teilnehmern

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.

Basisprotokoll für die Authentikation

Das vorgestellte Protokoll basiert auf der X.509-Empfehlung der ITU-T [X509_93, AnMi_90] und damit auf einem asymmetrischen Signatursystem [RiSh_78], 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 (Abb. 6.4).

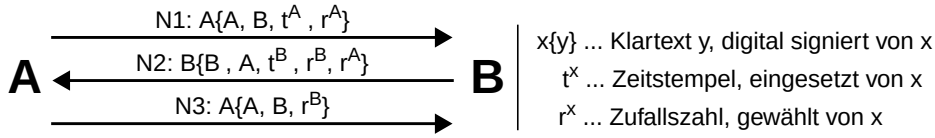


Abbildung 6.4: Technisches Authentikationsprotokoll basierend auf ITU-T X.509

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.

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 [HaSc_95] besprochen. Die VI in Abb. 6.2 kann beispielsweise einen solchen Verzeichnisdienst realisieren.

Prinzipiell könnte der Identitätsnachweis auch mit Hilfe symmetrischer Kryptosysteme realisiert werden. Die Kommunikationspartner müssen dabei über gemeinsame geheime Schlüssel verfügen. Die mit diesen gemeinsamen geheimen Schlüsseln der kommunizierenden Instanzen 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 [Tsud_92, Lang_96], ohne daß eine Verschlüsselung durchgeführt werden muß. Alternativ können auch die einfachen Hash-Werte mit dem geheimen Schlüssel verschlüsselt werden.

Diese auf gemeinsamen geheimen Schlüsseln aufbauenden Verfahren erscheinen in offenen Systemen – insbesondere bei der spontanen Kommunikation mit vorher nicht bekannten Kommunikationspartnern – unpraktikabel beziehungsweise setzen zur Installation gemeinsamer geheimer Schlüssel ihrerseits ein asymmetrisches Verschlüsselungssystem voraus. Die Urheberschaft von Nachrichten kann mit symmetrischen Verfahren nicht direkt 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 Vertrauensinstanz authentisieren.

Angriffsmodell für die Authentikation

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

Die Sicherheit des vorgestellten Authentikationsverfahrens ist abhängig von der Korrektheit der Implementierung des verwendeten Verfahrens [Moor_88] und der Sicherungsmechanismen des zugrundeliegenden Protokolles. Das Signatursystem muß u.a. robust sein gegen die allgemein bekannten Angriffsversuche

zur Erlangung des geheimen Schlüssels [BeSc_95], 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 [BlDi_96, Schn_96] 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 Abb. 6.4) während der Übertragung vor unerkannter 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:

1. Impersonation durch Angabe einer falschen Identität,
2. Einführen falscher öffentlicher Schlüssel,
3. Stehlen geheimer Schlüssel,
4. Ändern des Chiffrats,
5. Ändern des Klartextes und
6. Wiedereinspielen abgehörter Nachrichten.

Den Angriffen 1., 4., 5. und 6. kann durch die Verwendung sicherer Signatursysteme, durch Zeitstempel von synchronisierten Uhren, Zufallszahlen, Prüfsummen oder einfache Redundanz entgegengewirkt werden [AbNe_94, NeSt_93, WoLa_94].

Die Angriffe 2. und 3. können nur durch eine entsprechende Sicherungsinfrastruktur [HaSc_95] kompensiert werden. Dabei kann sich u.U. das häufige Wechseln von Schlüsseln zur Kompensation von Angriff 3. bei ungenügender Realisierung der Sicherungsinfrastruktur negativ auf die Robustheit gegen Angriff 2. 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.

Implementierungsabhängige Sicherheitsaspekte des Authentikationsprotokolles

Die Sicherheit des in Abb. 6.4 dargestellten Authentikationsprotokolles muß bei der Implementierung erhalten werden. Bei den bisherigen Sicherheitsuntersuchungen wurde implizit davon ausgegangen, daß die verschiedenen Nachrichten unterscheidbar und die enthaltenen Parameter eindeutig zuordenbar sind.

In [Syve_93] beschreibt Syverson eine Familie von Angriffen, deren erfolgreiche Durchführbarkeit von implementierungstechnischen Details abhängen kann. Obwohl Syverson die Angriffe anhand von Authentikationsprotokollen [NeSt_93] basierend auf symmetrischen Kryptosystemen beschreibt, ist dieser Angriffstyp auch bei Verwendung asymmetrischer Kryptosysteme denkbar.

Der beschriebene Angriffstyp beruht auf einer inkonsistenten Sicht der beiden Authentikationspartner auf die Parameter der Authentikationsnachrichten und nutzt die Wiederverwendbarkeit von abgehörten Authentikationsnachrichten aus. Nachrichten werden dabei an einer anderen Stelle innerhalb eines Authentikationsablaufes eingespielt und verursachen beim Empfänger – sofern dies unbemerkt bleibt – deshalb eine inkonsistente Sicht auf die nun in möglicherweise geänderter Reihenfolge enthaltenen Parameter [Syve_93].

Zur Absicherung gegen eine inkonsistente Sicht auf Parameter und Nachrichten wird deshalb an dieser Stelle die eindeutige Typisierung aller Parameter und auch die eindeutige Kennzeichnung der Position einer Nachricht innerhalb eines Authentikationsvorganges empfohlen. So sollten innerhalb einer Nachricht Zufallszahlen, Zeitstempel, Identitäten und gegebenenfalls weitere Parameter – insbesondere Schlüsselteile – unabhängig davon unterscheidbar sein, an welcher Position innerhalb der Nachricht sie auftreten. Diese zusätzliche Information scheint aufgrund der zusätzlich gewonnenen Eindeutigkeit in den meisten Fällen effizient. Die Bedrohung, im Rahmen der Erweiterung von Authentikationsnachrichten neue Angriffsmöglichkeiten dadurch einzuführen, daß kodierte Nachrichten nun an anderer Stelle eines Authentikationsvorganges unbemerkt eingespielt werden können, wird dadurch minimiert.

Um bei der Authentikation nicht von lose synchronisierten Uhren zwischen A und B abhängig zu sein, können die Zeitstempel t^A und t^B nach ihrer Erzeugung allen Nachrichten des fortlaufenden Authentikationsprotokolls mitgegeben

werden. Sie erhalten damit den Status einer fortlaufenden eindeutigen Transaktionsnummer und erfordern lediglich eine fortlaufende lokale Zeit. Dazu muß Nachricht N2 (Abb. 6.4) um den Zeitstempel t^A und Nachricht N3 um die Zeitstempel t^A und t^B erweitert werden. Die Instanzen prüfen innerhalb empfangener Nachrichten bei diesem Verfahren lediglich ihren eigenen Zeitstempel zur Sicherheit gegen das Wiedereinspielen von Nachrichten.

Alternativ können über zusätzliche Nachrichten solche inkonsistenten Sichten ausgeschlossen werden. Ein Beispiel für ein solches Protokoll zeigt [KeSc_92]. Dieses wirkt sich jedoch aufgrund zusätzlicher Signallaufzeiten und Antwortzeiten und aufgrund komplizierter werdender Behandlungsprozesse innerhalb der Signalisierung in offenen Telekommunikationsnetzen nachteilig aus.

6.5 Separation und Mediation im ISDN

Dieser Abschnitt beschreibt eine Möglichkeit zur Erweiterung der konventionellen Verbindungsbehandlung im ISDN dahingehend, daß die folgenden – aus Sicherheitssicht notwendigen – zusätzlichen Anforderungen an der Teilnehmer-Netz-Schnittstelle garantiert werden können:

a. Prüfung der Identität von Dienstnutzer (Teilnehmer) und Dienstanbieter (als Grundlage der Berechtigungsprüfung, etc.)

b. Sicherung der übermittelten Nutzdaten zwischen Endgerät und Teilnehmervermittlungsstelle

c. Prüfung der Identität der Kommunikationspartner (indirekt) unter Mitwirkung des Netzbetreibers

Als Bereiche werden Endgeräte, das Kommunikationsnetz zwischen den Vermittlungsstellen und der zwischenliegende Anschlußbereich unterschieden.

Das *Endgerät* unterliegt i.a. der direkten Zugriffskontrolle durch den Nutzer. Mindestens können zertifizierte Endgeräte genutzt werden (indirektes Vertrauen) oder eigene Endgeräte mitgeführt werden (Endgerätemobilität).

Zum *Anschlußbereich* zählen der S_0-Bus mit weiteren angeschlossenen Endgeräten anderer Nutzer, die Anschlußleitung, der Netzabschluß und gegebenenfalls weitere Infrastruktur. Der Anschlußbereich verbindet Endgeräte mit dem Kommunikationsnetz und unterliegt nicht der direkten Zugriffskontrolle durch den Nutzer oder den Netzbetreiber. Dieser Bereich muß deshalb grundsätzlich, d.h. ohne weitere Annahmen, als nicht vertrauenswürdig angesehen werden. Insbesondere bei der Nutzung fremder Anschlüsse durch mitgeführte Endgeräte können keine zuverlässigen Annahmen über die Sicherheit zwischen dem sichtbaren Netzanschluß und der Teilnehmervermittlungsstelle gemacht werden.

Das *Kommunikationsnetz* ist i.a. für nichtprivilegierte Angreifer nur mit besonders hohem Aufwand angreifbar – zusätzliche Sicherungsmechanismen können in diesem Bereich durch den Netzbetreiber bzw. Dienstanbieter realisiert werden (Zugangs- und Zugriffskontrollmechanismen, Verschlüsselung).

Im Rahmen der *Separation* werden die über den Anschlußbereich zwischen Endgerät und Kommunikationsnetz ausgetauschten Nutzdaten (gegebenenfalls auch die Signalisierdaten) im Endgerät bzw. innerhalb der Teilnehmervermittlungsstelle kryptographisch gesichert. Innerhalb des Anschlußnetzes wird Anforderung b. also durch eine *kryptographische Separation* der Nutzdaten garantiert. Innerhalb des Endgerätes und innerhalb des Kommunikationsnetzes sind die Nutzdaten mindestens logisch separiert (Verbindungskennung, Adressen, konventionelle Zugriffsmechanismen).

Mediatoren sollen die Bereichsgrenzen von Endgerät und Kommunikationsnetz absichern und zwischen diesen Bereichen vermitteln. Die dazu notwendigen Mechanismen und ihre Eingliederung in das ISDN stehen im Mittelpunkt der folgenden Betrachtungen.

Das Durchschalten einer Verbindung zwischen dem Endgerät und dem Netz ist bezüglich der Nutzung von Funktionen (Diensten) und dem Austausch von Nutzdaten nach Abschnitt 6.3 durch einen entsprechenden Mediator zu sichern. Die Anforderungen a. und c. müssen durch diesen Mediator garantiert werden.

Die folgenden Abschnitte beschreiben sowohl die gegenwärtig vorhandenen Mechanismen zur Abgrenzung der Bereiche Endgerät und Kommunikationsnetz als auch die Realisierung erweiterter Funktionen zur ergänzenden Absicherung und zur Realisierung der Anforderungen a. - c. Dabei wird vorausgesetzt, daß die Kommunikations- und Nutzdaten innerhalb der Netze und innerhalb des Endgerätes sicher sind, d.h. daß dem Netzbetreiber und Dienstanbieter bezüglich der Sicherheit der übermittelten Daten innerhalb des Netzes vertraut wird. Gegebenenfalls können innerhalb der Endgeräte (z. B. innerhalb der Anwendung) Sicherheitsmechanismen realisiert werden, welche Ende-zu-Ende zwischen den Endgeräten wirken und Nutzdaten auch im Netz absichern.

Teilnehmer- und Netzbereich im ISDN

Das ISDN bietet für den Teilnehmer Möglichkeiten zum gleichzeitigen Betrieb mehrerer Endgeräte am selben ISDN-Teilnehmeranschluß. Die hier betrachtete Konfiguration (Basisanschluß) sieht 2 Nutzkanäle je Anschluß vor. Diese Nutzkanäle können unabhängig voneinander genutzt werden. Die Steuerungsprozesse im Endgerät und in der Vermittlungsstelle handeln beim Aufbau einer Verbindung den für diese Verbindung verwendeten Nutzkanal aus. Die klare Schnittstelle zwischen Netzbereich und Teilnehmerbereich, welche aus Gründen der Sicherheit des Netzes vor unautorisierter Nutzung besteht, erfordert

auch bisher Mechanismen, welche innerhalb der Vermittlungsstelle und im Endgerät eine Abgrenzung realisieren.

Abb. 6.5 zeigt ein Endgerät im Teilnehmerbereich, den Netzabschluß (NT1) und die erste Vermittlungsstelle im ISDN. Eine Verbindung wird vom Endgerät und der Vermittlungsstelle mit Hilfe der Verbindungssteuerung aufgebaut. Zur Synchronisierung (z.B. Anstoß eines Verbindungsaufbaus) tauschen die Prozesse zur Verbindungsbehandlung in Endgerät und Vermittlungsstelle sogenannte Steuernachrichten aus. Nach erfolgreichem Verbindungsaufbau wird ein Nutzkanal des Anschlusses auf den durch das Netz vermittelten Verbindungskanal durchgeschaltet. Entsprechend wird der jeweilige Nutzkanal am gerufenen Anschluß zur Übertragung von Nutzdaten freigegeben.

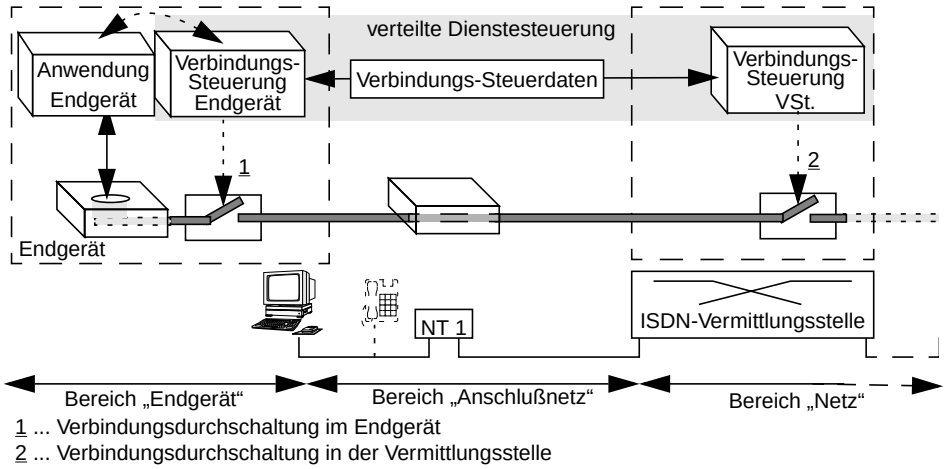


Abbildung 6.5: Herkömmliche Abgrenzung von Teilnehmer- und Netz-Bereichen im ISDN

Sowohl im Endgerät, als auch in der Vermittlungsstelle im ISDN sind bereits Zugriffskontrollmechanismen integriert, welche – wie oben beschrieben – die Schnittstelle zwischen Teilnehmerbereich und Kommunikationsnetz absichern. Hierzu gehört beispielsweise die Identifizierung des Ursprungs der Verbindungsanforderung (physikalische Anschlußadresse) und eine aufsetzende Berechtigungsprüfung für den angeforderten Ruf innerhalb der Teilnehmervermittlungsstelle. Auch die Zuordnung der Nutzungsentgelte beruht auf dem identifizierten Anschluß.

Die *Verbindungssteuerung im Endgerät* regelt z. B. den Verbindungsaufbau und die Nutzung der zur Verfügung stehenden Nutzkanäle im Teilnehmerbereich. Bevor eine Verbindung zum Austausch von Nutzdaten zwischen verschiedenen

Endgeräten genutzt werden kann, muß eine Nutzkanalverbindung aufgebaut werden. Dazu fordert die entsprechende Anwendung die Verbindungssteuerung im Endgerät auf, eine Verbindung zum gewünschten ISDN-Anschluß herzustellen (z. B. beim Telefondienst). Die Verbindungssteuerung im Endgerät muß dazu mehrere Teilaufgaben durchführen:

- Anforderung einer durchgeschalteten Verbindung zum jeweiligen Ziel bei der Teilnehmervermittlungsstelle.
- Austausch entsprechender Synchronisierinformation (Steuernachrichten) mit der Vermittlungsstelle (z.B. Wahlziffern).
- Aushandlung eines freien Nutzdatenkanals zwischen Endgerät und Vermittlungsstelle, der dieser Verbindung exklusiv zugeordnet wird.
- Freigabe eines aufgebauten Nutzkanals für Anwendungen im Endgerät.

Die *Verbindungssteuerung in der Teilnehmervermittlungsstelle* ist für weitergehende Aufgaben und Prüfungen zuständig:

- Zunächst wird auf der Basis von Berechtigungsinformation innerhalb der Vermittlungsstelle geprüft, ob die Verbindungsanforderung vom jeweiligen Anschluß aus zulässig ist (z. B. Prüfung von Dienstberechtigung, Rufziel).
- Verläuft die Berechtigungsprüfung positiv, so muß eine Verbindung durch das Netz zum entsprechenden Anschluß (Rufziel) vermittelt werden.
- Sofern der Verbindungsaufbau erfolgreich ist, wird die netzinterne Nutzdatenverbindung auf die ausgehandelten Nutzkanäle der jeweiligen Anschlüsse durchgeschaltet und den beteiligten Endgeräten die nun bestehende Verbindung angezeigt.

Die folgenden Abschnitte werden diese bestehenden Funktionen, welche von der Verbindungsbehandlung angestoßen werden, zur Realisierung zusätzlicher Sicherheitsanforderungen erweitern.

Erweiterung der Bereichsabsicherung

Dieser Abschnitt skizziert eine Integrationsmöglichkeit des in Abschnitt 6.4 vorgestellten Authentikationsverfahrens als Ergänzung der Verbindungsbehandlung zur Realisierung der Anforderungen a. und c. unter Mitwirkung des Netzbetreibers im ISDN und zur Installation von geheimen Schlüsseln zwischen den Endgeräten und der jeweiligen Teilnehmervermittlungsstelle zur Unterstützung von Anforderung b.

Die zu integrierenden Sicherheitsmechanismen müssen gegen Angriffe geschützt sein, damit sie ihre Wirkung entfalten können. Für die Umgebung am ISDN-Teilnehmeranschluß werden deshalb folgende *Annahmen* getroffen:

- Das Endgerät arbeitet korrekt und seine Funktion ist gegen Angriffe ausreichend geschützt. Es bildet also einen Vertrauensbereich für den Nutzer im Sinne von [SaFe_97].
- Der Netzbetreiber muß ebenfalls vertrauenswürdig sein. Die Sicherheit der Daten innerhalb des Netzes muß für die Nutzer ausreichend sein; die Nutzdaten müssen im Netz bei Bedarf durch den Netzbetreiber geschützt werden[1].

Die Konzeption für eine erweiterte Verbindungsbehandlung am ISDN-Teilnehmerzugang zeigt Abb. 6.6. Die Bereiche *Endgerät*, *Anschlußnetz* und *Netz* werden durch geeignete Maßnahmen gegeneinander abgegrenzt.

Das Endgerät prüft vor dem Durchschalten der Verbindung bzw. vor der Verbindungsannahme die *Identität des Netzbetreibers*. Darauf aufsetzende Anwendungen dürfen die Verbindung nur nach erfolgreicher Prüfung nutzen. Ebenso wird in der Teilnehmervermittlungsstelle die *Identität des Nutzers* geprüft, bevor seinem Verbindungswunsch entsprochen wird (Anforderung a.). Die dazu notwendige Authentikation baut auf einem asymmetrischen Signatursystem auf (vgl. Abschnitt 6.4). Die geheimen Signatur-Schlüssel befinden sich auf Kryptokarten, welche vor der Inanspruchnahme eines Endgerätes oder einer Anwendung dem entsprechenden Endgerät zugänglich gemacht werden müssen. Innerhalb der ortsfesten Vermittlungsstelle kann der zugehörige geheime Signaturschlüssel in einem Sicherheitsmodul fest installiert werden. Das zugrundegelegte Protokoll zur Identifikation der zugriffsfordernden Instanzen basiert auf dem Authentikationsprotokoll aus Abb. 6.4.

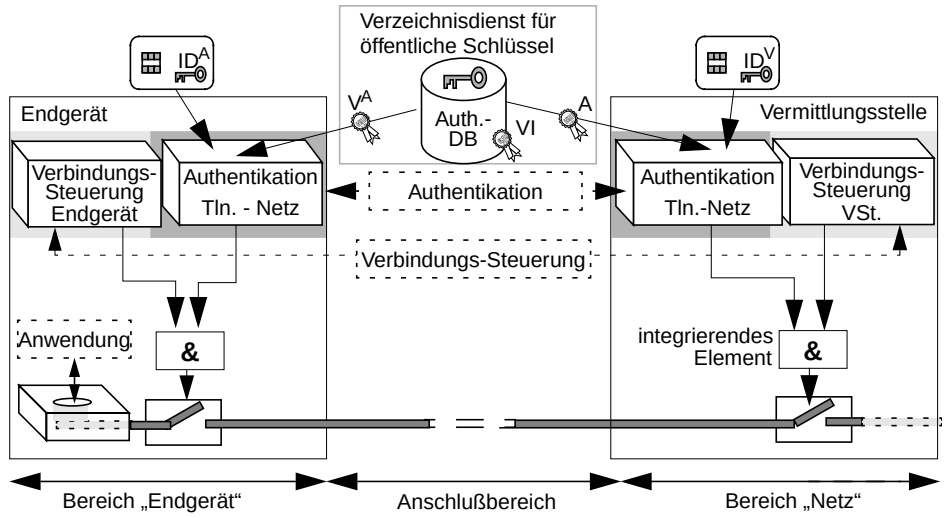
Zur **kryptographischen Separation** aller anschließend zwischen Endgerät und Vermittlungsstelle ausgetauschten Nutzdaten werden diese im Endgerät bzw. innerhalb der Vermittlungsstelle verschlüsselt. Der zugehörige Schlüssel kann im Rahmen der Authentikation ausgetauscht und installiert werden. Die verschlüsselten und integritätsgeschützten Daten können über den ungesicherten Anschlußbereich übertragen werden (Anforderung b.).

Die Prozeduren für die **Identifikation und Verschlüsselung** werden von allen am Kommunikationsdienst beteiligten Endgeräten durchgeführt. Das Ergebnis der Authentikation muß im Endgerät und in der Vermittlungsstelle verarbeitet werden, um die Verbindung genau dann durchschalten zu können, wenn alle Identitäten erfolgreich geprüft worden sind (Anforderung c.). Dieses muß durch das integrierende Element (vgl. Abb. 6.6) sichergestellt werden.

---

1 Sind die Endgeräte der Kommunikationspartner in der Lage, Daten zu ver- und entschlüsseln und sind die Implementierungen der Verfahren kompatibel, so kann beim Verbindungsaufbau auch ein gemeinsamer Sitzungsschlüssel zwischen den Endgeräten vereinbart werden. Damit können die nachfolgend ausgetauschten Daten Ende-zu-Ende-gesichert werden. Bezüglich der so gesicherten Daten stellen Verarbeitungsfehler im Netz nur noch im Hinblick auf die Verfügbarkeit dieser Daten beim Empfänger eine Bedrohung dar.

Abb. 6.6 zeigt die hinzugefügte Authentikationsfunktion und das integrierende Element, welches zusätzlich zu bestehenden Voraussetzungen für eine Verbindungsdurchschaltung auch die Ergebnisse der Authentikationsvorgänge miteinbezieht und den ausgehandelten Sitzungsschlüssel an eine entsprechende Verschlüsselungsfunktion weiterleitet. Die Ver- bzw. Entschlüsselungsfunktionen zum Schutz der Nutzdaten während ihrer Übertragung über den Anschlußbereich sind aus Gründen der Übersichtlichkeit nicht eingezeichnet.



ID^A ... Identität des A-Teilnehmers (Karte enthält Signierschlüssel + -algorithmus)
ID^V ... Identität der A-Teilnehmervermittlungsstelle (Karte enthält Signierschlüssel)
[&] ... Integrierendes Element für Verbindungssteuerung und Authentikation

Abbildung 6.6: Authentikation in Endgerät und ISDN-Teilnehmervermittlungsstelle

Die folgenden Abschnitte beschreiben die Integration dieser zusätzlichen Funktionen unter besonderer Berücksichtigung der bestehenden Technik und zielen somit auf eine wirtschaftliche Lösung ab.

Realisierungsaspekte der Bereichsabgrenzung

Der Schwerpunkt der folgenden Betrachtungen liegt auf der Architektur und Implementierung der erweiterten Bereichssicherung und auf dem Inhalt der Steuer-Nachrichten, welche zur Realisierung der zusätzlichen Sicherheitsfunktionen zwischen Teilnehmer und Netz ausgetauscht werden müssen. Es wird

eine Möglichkeit zur Integration entsprechender Nachrichten in die Teilnehmersignalisierung im Schmalband-ISDN aufgezeigt.

Abb. 6.7 zeigt die an der ergänzenden Sicherheitsfunktionalität beteiligten Instanzen (unterlegt). Der Nutzer muß im Besitz einer entsprechenden Kryptokarte sein, welche seinen geheimen Signierschlüssel und die Algorithmen zu seiner Nutzung enthält. In Endgerät und Vermittlungsstelle muß die *Authentisierungssteuerung* (AS) realisiert werden. Sie setzt – ebenso wie die herkömmliche Verbindungssteuerung und weitere Dienstmerkmale – auf den Funktionen der Schichten 1-3 des ISDN-D-Kanals auf. Diese Schichten unterstützen eine gesicherte Übertragung von Steuernachrichten zwischen Endgerät und Vermittlungsstelle im ISDN [SaFe_97].

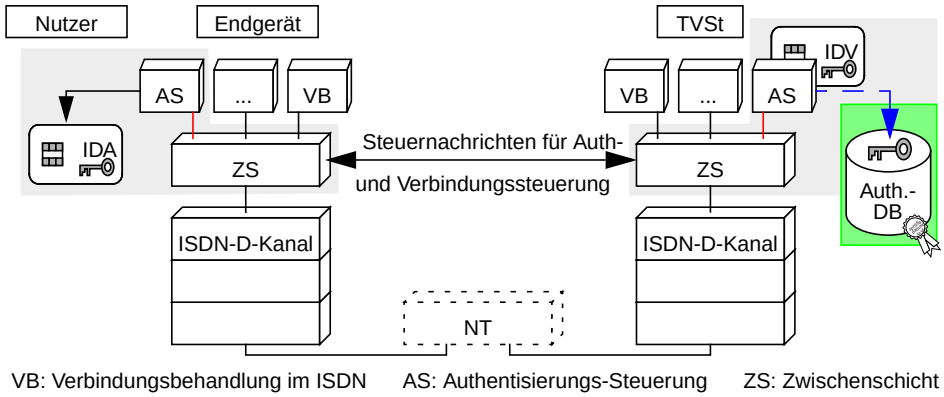


Abbildung 6.7: Einordnung ergänzender Mechanismen [SaKa_97]

Die *Zwischenschicht* (ZS) dient der transparenten Integration zusätzlicher Authentisierungs- und Verschlüsselungsfunktionen in Bezug auf die bestehenden Protokolle zur Signalisierung am ISDN-Teilnehmeranschluß und die Verbindungsbehandlung in Endgerät und (Teilnehmer-) Vermittlungsstelle. Die ZS erfüllt als Mediator in diesem Zusammenhang folgende Aufgaben:

- Die zusätzlich zwischen den AS-Blöcken in Endgerät und Vermittlungsstelle zu übertragenden Authentikationsnachrichten werden in die herkömmlichen Steuernachrichten des Verbindungsaufbaus integriert.
- Die bestehenden Anforderungen der Verbindungsbehandlung und die erweiterten Anforderungen der Authentikation müssen im Hinblick auf die Durchschaltung von Verbindungen integriert werden (integrierendes Element in Abb. 6.6).

Bevor auf die Funktion der Zwischenschicht näher eingegangen wird, soll das Protokoll erläutert werden, welches zwischen den ergänzten AS-Blöcken zur Authentisierung von Teilnehmern und Netzbetreiber ablaufen soll.

Protokoll zur Synchronisierung der Authentikationssteuerung

Die AS-Blöcke im Endgerät und in der Teilnehmervermittlungsstelle tauschen zur Authentisierung signierte Nachrichten basierend auf dem Authentikationsprotokoll nach CCITT X.509 (siehe Abb. 6.4 in Abschnitt 6.4) aus. Abb. 6.8 beschreibt die während der Authentikation ausgetauschten Nachrichten. Die zwischen Endgerät und Teilnehmervermittlungsstelle ausgetauschten Nachrichten (Nr. 1, 4‘, 5, 5‘, 6, 7) steuern die Authentikation. Die Nachrichtenteile S^{ix} enthalten die für die Authentikation notwendigen Parameter der *Nachricht i* aus Abb. 6.4 zur Authentikation von *Teilnehmer x* und *Vermittlungsstelle* V^x. Sie sind als Teil der Gesamtnachricht in der entsprechenden Signatur eingeschlossen und entsprechen so den Anforderungen aus Abschnitt 6.4.

Die Angabe des gewünschten Kommunikationspartners (A bzw. B) ist durch die Einbeziehung in die signierten Authentikationsnachrichten gesichert und ermöglicht – unter der Voraussetzung entsprechend ausgelegter Netzfunktionen – die Realisierung von Anforderung c.

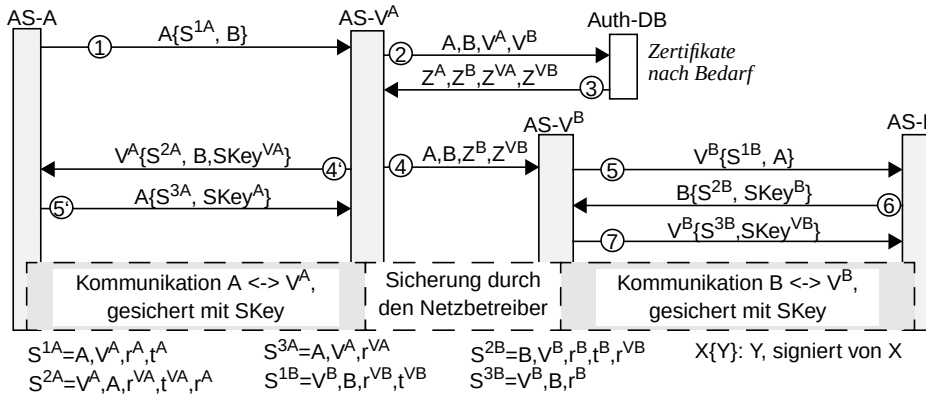


Abbildung 6.8: Authentisierungssteuerung zwischen Teilnehmer und Netz nach Abb. 6.7

Der Parameter $SKey^x$ bezeichnet den von der jeweiligen Instanz X erzeugten Schlüsselteil, der durch seine Einbeziehung in die signierten Nachrichten authentisch übertragen wird. Er wird zur Installation eines gemeinsamen gehei-

men Schlüssels (Sitzungsschlüssel, *SKey*) nach dem Diffie-Hellman-Verfahren in den Nachrichtenaustausch eingebettet [DiHe_76].

Jeder Kommunikationspartner X wählt bei diesem Verfahren einen Schlüsselteil $Skey^X$, der nach einer speziellen Vorschrift erzeugt wird. 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 Diffie-Hellman-Verfahrens [RiSh_84] werden durch die zugrundeliegende Authentikation kompensiert. Werden die Schlüsselteile entsprechend des Diffie-Hellman-Verfahrens erzeugt, zu Sitzungsschlüsseln zusammengesetzt und die über die Nutzdatenverbindung ausgetauschten Daten mit diesem Schlüssel kryptographisch gesichert, so ist auch Forderungen b. erfüllt.

Die Nachrichten 2 und 3 in Abb. 6.8 dienen zur Abfrage zertifizierter Prüfschlüssel für die Überprüfung der signierten Authentikationsnachrichten. Die Vertraute Instanz realisiert einen Verzeichnisdienst für die jeweils gültigen öffentlichen Schlüssel (Protokollnachrichten 2 und 3) und muß bei entsprechenden Caching-Verfahren innerhalb der Vermittlungsstelle nicht bei jeder Dienstanforderung zwischengeschaltet werden (siehe auch Abb. 6.2). Eine entsprechende Caching-Strategie muß ausgleichen zwischen möglichst geringer zusätzlicher Netzlast durch Abfragen bei der Vertrauten Instanz und der Aktualität der Zertifikate. Das Sperren ungültig gewordener öffentlicher Schlüssel kann bei der Nutzung zwischengespeicherter Zertifikate nicht ohne weiteres erkannt werden.

In Nachricht 4 werden die Identitäten A und B der Teilnehmer zusammen mit den Zertifikaten Z^B und Z^{VB} für die gerufene Seite von der Vermittlungsstelle V^A des rufenden Teilnehmers zur Zielvermittlungsstelle V^B übertragen, um weitere Abfragen einzusparen[1]. Die Verbindung darf im Netz nur dann durchgeschaltet werden, wenn die Authentikation der Teilnehmer A und B erfolgreich verläuft. Dann ist auch Forderung c. erfüllt. Eine Ausnahmebehandlung muß sowohl die Auslösung einer im Aufbau befindlichen Verbindung mit entsprechender Ausweisung (z.B. Cause = „Authentication Failed“), als auch das unbedingte Durchstellen von Notrufen ohne Authentikation ermöglichen.

Das in Abb. 6.8 dargestellte Authentikationsprotokoll realisiert auch für mobile Festnetz-Teilnehmer weitgehende Sicherheit unter Einbeziehung des Netzbetreibers. Dieser kann aufgrund der bekannten Identität des rufenden Teilnehmers die Zuordnung der Gebühren selbst vornehmen. Die korrekte Funktion des Endgerätes zur Sicherung der Nutzdaten wird vorausgesetzt. Der geheime

1 Weiterhin ist es denkbar, daß Zertifikate unabhängig von der Dienstnutzung beschafft werden, z. B. mit Hilfe von per Briefpost ausgetauschten Datenträgern, unabhängigen IN-Diensten oder abrufbar als Dienstmerkmal oder per E-Mail.

Signaturschlüssel verläßt die Kryptokarte des Teilnehmers jedoch nicht, so daß dieser bei korrekter Funktion der Kryptokarte nicht gefährdet ist.

Implementierungsaspekte

Die Implementierung der Protokolle im ISDN-Teilnehmerbereich erfordert zunächst die Kodierung der Nachrichten (1) bis (7) aus Abb. 6.8. Die Authentisierungssteuerung selbst, welche diese Nachrichten generiert und prüft, soll an dieser Stelle nicht näher beschrieben werden. Sie soll als Black-Box betrachtet werden, die auf Anforderung Authentikationsnachrichten erzeugt und verarbeitet und als Ergebnis ausgibt, ob die Authentikation erfolgreich verlief.

Die in Tabelle 6.1 angegebenen Längen von Nachrichtenparametern sind als Richtwerte gedacht und sollen als Ausgangspunkt für die Bewertung der Integrationsfähigkeit des Authentikationsprotokolles in die bestehende ISDN-Teilnehmersignalisierung dienen.

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 6.1: Längenkodierung der Nachrichtenelemente des Protokolles

Aus dieser Kodierung folgt, daß die Nachrichtenlängen kleiner als 1536 Bits (= 192 Oktetts) sind. Auch eine ergänzende Typ-Information der Parameter ist noch integrierbar und erhöht die Robustheit der Implementierung gegen den in Abschnitt 6.4 dargestellten Angriffstyp. Eine RSA-Signatur [Schn_96] 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 angegebenen 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 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.

1 Das öffentliche RSA-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 auf dieser Basis aus [Schn_96], S. 162, Tab. 7.6 abgeleitet.

Implementierung der Zwischenschicht Die in Abb. 6.7 dargestellte Zwischenschicht (ZS) muß die Nachrichten zur Authentikationssteuerung in die herkömmlichen Verbindungsaufbaunachrichten integrieren beziehungsweise durch Nutzung verfügbarer Zusatznachrichten die Authentikationsinformationen zwischen Endgerät und Vermittlungsstelle übertragen. Wir verwenden zur Implementierung das Facility-Informationselement (FAC), welches im Euro-ISDN zur Übertragung von Steuerinformationen für Dienstmerkmale in Verbindungsaufbaunachrichten integriert werden kann. Zusätzlich steht eine Facility-Nachricht zur Verfügung, welche dann zur Übertragung entsprechender Informationen genutzt wird, wenn keine anderen Verbindungssteuerungsnachrichten auszutauschen sind.[1]

Bei den in die bestehende Teilnehmersignalisierung im ISDN zu integrierenden Authentisierungsnachrichten wird eine Länge von 1536 Bits angenommen (s.o.). Zur effizienten Signaturprüfung beim Empfänger ist es sinnvoll, die Identität des Signaturerzeugers unverschlüsselt voranzustellen, damit der entsprechende Prüfschlüssel identifiziert werden kann.

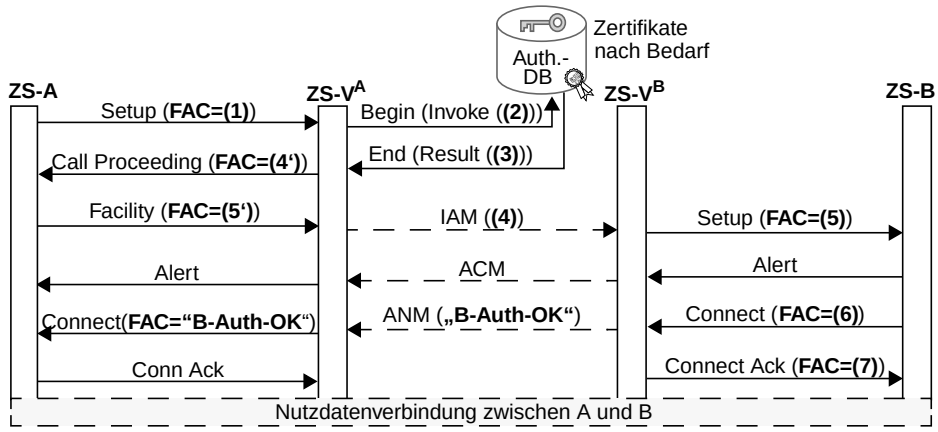


Abbildung 6.9: Integration der Nachrichten in die Verbindungssignalisierung im (N-) ISDN

Abb. 6.9 zeigt die Signalisierung für einen erfolgreichen Verbindungsaufbau im ISDN [BaGo_95, Q9xx_89]. Die beim Verbindungsaufbau ausgetauschten Signale werden durch die Zwischenschicht um die Authentisierungs-Nachrichten

1 Sollte das Facility-Informationselement implementierungsbedingt nicht in eine der genannten Signalisiernachrichten eingefügt werden können, so ist an der entsprechenden Stelle eine ergänzende Facility-Signalisiernachricht zu verwenden. Grundsätzlich sollte jede Nachricht (mit Ausnahme der NOTIFY-Nachricht) dieses Protokollelement aufnehmen können [BaGo_95, S. 67].

aus Abb. 6.8 erweitert. Die Integration des Nachrichtenaustausches erfordert nur eine zusätzliche Facility-Nachricht zur Übertragung der Nachricht (5‘) aus Abb. 6.8. Die weiteren Authentisierungsnachrichten können in reguläre Signalisiernachrichten des Verbindungsaufbaus integriert werden.

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 zugelassen – die geprüfte Identität von A angezeigt werden (Forderung c.).

Um das Verfahren möglichst wirtschaftlich integrieren zu können, ist es notwendig, daß die zusätzliche Funktionalität für die bestehende Verbindungsbehandlung und die Signalisierprotokolle an der Teilnehmerschnittstelle transparent bleibt. Die Zwischenschicht wird transparent oberhalb der D-Kanal-Protokolle eingefügt und durch die Verbindungsbehandlung wie bisher die Schicht 3 angesprochen. Für Nutzdaten-Anwendungen im Endgerät ist die zusätzliche Sicherungsfunktion nur indirekt erkennbar, wenn eine Verbindungsaufbauanforderung aufgrund einer erfolglosen Authentikation nicht zustandekommt oder Seiteneffekte auftreten, die aus der Verschlüsselung der Nutzdaten resultieren können[1].

Abb. 6.10 beschreibt das Verhalten der Zwischenschicht bei erweitertem Verbindungsaufbau. Das Bild beschreibt die verschiedenen Funktionsblöcke im Endgerät des rufenden Teilnehmers, welche mit der Zwischenschicht direkt in Beziehung stehen und die Dienstprimitive, welche zwischen diesen Funktionsblöcken im erfolgreichen und nicht erfolgreichen Fall ausgetauscht werden.

Die Implementierung der Zwischenschicht synchronisiert die Protokolle zum Verbindungsaufbau und zur Authentisierung. Sie integriert zu sendende Nachrichten der Verbindungsbehandlung (VB) und der Authentikationssteuerung (AS) und verteilt empfangene Nachrichten. Die Zwischenschicht parametrisiert und aktiviert beziehungsweise deaktiviert die Zusatzfunktionen *Authentikation* und *Verschlüsselung* und ermöglicht somit eine bedarfsorientierte Aktivierung der Sicherheitsfunktionen.

1 Eine Verschlüsselung kann i.a. eine Verzögerung einführen und verlangt eine Synchronisierung der Ver- und Entschlüsselungsfunktionen.

Die Zwischenschicht stößt bei Bedarf die Authentikationssteuerung durch das *Auth-Req-Primitiv* an und bricht den Verbindungsaufbau geordnet ab, falls eine Authentikation erfolglos verläuft. Verläuft die Authentikation nicht erfolgreich, dann veranlaßt die Zwischenschicht durch ein *Disc-Req-Primitiv* das Senden einer Disconnect-Nachricht durch die Schicht 3 und weist so den Verbindungswunsch ab. Dieses wird der Verbindungssteuerung durch das *Disc-Ind*-Primitiv angezeigt. Abb. 6.10b zeigt dies für den Fall, daß sich der B-Teilnehmer nicht erfolgreich authentisieren konnte, was dem A-Teilnehmer durch *B-Auth-NOK* angezeigt wird.

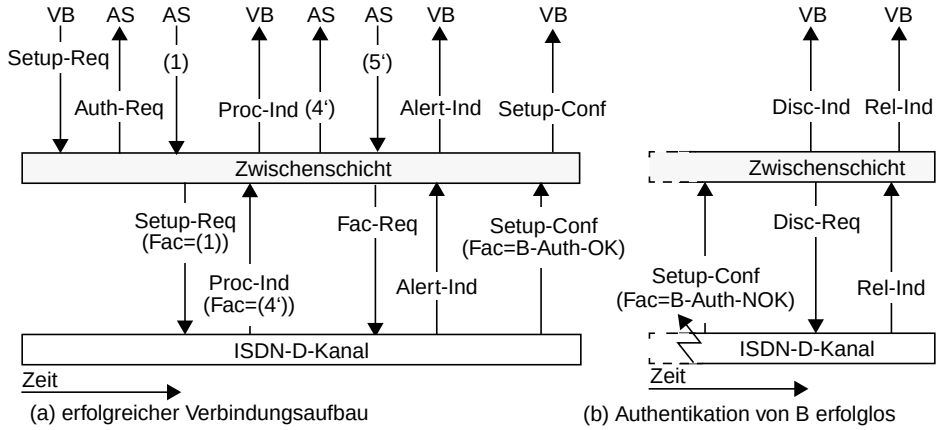


Abbildung 6.10: Primitive der Zwischenschicht im Endgerät (rufende Seite) vgl. Abb. 6.7

Weitere Funktionen zur Information des Teilnehmers über ein Display sind denkbar. Nach einem erfolgreichen Verbindungsaufbau mit Authentikation muß die Zwischenschicht oder die Authentikationssteuerung den ausgehandelten Sitzungsschlüssel zur Verschlüsselungsfunktion weiterleiten. Der Verbindungsabbau wird hier nicht näher beschrieben, doch auch er muß geordnet implementiert werden[1].

Beschaffung zertifizierter Prüfschlüssel Zur Abfrage gültiger Zertifikate der öffentlichen Schlüssel durch das Netz wird das Transaction Capability Application Service Element (TCAP-ASE) verwendet, welches im Zwischenamtsbereich

1 Alle Signalisiermeldungen sollten nach erfolgter Authentikation signiert oder mit einem Authentikations-Code versehen werden, um das Einspielen falscher Nachrichten oder das Manipulieren von Steuerinformation z.B. zur Übernahme einer bestehenden Verbindung zu erschweren oder auszuschließen.

für die verbindungsunabhängige Signalisierung zur Verfügung steht[1]. Da die Signalisierung eine gesicherte Übertragung bietet (bezüglich Verlust von Nachrichten und Übertragungsfehlern) und die Zertifikate sowieso signiert sind, wird diese Anfrage bei der Vertrauensinstanz nicht zusätzlich gesichert. Die Teilnehmer können die Zertifikate der Dienstanbieter bei Bedarf z.B. über ein Dienstmerkmal anfordern.

Verschlüsselung von Nutzdaten Eine Möglichkeit zur Plazierung der Verschlüsselungsfunktion am ISDN-Teilnehmeranschluß ist in [SaFe_97] dargestellt. Hier sind vielfältige Lösungen denkbar, auf die an dieser Stelle nicht näher eingegangen werden kann. Das ausgewählte Verfahren muß in Endgerät und Vermittlungsstelle kompatibel realisiert sein und sollte eine Aushandlung der verwendeten Algorithmen und Schlüssellängen für unterschiedliche Randbedingungen oder erhöhte Anforderungen erlauben (z.B. Triple-DES, [Schn_96]). Die Installation und der Wechsel des Sitzungsschlüssels erfolgt durch die Zwischenschicht oder die Authentikationssteuerung automatisch.

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 Abb. 6.9 frühestens mit der Connect-Nachricht übertragen werden kann. Damit ist die Identität des B-Teilnehmer gegenüber dem Dienstanbieter nachgewiesen; das Ergebnis kann also innerhalb der Connect-Nachricht zum A-Teilnehmer übermittelt werden.

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. Die Ausrüstung zertifizierter öffentlicher Endgeräte könnte mit der hier vorgeschlagenen Erweiterung die sichere Zuordnung der Gebühren zum jeweiligen Nutzer (bzw. Inhaber der Kryptokarte) ermöglichen und damit die bargeldlose Nutzung und einheitliche Abrechnung über das dem Nutzer zugeordnete Fernmeldekonto ermöglichen.

---

1 Im GSM wird auf diese Weise vor dem Verbindungsaufbau der Aufenthaltsort des gerufenen Mobilteilnehmers ermittelt, um eine gezielte Ausstrahlung des Verbindungswunsches zu ermöglichen.

Es ist unter Zuhilfenahme dieser ergänzenden Funktionen eine nutzer- und dienstanbieter-orientierte Inanspruchnahme von Diensten möglich. Es wird Teilnehmermobilität dadurch unterstützt, daß ein Teilnehmer von einem beliebigen Anschluß aus Dienste nutzen kann, die sein persönliches Gebührenkonto belasten. Zusätzlich ist dem Teilnehmer die Identität des jeweils erreichten Dienstanbieters bekannt. Der Betrieb mitgeführter (bzw. vertrauenswürdig zertifizierter) Endgeräte wird in unvertrauter Umgebung möglich, da vor der Dienstnutzung der Dienstanbieter identifiziert wird und die übertragenen Nutzdaten kryptographisch gesichert werden. Entsprechend können auch zertifizierte Endgeräte an öffentlichen Anschlüssen genutzt werden.

Die Identifikation des Dienstnutzers – in Erweiterung der gegenwärtig durchgeführten Identifikation des genutzten Anschlusses – wird insbesondere im Hinblick auf die flexible Konfigurierbarkeit und Nutzung netzübergreifender Dienste des Intelligenten Netzes an Bedeutung gewinnen.

Aufgrund rechtlicher Anforderungen an den Netzbetreiber sind die im Netz übertragenen Informationen mit diesem Verfahren nicht gegen Zugriffe in- und ausländischer staatlicher Dienste geschützt. Deshalb sind gegebenenfalls ergänzende Sicherungsfunktionen innerhalb der Endgeräte vorzusehen.

6.6 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 zu 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 ist hier vor allem die Zertifizierung zu nennen [Rann_95], der im Rahmen der Zuverlässigkeit und der unabhängigen Kontrolle als Basis für die Vertrauenswürdigkeit von Technik eine zentrale Rolle zukommt. Die Implementierung von Verzeichnisdiensten für öffentliche Prüfschlüssel kann im Intelligenten Netz durch zertifizierte Dienste – basierend auf zertifizierten Plattformen – von unabhängigen Netzbetreibern oder Dienstanbietern realisiert werden [HaSc_95].

Das vorgestellte Authentikationsprotokoll zur ergänzenden Sicherung der Teilnehmer-Netz-Schnittstelle wurde hinsichtlich seiner 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, werden zur Zeit im Rahmen einer Simulation untersucht.

Die Vorteile einer Auslagerung der gesamten netzseitigen Authentikation und damit zusammenhängender Netzfunktionen in Vertrauensinstanzen wird an unserem Institut im Zusammenhang mit den neuen Möglichkeiten, welche das Intelligente Netz bieten wird, und im Hinblick auf netzübergreifende Dienste nach der Öffnung des Telekommunikationsmarktes untersucht.

Literatur

AbNe_94 M. Abadi, R. Needham: „Prudent Engineering Practice for Cryptographic Protocols“, Digital, Systems Research Center, Research Report No. 125, Palo Alto, California, June 1994

AnMi_90 C. I'Anson, C. Mitchell: „Security Defects in CCITT Recommendation X.509 - The Directory Authentication Framework“, ACM Computer Communication Review, Vol. 20, 2 / 1990, pp. 30-34

ArLu_93 G. Arndt, R. Lueder: „Bewegungsfreiheit in allen Netzen“, Siemens telcom report 16, 2 / 93

AbNe_94 M. Abadi, R. Needham: „Prudent Engineering Practice for Cryptographic Protocols“, Digital, Systems Research Center, Research Report No. 125, Palo Alto, California, June 1994

BaGo_95 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

BeSc_95 A. Beutelspacher, J. Schwenk, K. - D. Wolfenstetter: „Moderne Verfahren der Kryptographie“, Vieweg, 1995

BlDi_96 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, 1 / 1996

DiHe_76 W. Diffie, M. E. Hellman: „New Directions in Cryptography“, IEEE Transactions On Information Theory, Volume 22, No. 6, November 1976, pp. 644-654

HaSc_95 V. Hammer (Hrsg.), M. J. Schneider, A. Roßnagel, J. Bizer, C. Kumbruck, U. Pordesch: „Sicherheitsinfrastrukturen - Gestaltungsvorschläge für Technik, Organisation und Recht“, Springer 95

KeSc_92 A. Kehne, J. Schönwälder, H. Langendörfer: „A Nonce-Based Protocol For Multiple Authentication“, ACM Operating Systems Review, Vol. 26, No. 4 1992, pp. 84-89

Koen_91 H.-P. Königs: „Cryptographic Identification Methods for Smart Cards in the Process of Standardization“, IEEE Communications Magazine, June 1991, pp. 42-48

Lang_96 H. Langendörfer: „Authentifizierter Nachrichtenaustausch ohne Verschlüsselung“, Praxis der Informationsverarbeitung und Kommunikation (PIK), 1996, Heft 3, pp. 156

LaPo_96 W. Langenheder, U. Pordesch: „Sicherheit und Vertrauen in der Kommunikationstechnik - Soziologische Ansätze und Methoden“, it+ti Informationstechnik und Technische Informatik, Schwerpunktheft 4, 1996

MaPo_96 T. Magedanz, R. Popescu-Zeletin: „Intelligent Networks - Basic Technology, Standards and Evolution“, International Thomson Computer Press, 1996

Mill_94 B. Miller: „Vital signs of identity“, IEEE Spectrum, February 1994, pp. 22-30

Moor_88 J. H. Moore: „Protocol Failures in Cryptosystems“, Proc. IEEE, Vol. 76, 5 / 1988, pp. 594-602

NeSt_93 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

PfPf_95 A. Pfitzmann, B. Pfitzmann, M. Schunter, M. Waidner: „Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule“, Proc. Verläßliche Informationssysteme (VIS‘ 95), Vieweg, 1995

Pohl_95 N. Pohlmann: „Schutz von LANs und LAN-Kopplung über öffentliche Netze“, DATACOM, 6, 1995, pp. 50ff

Q9xx_89 ITU-T: „Digital Subscriber Signalling System No. 1, Network Layer, User-Network Management“, ITU-T Recommendations Q.930-Q.940, Geneva, 1989

Rann_95 K. Rannenberg: „Evaluationskriterien zur IT-Sicherheit - Entwicklungen und Perspektiven in der Normung und außerhalb“, Verläßliche IT-Systeme, GI-Fachtagung, Vieweg, April 1995

RiSh_78 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

RiSh_84 R. L. Rivest, A. Shamir: „How to Expose an Eavesdropper“, Comm. ACM, Vol. 27, No. 4, 1984, pp. 393-398

RiSo_96 B. Richter, M. Sobirey, H. König: „Auditbasierte Netzüberwachung“, PIK, 1/1996, pp. 24-32

RoWe_90 A. Roßnagel, P. Wedde, V. Hammer, U. Pordesch: „Die Verletzlichkeit der Informationsgesellschaft“, 2. Auflage, Westdeutscher Verlag GmbH, Opladen, 1990

RuRa_83 R. Rushby, B. Randell: „A Distributed Secure System“, IEEE Computer, 7/1983, pp. 55-67

SaFe_97 R. Sailer, H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann: „Allokation von Sicherheitsfunktionen in Telekommunikationsnetzen“, in diesem Buch

SaKa_97 R. Sailer, M. Kabatnik, Internes Arbeitspapier, Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart, 1997

SaKu_96 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

SaSa_94 R. Sandhu, P. Samarati: „Access Control: Principles and Practice“, IEEE Comm. Magazine, 9/1994, pp. 40ff

Schn_96 B. Schneier: „Applied Cryptography“, 2nd ed., John Wiley & Sons, Inc., 1996

Shat_84 J. Shattuck: „Computer Matching Is A Serious Threat to Individual Rights“, Comm. ACM, Vol. 27, No. 6, June, 1984, pp. 538-541

Syve_93 P. Syverson: „On Key Distribution Protocols for Repeated Authentication“, ACM Operating Systems Review, Vol. 27, No. 4 1993, pp. 24-30

Tsud_92 G. Tsudik: „Message Authentication with One-Way Hash Functions“, ACM Computer Communication Review, Vol. 22, No. 5, October, 1992, pp. 29-38

Warw_96 M. Warwick: „Feeling Insecure?“, Communications International, 1 / 1996, pp. 37

WoLa_94 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

X509_93 ITU-T: „Data Networks And Open System Communications, Directory, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework“, ITU-T Recommendation X.509, 1993