K.G. Saur Verlag, München, 1999

S. Gold, D. Keck, P.J. Kühn und G. Müller

Sichere Telekommunikationsdienste mit Intelligenten Netzen

Dr. *Sönke S. Gold* ist Diplom-Informatiker und Betriebswirt (WAH). Seit 1995 ist er wissenschaftlicher Mitarbeiter der Abteilung Telematik des Institutes für Informatik und Gesellschaft (IIG) an der Universität Freiburg. Seine Forschungsschwerpunkte sind Sicherheit in der Informations- und Kommunikationstechnik, Intelligente Netze und Mobilkommunikation.

Dirk O. Keck hat 1994 von der Universität Stuttgart das Diplom in Elektrotechnik erhalten. Bis 1995 war er wissenschaftlicher Mitarbeiter am Institut für Mikroelektronik Stuttgart (Prof. B. Höfflinger). Anschließend ging er als wissenschaftlicher Mitarbeiter ans Institut für Nachrichtenvermittlung und Datenverarbeitung an der Universität Stuttgart, wo er heute tätig ist. Seine Interessengebiete sind private und öffentliche Kommunikationsnetze (ISDN, IN) und die Anwendung formaler Techniken beim Entwurf von Telekommunikationssystemen. D. Keck ist Mitglied der ITG.

Prof. Dr.-Ing. *Paul J. Kühn* studierte Elektrotechnik von 1962 bis 1967 und promovierte 1972 zum Dr.-Ing. an der Universität Stuttgart. Nach Leitung einer Informatik-Forschungsgruppe und einer Industrietätigkeit bei den Bell Laboratorien in den USA nahm er 1978 einen Ruf für Nachrichtenvermittlung an die Universität Siegen und 1981 einen Ruf auf den Lehrstuhl für Nachrichtenvermittlung und Datenverarbeitung an die Universität Stuttgart an, der mit der Leitung des gleichnamigen Instituts verbunden ist. Seine Lehr- und Forschungsgebiete sind die Technische Informatik, Kommunikationsnetze und Nachrichtenverkehrstheorie. Seit 1991 leitet Prof. Kühn das Int. Advisory Council des Int. Teletraffic Congress (ITC). Er ist Mitglied der Heidelberger Akademie der Wissenschaften und der Leopoldina Halle und Professor Associé der Ecole Nationale Superieur de Telecommunications (ENST), Paris. 1996 wurde ihm vom Lund Institute of Technology die Ehrendoktorwürde für Verdienste auf dem Gebiet der Telekommunikation verliehen, 1998 erhielt er den Grad des Dr.-Ing. E.h. von der Technischen Universität Dresden. Prof. Kühn ist Mitinitiator des DFG-Schwerpunktprogramms „Sicherheit in der Informations- und Kommunikationstechnik".

Prof. Dr. *Günter Müller* wurde 1976 an der Universität Duisburg promoviert und erhielt 1983 an der Wirtschafts-Universität Wien die venia legendi in Informatik. Nach zwei Jahren bei IBM Almaden Research/USA war er von 1978 bis 1990 bei IBM Deutschland, wo seine Arbeiten zu offenen Systemen 1985 zur Gründung des Europäischen Netzwerkzentrums führten, dessen Direktor er bis zu seinem Ruf an die Universität Freiburg war. Als Gründungsdirektor des Institutes für Informatik und Gesellschaft und als Ordinarius für Telematik beschäftigt er sich mit IT-Sicherheit, Electronic Commerce, virtuellen Unternehmen und autonomen Agenten. Er ist Sprecher des DFG-Schwerpunktprogramms „Sicherheit in der Informations- und Kommunikationstechnik".

ZUSAMMENFASSUNG

Das Konzept von Intelligenten Netzen (IN) wurde entwickelt, um in Telekommunikationsnetzen eine schnelle und effiziente Entwicklung und Einführung neuartiger Mehrwertdienste zu ermöglichen. Dienste wie Universal Personal Telecommunications (UPT) oder Electronic Commerce-Anwendungen verändern die Sicherheitsanforderungen aller beteiligten Parteien an Kommunikationssysteme. Die Umsetzung dieser Anforderungen erfolgt durch den Einsatz geeigneter Schutzmechanismen.

In diesem Beitrag wird untersucht, inwieweit sich Schutzmechanismen mit Intelligenten Netzen realisieren lassen. Dabei werden zusätzliche Anforderungen identifiziert, die im bisherigen Standardisierungsprozeß (CS-1 und CS-2) nicht berücksichtigt wurden. Es zeigt sich nämlich, daß fast alle Schutzmechanismen die Ausführung einzelner Funktionalitäten in Endgeräten oder in vertrauenswürdigen Netzknoten benötigen. Eine IN-basierte Realisierung zukünftiger Dienste mit ausreichenden Sicherheitseigenschaften ist daher nicht möglich.

Zukünftige Standardisierungsbemühungen sollten die Erweiterung der IN-Recommendations auch auf Endgeräte und andere Knoten außerhalb des eigentlichen Telekommunikationsnetzes miteinschließen. Ein Lösungsansatz wird im letzten Abschnitt skizziert.

1 EINFÜHRUNG

Immer mehr Kommunikationsprozesse aus dem privaten, öffentlichen und geschäftlichen Bereich werden durch Telematiksysteme abgewickelt bzw. unterstützt. Die Nachfrage nach im-

mer neuen, komplexen Kommunikationsdiensten und -anwendungen steigt insbesondere in folgenden Bereichen:

– *Mobilkommunikation:* Im Telekommunikationsmarkt werden vermehrt universelle persönliche Kommunikationsdienste nachgefragt [20, 23, 30]. Dienstzugang soll auch über Netz- und Betreibergrenzen hinaus möglich sein (Interworking). Um einen einheitlichen Zugang auch in unterschiedlichen Netztypen zu ermöglichen, bedarf es der nahtlosen Integration unterschiedlicher Systeme wie Festnetze, drahtloser Systeme und Mobilfunknetze sowie einer uniformen Dienstepräsentation und -nutzung unabhängig von Zugangsmedium, Netztyp, Dienstenerbringung und Umgebung [21, 2, 6].

– *Elektronischer Handel (Electronic Commerce):* Eine rasch zunehmende Zahl von Unternehmen ist heute damit befaßt, das Potential von Telekommunikationsnetzen für ihre Geschäftszwecke zu erschließen. Zur Abwicklung kommerzieller Aktivitäten bedarf es u.a. Verfahren für sicheren Werteaustausch (z.B. Geldtransaktionen) und verbindliche Kommunikation.

Diese neuen Dienste und Anwendungen verändern die Sicherheitsbedürfnisse von Netzbetreibern, Dienstanbietern und Anwendern. So erfordern persönliche mobile Kommunikationsdienste wie UPT im verstärkten Maße die Speicherung personenbezogener Daten, die die Erstellung von Nutzungs- und Bewegungsprofilen ermöglichen [30]. Im wirtschaftlichen Kontext setzt die universelle Nutzung der elektronischen Kommunikationsmedien, bei der Unternehmen Konstruktions-, Kunden- oder Produktionsdaten austauschen und Geldtransaktionen vornehmen, oder Privatleute Güter und Informationen Über das Netz bestellen und bezahlen, das Vertrauen aller Teilnehmer, insbesondere auch der Kommunikationspartner, in die Sicherheit der verwendeten Technik voraus. Sicherheit wird daher zu einem wichtigen Qualitätsmerkmal von Kommunikationsdiensten, das mitausschlaggebend für deren Akzeptanz und Nutzung ist.

Eine Infrastruktur, mit der Mehrwertdienste architekturübergreifend und rationell realisiert werden können, sind die im nächsten Abschnitt vorgestellten Intelligenten Netze (IN). Anschließend stellen wir das Konzept der mehrseitigen Sicherheit vor, das die Sicherheitsanforderungen neuartiger Telekommunikationsdienste beschreibt. Wir werden zeigen, daß bisher bekannte Schutzmechanismen zu deren Durchsetzung bisher nicht IN-unterstützt realisiert werden können. Wir schlagen daher am Ende dieses Aufsatzes eine Erweiterung der funktionalen und physikalischen IN-Architektur vor.

2 INTELLIGENTE NETZE

Der Begriff *Intelligentes Netz* (IN) [17, 20, 11] bezeichnet keine neue Technik oder Netzarchitektur, die vorhandene ablösen wird. Vielmehr handelt es sich um ein Konzept zur Ergänzung beliebiger Netze mit einheitlichen und dienstunabhängigen funktionalen Eigenschaften. Mehrwertdienste, die auf diesen Funktionen aufbauend implementiert wurden, sind dann grundsätzlich auch auf andere Architekturen übertragbar, sofern diese die IN-Funktionalitäten bereitstellen. Weiterentwicklung und Standardisierung von IN erfolgt bei der ITU in mehreren Stufen, den sogenannten Capability Sets (CS). Derzeit sind das CS-1 und das CS-2 standardisiert. IN werden schon seit einigen Jahren international von den Netzbetreibern in deren Netzen aufgebaut.

Die ITU-T beschreibt in ihrer Q.12xy-Serie die Funktionen des IN aus unterschiedlichen, abstrakten Sichten. Dienstesicht (Service Plane, SP) und globale Funktionssicht (Global Functional Plane, GFP) betrachten das IN als komplexe funktionale Einheit. Die Dienstesicht betrachtet das Verhalten von Diensten und Dienstmerkmalen, etwa aus der Sicht des Nutzers. Die globale Funktionssicht beschreibt globale, dienstunabhängige funktionale Bausteine (Service Independent Building Blocks, SIBs), durch deren Verkettung sich das Verhalten von Diensten beschreiben läßt.

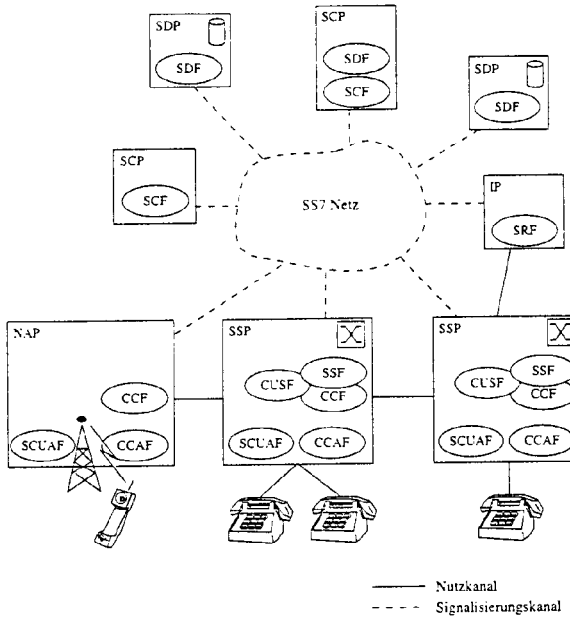

Abb. 1 Typisches IN-Szenario (physikalische Sicht)

CCAF	*Call Control Agent Function*
CCF	*Call Control Function*
CUSF	*Call Unrelated Service Function*
IP	*Intelligent Peripheral*
SCF	*Service Control Function*
SCP	*Service Control Point*
SDF	*Service Data Function*
SDP	*Service Data Point*
SRF	*Specialized Resource Function*
SSF	*Service Switching Function*
SSP	*Service Switching Point*

Die verteilte Funktionssicht (Distributed Functional Plane, DFP) zeigt die Funktionsverteilung innerhalb der IN-Architektur. Dienste werden durch miteinander kooperierende funktionale Einheiten (Functional Entities, FE) realisiert. Die physikalische Sicht (Physical Plane, PP) beschreibt unterschiedliche Allokationsszenarien dieser FEs in den Netzknoten bzw. physikalischen Einheiten (Physical Entity, PE). Ein mögliches IN-Szenario wird in Abb. 1 beschrieben. Die Endgeräte der Teilnehmer werden über einen Network Access Point (NAP) oder einen Service Switching Point (SSP) angeschlossen, in denen eine Call Control Agent Function (CCAF) die Interaktion mit dem Endgerät übernimmt.

Die Grundidee ist es, die Steuerung der Dienstausführung an wenigen Stellen zu zentralisieren. Dadurch ist es nicht mehr erforderlich, die zur Ausführung notwendigen Funktionen in allen Vermittlungsstellen zu implementieren. Die einen IN-Dienst steuernde Dienstelogik (Service Logic) und erforderliche Daten müssen nur noch an wenigen zentralen Stellen eingebracht werden. Der Aufruf eines IN-Dienstes wird von einer Call Control Function (CCF), typischerweise in einem Service Switching

Point (SSP), erkannt. Daraufhin wird dort die Rufbearbeitung unterbrochen, um ein Dienstelogikprogramm einer Service Control Function (SCF), beispielsweise in einem Service Control Point (SCP) aufzurufen, welche entscheidet, wie mit diesem Dienst weiter zu verfahren ist. Alle dazu benötigten Daten, auch teilnehmerbezogene, werden von Service Data Functions (SDF) zur Verfügung gestellt.

Beispiele für von CS-1 unterstützte Dienste sind die Umsetzung von Rufnummern, alternative Abrechnungsdienste oder auch die Filterung von ein- und ausgehenden Rufen [20]. Zusätzliche, für das CS-2 geplante funktionale Einheiten sollen auch den Aufruf von Dienstlogikprogrammen erlauben, ohne daß dies im Bezug zu einer bestehenden oder aufzubauenden Nutzverbindung steht. Ein Beispiel hierfür ist die Unterstützung von Mobilitätsdiensten, bei denen die Aufenthaltsinformationen eines mobilen Teilnehmers, der nicht telefoniert, geändert werden müssen. Der Aufruf dieser Dienstelogiken erfolgt durch eine Call Unrelated Service Function (CUSF). Die Schnittstelle für die Interaktion mit dem Endgerät wird durch eine Service Control User Agent Function (SCUAF) bereitgestellt.

3 MEHRSEITIGE SICHERHEIT

Der Sicherheitsbegriff verändert sich mit dem technischen Fortschritt [24]. Im Bereich der Telekommunikationstechnik war der Sicherheitsbegriff noch vor 25 Jahren gleichbedeutend mit dem Verhindern von Übertragungsfehlern, die durch die Fehleranfälligkeit der verwendeten Übertragungstechnik oder die Unzuverlässigkeit der Übertragungswege verursacht waren. Die Vorsorge vor beabsichtigten Angriffen von Menschen oder Organisationen auf Kommunikationssysteme und insbesondere auf die gespeicherten und übertragenen Informationen führte zum Leitgedanken der mehrseitigen Sicherheit, d.h. zur Übertragung des Datenschutzgedankens auf die Kommunikationstechnik.

In offenen Kommunikationssystemen kann nicht davon ausgegangen werden, daß sich alle Parteien vollständig vertrauen. Vielmehr sind bei der Analyse der Sicherheit dieser Systeme neben externen Angreifern auch alle beteiligten Parteien als potentielle Angreifer zu betrachten [29]. Forschungsarbeiten zur *mehrseitigen Sicherheit* befassen sich daher mit den Sicherheitsanforderungen aller beteiligten Parteien (miteinander kommunizierende Teilnehmer, Dienstanbieter, Netzbetreiber, Gerätehersteller, usw.), den technischen Umsetzungen, dem regulativen Umfeld und den gesellschaftlichen und wirtschaftlichen Auswirkungen. Die Anforderungen mehrseitiger Sicherheit übernehmen wir aus Rannenberg et al. [28], die eine Untergliederung in vier Schutzziele vorschlagen:

- *Schutzziel Vertraulichkeit* (Confidentiality):
  - *c1* Nachrichteninhalte sollen vor allen Instanzen außer den Kommunikationspartnern vertraulich bleiben.
  - *c2* Kommunikationspartner sollen voreinander anonym bleiben können. Unbeteiligte sollen nicht in der Lage sein, sie zu beobachten.
  - *c3* Niemand soll den momentanen Ort eines Teilnehmers bzw. einer Mobilstation ohne dessen Einwilligung ermitteln können.
- *Schutzziel Integrität* (Integrity):
  - *i1* Fälschungen des Nachrichteninhaltes bzw. des Absenders sollen erkannt werden.
- *Schutzziel Zurechenbarkeit* (Accountability):
  - *a1* Der Empfänger soll gegenüber einem Dritten beweisen können, daß Instanz *x* die Nachricht *y* geschickt hat.
  - *a2* Der Absender soll das Absenden einer Nachricht mit korrektem Inhalt beweisen können, möglichst sogar den Empfang.
  - *a3* Niemand kann dem Netzbetreiber Entgelte für erbrachte Dienstleistungen vorenthalten – zumindest erhält der Dienstanbieter bei Inanspruchnahme entsprechende Beweismittel. Umgekehrt können nur für korrekt erbrachte Dienstleistungen Entgelte gefordert werden.
- *Schutzziel Verfügbarkeit* (Availability):
  - *v1* Das Netz ermöglicht Kommunikation zwischen allen Partnern, die dies wünschen und denen es nicht verboten ist.

Diese Ziele sind nicht konfliktfrei und müssen beim Entwurf von Systemen in eine sinnvolle und für alle Beteiligten akzeptable Balance gebracht werden [28]. Da die Anforderungen der Beteiligten individuell und situationsbedingt sehr stark differieren und sich mit der Zeit ändern, ist es kaum möglich, die Interessen aller Beteiligten ex ante zu analysieren, gegeneinander abzuwägen, und daraus ein starres, technisches Sicherheitskonzept zu formen. Einige Ansätze gehen daher davon aus, daß die Teilnehmer ihre Sicherheitsbedürfnisse in einem Aushandlungsprozeß formulieren und sich auf ein gemeinsames Sicherheitsniveau einigen. Damker et al. [7] zeigen mit ihrem Erreichbarkeitsmanager exemplarisch, wie ein solcher Aushandlungsprozeß aussehen kann.

4 BAUSTEINE FÜR SICHERE KOMMUNIKATIONSDIENSTE

Damit ein bestimmtes Sicherheitsniveau erreicht werden kann, muß die Technik Mechanismen bereitstellen, mit denen die Umsetzung der Sicherheitsanforderungen erreicht werden kann. Federrath und Pfitzmann [9] stellen Sicherheitsmechanismen vor, die als Bausteine für sichere Kommunikationsdienste dienen können:

- *Vertraulichkeit*
  - *c1* Ende-zu-Ende-Verschlüsselung mit symmetrischen oder asymmetrischen kryptographischen Verfahren verbirgt den Inhalt von Nachrichten vor anderen Parteien als den Kommunikationspartnern.
  - *c2* MIXe [26] ermöglichen unbeobachtbare Kommunikationsverbindungen. An alle Teilnehmer gesendeten Nachrichten (Broadcast) schützen den Empfänger, der als einziger die Nachricht entschlüsseln kann. DC-Netze [5, 27] schützen den Absender durch überlagertes Senden aller Teilnehmer.
  - *c3* Sensible Nutzerdaten wie z.B. Aufenthaltsinformationen können durch Pseudonymisierungsverfahren oder durch Speicherung in vertrauenswürdigen Netzknoten geschützt werden. Bandspreizverfahren [31] verhindern die Peilung von mobilen Stationen, werden hier jedoch nicht weiter betrachtet, da sie sich nur auf den Funkkanal zwischen Basis- und Mobilstation beziehen und nicht IN-typisch sind.
- *Integrität*
  - *i1* Mit Hilfe eines asymmetrischen oder symmetrischen kryptographischen Verfahrens wird der lesbaren Nachricht ein verschlüsselter Prüfteil (digitale Signatur) angehängt, der nur mit Wissen des gemeinsamen bzw. des privaten Absenderschlüssels einem veränderten Nachrichteninhalt angepaßt werden kann.
- *Zurechenbarkeit*
  - *a1* Digitale Signaturen sind mit asymmetrischen Kryptographieverfahren möglich.

a2 Der Empfänger muß den Empfang einer Nachricht mit einer digitalen Signatur bestätigen.

a3 Nutzer können in Anspruch genommene Dienste digital quittieren. Authentifizierungsverfahren sollen verhindern, daß Dritte die Identität eines Teilnehmers vortäuschen können, um auf dessen Kosten Dienste in Anspruch zu nehmen. Anonyme und unbeobachtbare Abrechnungsverfahren (z.B. digitales Bargeld) ermöglichen das Bezahlen von anonym in Anspruch genommenen Diensten.

- *Verfügbarkeit*

  v1 Verfahren zur Fehlertoleranz sichern den Betrieb auch bei Ausfall einzelner technischer Komponenten, werden hier jedoch nicht weiter betrachtet.

Die Allokation dieser Sicherheitsmechanismen entscheidet einerseits über deren Wirksamkeit, andererseits ist sie notwendige Voraussetzung für deren Akzeptanz [29]. Ebenso verhält es sich mit der Speicherung von anwenderbezogenen Daten. Aus Anwendersicht ist die grundsätzlich wirksamste Strategie zur Vermeidung von Risiken die möglichst weitgehende Vermeidung der Erhebung, Übertragung und Speicherung riskanter Daten (*Datensparsamkeit*) oder deren Verteilung auf mehrere Teile eines verteilten Systems (*Dezentralisierung*), um Möglichkeit und Folgen eines Mißbrauchs zu begrenzen [28, 30]. Sind Daten nicht vermeidbar, etwa weil sie zur ordnungsgemäßen Erbringung eines Dienstes unverzichtbar sind, sind Schutzmechanismen für die Sicherung der vorhandenen Daten erforderlich. Ansätze hierzu sind *Pseudonymisierungsverfahren* [9], die eine Verwaltung der Daten durch den Netzbetreiber zulassen, jedoch eine Zuordnung zur Identität des Teilnehmers verhindern bzw. erschweren, oder die Speicherung dieser Daten in *vertrauenswürdigen Instanzen*. Innerhalb des Netzes kann dies durch *Tamper Proof Environments* (TPEs) [32] geschehen, setzt jedoch die Entwicklung spezieller Hardware voraus und wird daher in naher Zukunft nicht möglich sein. Andere Konzepte wie der *Freiburger Kommunikationsassistent* (FKA) [25, 30] und der *Home Personal Computer* HPC [10, 9] lagern sensible Daten in vom Nutzer kontrollierte Endgeräte außerhalb des eigentlichen Netzes aus. Diese Ansätze wurden insbesondere zum Schutz der Aufenthaltsdaten in Mobilfunknetzen entwickelt. Aufenthaltsdaten werden erst dann dem Netz zur Verfügung gestellt, nachdem ein angehender Anruf vom der Heimatstation akzeptiert wurde. FKA und HPC erfordern im Gegensatz zum TPE keine neue (und noch nicht entwickelte) Hardware, so daß ihre Umsetzung in naher Zukunft realistischer ist.

Im nächsten Abschnitt werden wir untersuchen, inwieweit sich die vorgestellten Bausteine (Ende-zu-Ende-Verschlüsselung, digitale Signaturen, Authentifizierungsverfahren, Pseudonyme, anonyme und unbeobachtbare Zahlungssysteme, der Freiburger Kommunikationsassistent, MIXe, Broadcasting und DC-Netze) mit Hilfe von Intelligenten Netzen realisieren lassen.

5 IN IN VORGESEHENE SICHERHEITSMECHANISMEN

In den letzten Jahren sind bereits ein Reihe von Arbeiten über die Sicherheit in Intelligenten Netzen veröffentlicht worden. Die meisten beziehen sich jedoch auf die Sicherung der Kommunikation zwischen Netzkomponenten: In [18] werden Gefahren und Risiken bezüglich des Signalisiernetzes SS7 beschrieben und Lösungsmöglichkeiten diskutiert. Insbesondere beim Interworking, wenn Dienstzugang auch über die Grenzen des Heimatnetzes hinweg gewährt werden soll, treten die beteiligten Netzbetreiber auch als potentielle Konkurrenten auf. Für diese Szenarien wurde von Herrigel et al [13, 14, 15] eine Sicherheitsarchitektur entworfenen, um sensible Management- und Steuerdaten, die für die Ausführung von Diensten zwischen Netzknoten ausgetauscht werden müssen, zu schützen. Kernelemente dieses Ansatzes sind kryptographische Verfahren, Trusted Third Parties sowie Protokolle für den Austausch öffentlicher Schlüssel und für die Berechnung von Sitzungsschlüsseln. Netzknoten auch unterschiedlicher Hersteller können sich damit gegenseitig authentifizieren und übertragene Nachrichten durch Verschlüsselung schützen. Die hier beschriebenen Ansätze beziehen sich nur auf die Abläufe innerhalb des Netzes und haben aus der Sicht des Teilnehmers keinen direkten Einfluß auf die Sicherheitseigenschaften eines in Anspruch genommenen Dienstes.

Arbeiten, die direkten Einfluß auf für den Teilnehmer sichtbare Sicherheit haben, beziehen sich ausschließlich auf die Authentifizierung des Teilnehmers: Authentifizierung ist in den Empfehlungen der ITU-T als Dienstmerkmal geplant, beispielsweise als Zugangskontrolle für den UPT-Dienst. Mögliche IN-Realisierungen werden in [4, 12, 22] beschrieben. In [16] wird vorgeschlagen, die verteilte Funktionssicht um die funktionalen Einheiten *Calculator Function* (CalF) und *Service Authentication Function* (SAF) zu erweitern. CalF übernimmt dabei die kryptographischen Berechnungen zur Authentifizierung des Teilnehmers gegenüber der SAF.

Untersucht man die anderen Bausteine hinsichtlich ihrer Realisierbarkeit mit IN, so stellt man fest, daß alle Mechanismen, selbst Authentifizierung, die Allokation einzelner Funktionalitäten im Endgerät, einer SIM oder einem vertrauenswürdigen Netzknoten voraussetzen:

- *Ende-zu-Ende-Verschlüsselung:* Um Daten auf der gesamten Übertragungsstrecke zu schützen, müssen die kryptographischen Berechnungen in den Endgeräten oder in Chipkarten ausgeführt werden. Geheime bzw. private Schlüssel müssen in vertrauenswürdigen Netzknoten, in Terminals oder auf einer Chipkarte gespeichert werden.
- *Digitale Signaturen:* Um private Schlüssel vor dem Zugriff anderer Parteien zu schützen, müssen digitale Signaturen in einem Gerät berechnet werden, das durch den Anwender kontrolliert wird. Dies wird z.Zt. durch IN nicht unterstützt.
- *Authentifizierung:* Mechanismen zur Authentifizierung sind in den ITU-T Empfehlungen geplant und werden auch in entsprechenden Veröffentlichungen diskutiert (s.o.). Allerdings müssen funktionale Einheiten wie die Berechnung von kryptographischen Funktionen im Endgerät oder einer SIM allokiert sein, um die PIN oder eines möglicherweise benötigten privaten Schlüssels zu schützen. Diese Allokation wird nicht durch IN unterstützt.
- *Pseudonyme:* Pseudonymverfahren benötigen entweder einen vertrauenswürdigen Knoten, die bei eingehenden Anrufen die Teilnehmeridentität auf das aktuelle Pseudonym abbilden, oder sie arbeiten mit asymmetrischen kryptographischen Verfahren. Dies benötigt wiederum die Allokation von Funktionalitäten im Endgerät.
- *Anonyme und unbeobachtbare Zahlungssysteme:* Viele elektronische Zahlungssysteme verlangen die Allokation von Funktionen und Daten in vertrauenswürdiger Hardware [1].
- *FKA/HPC:* Die IN-Konzepte gehen von einer Speicherung von Daten, auch von teilnehmerbezogenen, in zentralen Datenbanken (SDF) aus. Eine Dezentralisierung durch Speicherung in externen, durch den Teilnehmer kontrollierten Knoten ist für IN nicht vorgesehen und wird auch nicht unterstützt.

- *MIXe:* MIXe sollen die Existenz einer bestehenden Kommunikationsbeziehung vor dritten Parteien, auch vor den Netzbetreibern, verschleiern. Aus diesem Grund müssen MIXe auf vertrauenswürdigen Knoten betrieben werden, auf die der Netzbetreiber keinen Zugriff hat.
- *Broadcasting und DC-Netze:* Zur Implementierung dieser Mechanismen müssen einige kryptographische Berechnungen in den Endgeräten ausgeführt werden.

Tab. 1 faßt diese Diskussion nochmals zusammen. Bisher wurden nur Authentifizierungsmechanismen für IN diskutiert und auch geplant. Damit ist neben *v1* bisher nur die Durchsetzung der Anforderung *a3* vorgesehen. Allerdings setzen alle Mechanismen die Allokation einzelner Funktionalitäten in Knoten außerhalb des eigentlichen Netzes voraus, so daß eine Realisierung mit den derzeitigen IN-Konzepten nicht möglich ist. Wichtige künftige Anwendungen wie beispielsweise Electronic Commerce, wo z.T. Mechanismen für verbindliche Verträge nötig sind, sind daher nicht IN-basiert realisierbar, da Anforderungen wie *a1* und *a2* nicht umgesetzt werden können.

Tab. 1 Sicherheitsmechanismen und ihre Allokation

	für IN vorgesehen	benötigt Allokation einzelner Funktionalitäten in	
		Endgerät/ SIM	vertrauenswürdigem Netzknoten
Ende-zu-Ende-Verschlüsselung		•	
digitale Signaturen		•	•
Authentifizierung	ja	•	
Pseudonyme		•	•
anonym. und unbeobachtb. Abrechnungsverfahren		•	•
FKA, HPC			•
MIXe			•
Broadcast		•	
DC-Netze		•	

6 ERWEITERUNG DER IN-ARCHITEKTUR

Im letzten Abschnitt wurde gezeigt, daß die Implementierung von Sicherheitsmechanismen die Allokation einzelner funktionaler Einheiten in Endgeräten oder Netzknoten außerhalb des eigentlichen Netzes benötigt. Diese Anforderung wird weder durch das CS-1 noch durch das CS-2 erfüllt, so daß eine auf IN basierende Implementierung der beschriebenen Schutzmechanismen mehrseitiger Sicherheit derzeit nicht möglich ist. Wir schlagen daher vor, die physikalische Sicht des konzeptionellen Modells um Endgeräte und vertrauenswürdige physikalische Einheiten (*Trustworthy Points, TPs*) zu erweitern, so daß funktionale Einheiten auch außerhalb des Zugriffs- und Kontrollbereiches der Netzbetreibers allokiert werden können. Abb. 2 zeigt eine mögliche Anordnung von funktionalen Einheiten in dieser erweiterten Architektur.

Die zusätzlichen externen physikalischen Einheiten müssen auch an das Signalisiernetz angeschlossen werden. Externen Dienstanbietern oder privaten Teilnehmern einen direkten Zugang zum SS7-Signalisiernetz zu gewähren, birgt potentielle Risiken für den Netzbetreiber. Angreifer könnten sich Zugang zu Daten von solchen Teilnehmern verschaffen, welche keinen TP betreiben wollen. Auch können unsachgemäß betriebene externe Komponenten die Verfügbarkeit des gesamten Systems beeinträchtigen. Direkter SS7-Zugang ist daher nur sehr restriktiv zu gewähren, Funktionalität und Verkehrsfluß an solchen Verbindungen sind daher einzuschränken [18]. Die Signalisierung zwischen TP und anderen IN-Komponenten sollte aus diesem Grund nicht über das Signalisiernetz, sondern über andere Wege, z.B. den ISDN-D-Kanal, abgewickelt werden.

Funktionale Einheiten (*Functional Entities*, FEs), die sensible Teilnehmerdaten speichern bzw. verarbeiten, können nun in der TP, in einem Endgerät oder in einer geeigneten Chipkarte angesiedelt werden. Ähnliches gilt für Daten, die aus Sicht des Betreibers kritisch sind (z.B. Abrechnungsdaten) und daher auch weiterhin innerhalb des eigentlichen Netzes abgelegt werden.

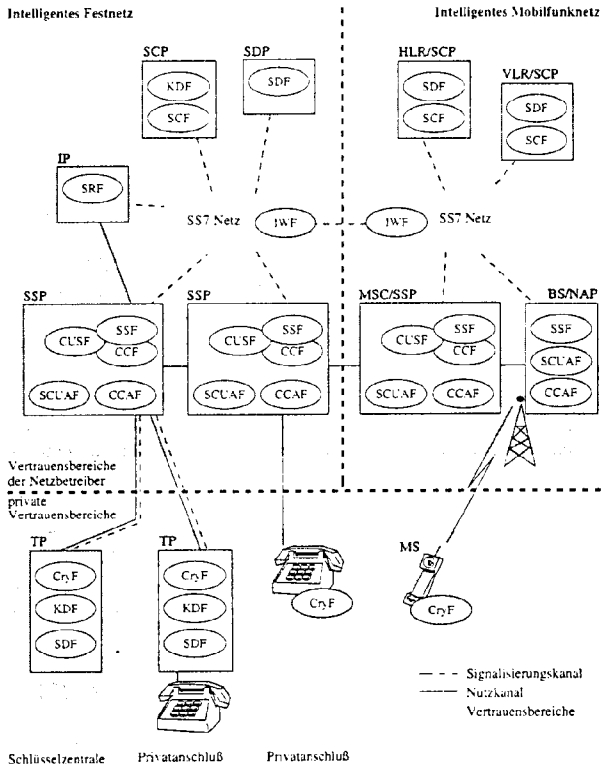

Abb. 2 Mehrseitig sicheres IN-Szenario

CCAF	*Call Control Agent Function*
CCF	*Call Control Function*
CryF	*Crypto Function*
CUSF	*Call Unrelated Service Function*
IP	*Intelligent Peripheral*
KDF	*Key Distribution Function*
SCF	*Service Control Function*
SCP	*Service Control Point*
SDF	*Service Data Function*
SDP	*Service Data Point*
SRF	*Specialized Resource Function*
SSF	*Service Switching Function*
SSP	*Service Switching Point*
TP	*Trustworthy Point*

Das Szenario in Abb. 2 zeigt eine mögliche Anordnung der FEs in die erweiterten physikalische Sicht. Zur Unterstützung von kryptographischen Berechnungen und des Einsatzes von Schlüsseln schlagen wir zwei zusätzliche FEs vor:

– Die meisten der beschriebenen Sicherheitsmechanismen setzen kryptographische Berechnungen wie das Verschlüsseln und Signieren von Nachrichten voraus. Diese sollen von der funktionalen Einheit *Cryptographic Funktion* (CryF) ausgeführt werden. Bei Verschlüsselung sollte jede FE in der gleichen physikalischen Einheit (Physical Entity, PE) angesiedelt sein wie

die ihr zugeordnete CryF, damit geheime Schlüssel oder PINs sowie zu verschlüsselnde oder zu signierende Nachrichten nicht ungeschützt übertragen werden.

– Für die praktische Verwendbarkeit von Verschlüsselungsverfahren wie digitalen Signaturen sind Einrichtungen zur Zertifizierung öffentlicher Schlüssel, sog. Zertifizierungsstellen (oft auch Trust Center genannt), notwendig [8], die sowohl vom Netzbetreibern als auch von Dritten betrieben werden können. Deren wichtigste Aufgabe ist die Bereitstellung von (öffentlichen) Schlüsseln, für deren Richtigkeit sie garantieren. Wir schlagen vor, daß die Protokolle zur Erzeugung und Verteilung durch spezielle *Key Distribution Functions* (KDF) abgewickelt werden. Eine CryF kann von einer KDF, die auch in der lokalen PE vorhanden sein kann, öffentliche Schlüssel von Kommunikationspartnern oder einen Sitzungsschlüsseln erfragen. Die befragte KDF holt öffentliche Schlüssel von der KDF einer Schlüsselzentrale ein und erzeugt Sitzungsschlüssel in Kooperation mit der KDF des Kommunikationspartners.

7 ZUSAMMENFASSUNG

Eine wesentliche Eigenschaft des IN-Ansatzes ist die Allokation von Dienstlogikprogrammen und Dienstdaten in zentralen Netzknoten. Sicherheitsmechanismen setzen jedoch die Speicherung von Daten und die Ausführung einzelner Funktionalitäten außerhalb des eigentlichen Netzes, beispielsweise im Endgerät, voraus. Dies bedeutet, daß unter Gewährleistung mehrseitiger Sicherheit kommende Dienste wie elektronischer Handel nicht auf der Basis des aktuellen IN-Konzeptes realisiert werden können.

Intelligente Netze wurden entwickelt und aufgebaut, um die Realisierung neuartiger Mehrwertdienste zu unterstützen. In dieser Arbeit haben wir Erweiterungen der IN-Konzepte vorgeschlagen, damit künftige Dienste im Rahmen dieser Architektur realisierbar bleiben. Ansonsten ist zu befürchten, daß IN sich auf simple Funktionen wie Rufnummernumsetzung beschränkt bleiben.

8 LITERATUR

[1] Asokan, N.; Janson, P.; Steiner, M.; Waidner, M.: Electronic Payment Systems, verfügbar unter *http://www.semper.org/*.

[2] Buitenwerf, E.; Colombo, G.; Mitts, H.; Wright, P.: UMTS: Fixed Network Issues and Design Options. IEEE Personal Communications, Bd. 2, Nr. 1, Februar. 1995, S. 30-37.

[3] Cambre, A.: Intelligente Netze: der Schlüssel für neue Dienste, in: Alcatel Telecom Rundschau, 1/96, S. 14-21.

[4] Campana, M.; Chauvaud, P.; Gilbert, H.: Security Architecture for the UPT Service, in: XV International Switching Symposium (ISS) 95, Bd. 1, S. 226-230.

[5] Chaum, D.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, in: Journal of Cryptology 1/ 1988, S. 65-75.

[6] Cheung, J.C.S.; Beach, M.A.; McGeehan, J.P.: Network Planning for Third-Generation Mobile Radio Systems, in: IEEE Communications Magazine, Bd. 32, Nr. 11, November 1994, S. 54-59.

[7] Damker, H.; Federrath, H.; Reichenbach, M.; Bertsch, A.: Persönliches Erreichbarkeitsmanagement, in: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn 1997.

[8] Federrath, H.; Jerichow, A.; Pfitzmann, A.; Pfitzmann, B.: Mehrseitig sichere Schüsselerzeugung, in: Horster, P. (Hrsg.): Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung. Vieweg, Braunschweig/Wiesbaden 1995, S. 117-131.

[9] Federrath, H.; Pfitzmann, A.: Bausteine zur Realisierung mehrseitiger Sicherheit, in: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn 1997.

[10] Federrath, H.; Jerichow, A.; Kesdogan, D.; Pfitzmann, A.; Spaniol, O.: Mobilkommunikation ohne Bewegungsprofile, in: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn 1997.

[11] Harju, J.; Karttunen, T.; Martikainen, O.: Introduction to Intelligent Networks, in: Harju, J.; Karttunen, T.; Martikainen, O. (Hrsg.): Intelligent Networks – Proceedings of the IFIP workshop on intelligent networks 1994, Chapman & Hall, London u.a. 1995, S. 1-33.

[12] Herrigel, A.; Rueppel, R.; Rerchichi, A.; Hubeaux, J.P.; Busch, K.; Huber, D.: The Integration of a Cryptographic Authentication Protocol in the IN Architecture, in: IEEE 95 IN-Workshop, 9.-11. Mai 1995, Ottawa.

[13] Herrigel, A.: A Security Architecture for the Core Part of CS-2, in: IEEE '96 IN Workshop, Melbourne, 21.-24. April 1996

[14] Herrigel, A.; Lai, X.: Interdomain Authentication for Co-operative IN Internetworking, in: IEEE IN '95 Workshop, Ottawa, 9.-11. Mai 1995.

[15] Herrigel, A.; Lai, X.: Secure IN Internetworking, in: IFIP TC6 Workshop on Intelligent Networks, Lappeenranta, Finnland, 8.-9. August 1994.

[16] Herrigel, A.; Lai, X.: Authentication and Authorization in the IN based on Symmetric and Asymmetric Techniques, in: 3rd International Conference on Intelligence in Networks (ICIN) 94, Bordeaux, 11.-13. Oktober 1994, S. 157-162.

[17] ITU-T: General Recommendations on Telephone Switching and Signalling – Intelligent Network – ITU-T Recommendations Q.12xx, Genf 1993 und 1995.

[18] Klüpfel, H.M.: Securing a Global Village and its Resources, in: IEEE Communications Magazine, September 1994, S. 82-89.

[19] Krusch, W.: Neue Dienste im intelligenten Telefonnetz, R.v. Decker's Verlag, Heidelberg 1993.

[20] Magedanz, T.; Popescu-Zeletin, R.: Intelligent Networks – Basic Technology, Standards and Evolution. International Thomson Computer Press, London u.a. 1996.

[21] MacFarlane, D.: Third Generation Mobile – UMTS and FPLMTS. Speaker's Papers, 7th World Telecommunications Forum, Technology Summit „Convergence of Technologies, Services and Applications" Bd. 2, ITU Telecom 95, 3.-11. Oktober 1995, International Telecommunication Union, 1995, S. 185-188.

[22] Maillot, D.; Spilling, P.: IN Service Security and Service Management Security and their Relationships – Using UPT as a Case Study, in: Kugler, H.-J.; Mullery, A.; Niebert, N. (Hrsg.): Towards a Pan-European Telecommunication Service Infrastructure – IS&N 94, Proceedings of Second International Conference on Intelligence in Broadband Services and Networks, Aachen, 7.-9. September 1994.

[23] Müller, G.; Kohl, U.; Schoder, D.: Unternehmenskommunikation: Telematiksysteme für vernetzte Unternehmen. Addison Wesley, Bonn 1997.

[24] Müller, G.; Pfitzmann, A.: Mehrseitig sichere Kommunikation – Vertrauen in Technik durch Technik, in: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn 1997.

[25] Müller, G.; Stoll, F.: Der Freiburger Kommunikationsassistent – Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation, in: PIK 19 (1996) 4, S. 189-197.

[26] Pfitzmann, A.: Technischer Datenschutz in öffentlichen Funknetzen, in: Datenschutz und Datensicherheit 8/93, S. 451-463.

[27] Pfitzmann, A.: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer, Berlin 1990.

[28] Rannenberg, K.; Pfitzmann, A.; Müller, G.: Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: it+ti (Informationstechnik und technische Informatik) 4/96, August 1996.

[29] Sailer, R.; Federrath, H.; Jerichow, A.; Kesdogan, D.; Pfitzmann, A.: Allokation von Sicherheitsfunktionen in Telekommunikationsnetzen, in: Müller, G.; Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn 1997.

[30] Stoll, F.: Dezentralisierung und Sicherheit in Mobilfunknetzen. Datakontext-Fachverlag, Frechen 1997.

[31] Thees, J.; Federrath, H.: Methoden zum Schutz von Verkehrsdaten in Funknetzen, in: Verläßliche IT-Systeme (VIS '95), Vieweg 1995, S. 181-192.

[32] Wilhelm, U.G.: Increasing Privacy in Mobile Communication Systems using Cryptographically Protected Objects, in: Verläßliche IT-Systeme (VIS) 1997, Vieweg 1997, S. 319-334.