[RARWoSt99] *Christoph Rensing, Ralf Ackermann, Utz Rödig, Lars Wolf, Ralf Steinmetz;* **Sicherheitsunterstützung für Internet Telefonie,** Sicherheitsinfrastrukturen'99, Hamburg, 09.-10.03.99

# Sicherheitsunterstützung für Internet Telefonie

Christoph Rensing[1], Ralf Ackermann[1], Utz Roedig[1], Lars Wolf[1], Ralf Steinmetz[1,2]

[1]Industrielle Prozeß- und Systemkommunikation
Fachbereich Elektrotechnik und Informationstechnik
Technische Universität Darmstadt
Merckstr. 25 • D-64283 Darmstadt
{Christoph.Rensing, Ralf.Ackermann, Utz.Roedig, Lars.Wolf, Ralf.Steinmetz}
@KOM.tu-darmstadt.de

[2]GMD IPSI
Forschungszentrum Informationstechnik GmbH
Dolivostr. 15 • D-64293 Darmstadt

## Zusammenfassung

IP-basierte Telefonie wird vielfach als ein neuer Schlüsseldienst für das Internet angesehen. Bei ihrer breiten und interoperierenden Nutzung ist neben der vorausgesagten Einsparung von Kosten eine Vielzahl von neuen, über die vorhandenen Angebote hinausgehenden Mehrwertdiensten realisierbar. Aktuell gibt es daher intensive Entwicklungs- und Standardisierungsbestrebungen zur Definition der zu nutzenden Architekturen, Dienste und Protokolle. Neben der Umsetzung der Basisfunktionen zum Audiodatentransfer, zur Teilnehmer-Identifizierung und -Lokalisierung sowie zur Signalisierung müssen, als Vorbedingung für eine allgemeine Akzeptanz und einen über den experimentellen oder in relativ abgeschlossenen Konfigurationen praktikablen Betrieb, diejenigen Sicherheitsmechanismen bereitgestellt werden, die in der heutigen Telekommunikationswelt selbstverständlich sind. Aus den neuen Ansätzen und Rahmenbedingungen resultieren jedoch auch neue Anforderungen, insbesondere ist aufgrund der nicht mehr festen Zuordnung eines Teilnehmers zu einem physischen Telefonanschluß die Entwicklung von einem "Trust-by-Wire" zu einem "Trust-by-Authentication" notwendig. Fragen der Sicherheit, die im Augenblick nur in begrenztem Umfang Aufmerksamkeit und Berücksichtigung finden, muß sinnvollerweise bereits bei der Entwicklung der für die Internet Telefonie zu realisierenden Protokolle und Mechanismen Rechnung getragen werden. Der Beitrag stellt ausgehend von einer Analyse typischer Anwendungsszenarien spezifische sicherheitsrelevante Anforderungen an Internet Telefonie Architekturen und Protokolle dar und diskutiert auf allgemeinen Sicherheitsmechanismen aufbauende Ergänzungen der vorliegenden Ansätze. Die vorgestellten Erweiterungsvorschläge bilden die Basis für die von den Autoren vorgesehenen Implementierungen und praktischen Untersuchungen.

# 1 Umfeld

Die Verschmelzung der Sprach- und Datenkommunikationsinfrastruktur ist heute ein allgemeiner Trend. So werden zunehmend klassische, in der Vergangenheit traditionell verbindungsorientierte Dienste unter Nutzung von paketvermittelten Datennetzen erbracht. Dafür gibt es zwei wesentliche Gründe. Durch eine bessere Ausnutzung der vorhandenen oder weiterzuentwickelnden Infrastruktur und die Möglichkeit, diese einheitlich zu betreiben und zu verwalten, lassen sich Kosten sparen. Zudem ist durch die Bereitstellung von neuartigen Mehrwertdiensten ein Zusatznutzen für die Anwender erzielbar. Dies gilt insbesondere für die, in der Regel als IP-Telefonie bezeichnete, paketbasierte Sprachkommunikation in Intranetzen oder dem Internet.

Internet Telefonie erlaubt, zum einen wegen der derzeit vorhandenen flachen Tarifstruktur im Internet, zum anderen aufgrund der möglichen gezielten Einflußnahme des Benutzers oder Netzbetreibers auf die Art der Codierung der Sprachdaten und deren aktivitätsabhängige Übertragung, eine unmittelbare Kosteneinsparung [Schulzrinne97]. Auch können IP-basierte Telefoniedienste sehr gut in andere computerbasierte Anwendungen integriert werden oder diese ergänzen. Neben der Erweiterung des Leistungsumfanges von Applikationen zum rechnergestützten kooperativen Arbeiten (CSCW) stellt gerade die gegenüber den Angeboten in heutigen leitungsvermittelten Netzen einfachere Realisierung von Multipoint-Audio- aber auch Videokonferenzen eine interessante und ökonomisch relevante Anwendung dar. Von der PINT (Public Switched Telephone Network and Internet Internetworking) Arbeitsgruppe der IETF [IETF98a] aber auch den Standardisierungsgremien der ETSI, wie der Arbeitsgruppe TIPHON [TIPHON97], werden aktuell eine Vielzahl von Mehrwertdiensten konzipiert, die im öffentlichen Telefonnetz nur schwer oder nicht zu verwirklichen sind. Als Beispiele seien hier "Unified Messaging", "Voice Mail", "Automated Call Distribution" oder "Click To Dial" in Call-Centern sowie der telefonische Zugriff auf Informationen aus dem WWW oder anderen Informationsdiensten ("Voice Access To Content") genannt.

Einen weiteren und aus unserer Sicht besonders wichtigen Entwicklungstrend stellt die Schaffung und Nutzung von Übergangspunkten zwischen dem konventionellen Telefonnetz und IP-Telefonie-Endgeräten bzw. einer entsprechenden Infrastruktur dar. Diese Gateways erschließen der Internet-Telefonie unmittelbar einen sehr großen Anwenderkreis und können zu deren schnelleren Akzeptanz beitragen. Sollen Gatewaydienste kommerziell und im Wettbewerb unterschiedlicher Provider angeboten und abgerechnet werden und dabei Komponenten in einer heterogenen Gesamtkonstellation miteinander interagieren, so ist eine gesicherte und verbindliche Kommunikation unverzichtbar. Diese Überlegung sollte sich auch in den zu definierenden Architekturen und Protokollen niederschlagen.

# 2 Sicherheitsanforderungen der Internet Telefonie

Internet Telefonie hat sich, ausgehend von ersten durch die Firma VocalTec im Jahre 1995 kommerziell angebotenen Entwicklungen, zu einem wichtigen Forschungs- und Anwendungsfeld entwickelt, nachdem z. B. durch MBone-Anwendungen [Kumar95] die prinzipielle Nutzbarkeit paketvermittelter Netze zur Sprachdatenübertragung gezeigt wurde. Die einfachsten Applikationen erlauben eine simple Sprachkommunikation zwischen zwei über ein IP-Netz verbundenen, explizit zu adressierenden und mit Audio- Ein- und Ausgabemöglichkeiten ausgestatteten Rechnern.

Mittlerweile sind weitere, über diese unmittelbaren Ende-zu-Ende-Verbindungen hinausgehende Szenarien mit neuen Diensten und zusätzlichen Architekturkomponenten realisiert worden. Erste Internet Telefonie Gateways (ITG) erlauben Verbindungen zwischen dem Internet und dem öffentlichen leitungsvermittelten Telefonnetz (PSTN). So existieren insbesondere die in Abbildung 1-3 dargestellten Szenarien.

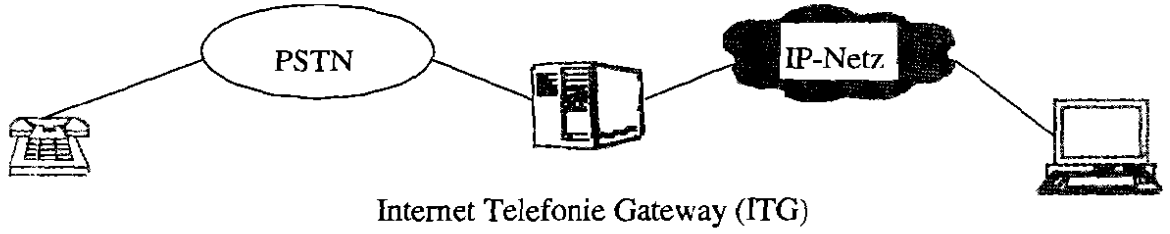


**Abb.1:** Gateway-Szenario: Telefon zu PC bzw. PC zu Telefon

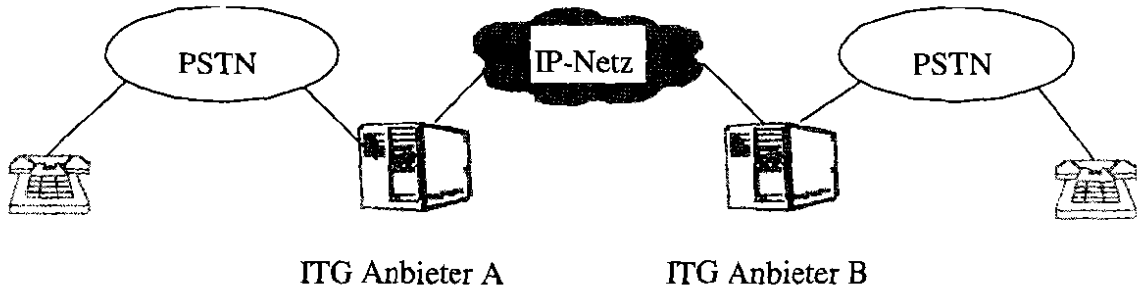


**Abb.2:** Gateway-Szenario: Telefon zu Telefon über IP-basierte Infrastruktur

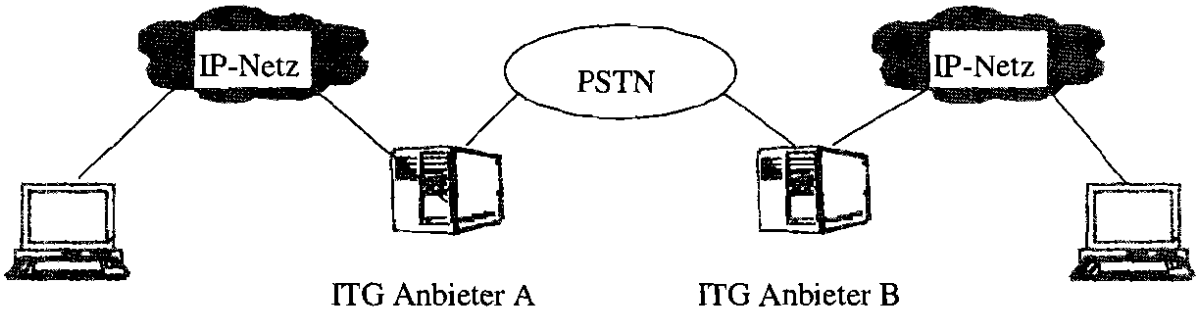


**Abb.3:** Gateway-Szenario: PC zu PC über konventionelles Telefonnetz

Die Qualität der Sprachkommunikation hat sich, sowohl durch die Weiterentwicklung der verwendeten Codecs als auch durch die Leistungsfähigkeit der genutzten Netze und durch Maßnahmen zur Erfüllung von Dienstgütegarantien in den vergangenen Jahren wesentlich verbessert. Somit erscheint heute ein kommerzieller Einsatz als sinnvoll.

Im Rahmen unserer weiteren Diskussion sicherheitsrelevanter Fragestellungen ist zu berücksichtigen, daß in den unterschiedlichen und möglicherweise von verschiedenen Anbietern betriebenen Übertragungssegmenten jeweils Kosten anfallen und entsprechende Abrechnungsinformationen geeignet weitergegeben werden müssen. In einem heterogenen und offenen

Szenario stellt zusätzlich bereits die Auswahl eines geeigneten Gateways, über das zunächst kein Wissen vorliegt und zu dem, anders als im Falle einer klassischen Telefonvermittlung, kein unmittelbares Vertrauen besteht, ein wichtiges und sensitives Problem dar. Prinzipiell können bereits heute eine Vielzahl von nicht a priori vertrauenswürdigen Betreibern entsprechende Dienste anbieten und dabei Zugang zu den übertragenen Sprachdaten erhalten. Durch die Weitergabe von unrichtigen, nachfolgend nicht eingehaltenen oder auch verfälschten Informationen auf Anfragen zur Auswahl eines Gateways kann es zu einer Wettbewerbsverzerrung aber auch zur gezielten Überlastung einzelner Systeme durch Denial-of-Service Attacken kommen.

Neben den Netzanbietern und den Internet Service Providern, denen eine eher passive Rolle als Betreiber der unterliegenden Verbindungsinfrastruktur zukommt, lassen sich zwei Hauptakteure innerhalb der Internet Telefonie Szenarien benennen. Dies sind einerseits die Gesprächsteilnehmer mit ihren computerbasierten oder konventionellen Telefonen und andererseits die Betreiber von Gateways.

Ein Gesprächsteilnehmer verlangt zunächst die Sicherheit, die ihm im konventionellen leitungsvermittelten Telefonnetz angeboten wird. Dies sind die Vertraulichkeit seines Kommunikationsverhaltens im Sinne des Datenschutzes, die Authentifizierung des Gesprächspartners über die Rufnummer und die ihm u. U. bekannte Stimme und eine korrekte Abrechnung. Darüber hinaus geht er von einer weitestgehenden Vertraulichkeit und Integrität des Gesprächsinhaltes aus. Will er diese komplett gewährleisten muß er spezielle Endgeräte mit Verschlüsselungsfunktion einsetzen. Im Falle der IP-Telefonie stellt eine etwaige Verschlüsselung der Sprachdaten (vgl. Abb. 5) somit ein Mehrwert dar. Zudem kann ein Mehrwert der Schutz vor nicht gewünschten Anrufen, durch eine Identifikation des Anrufenden vor der Signalisierung sein. Weitere Anforderungen des Gesprächsteilnehmers sind die Authentifizierung und Autorisierung neuer Teilnehmer bei Multiparty-Konferenzen und die korrekte Informationsbereitstellung (z. B. Kosten, Verbindungsmöglichkeiten und Abrechnungsverfahren) für die optimale Gateway Bestimmung.

Für den Betreiber eines Internet Telefonie Gateways, der mit der Bereitstellung seiner Dienste ein kommerzielles Interesse verbindet, besteht die Notwendigkeit, diese mit den Endteilnehmern und anderen Infrastrukturkomponenten korrekt auszuhandeln und widerspruchsfrei abzurechnen. Voraussetzungen dafür sind die:

- Authentifizierung und Überprüfung der Autorisierung des Gesprächspartners bzw. im Falle der Inter-Gateway-Kommunikation des korrespondierenden Gateways
- Überprüfung der Integrität der übermittelten Signalisierungsinformationen
- Nichtabstreitbarkeit und Verbindlichkeit angeforderter Kommunikationsdienste

In leitungsvermittelten Netzen ist anhand der Rufnummer, die einem physischen Anschluß fest zugeordnet ist, die Identifizierung des rufenden bzw. angerufenen Endsystems, die Auswahl eines Diensterbringers (unmittelbar oder auch durch Call-by-Call) und des genutzten Dienstes möglich [Schulzrinne98]. Diese Funktionen müssen in Internet Telefonie Anwendungen explizit durch eine entsprechende Signalisierung zwischen den einbezogenen Akteuren realisiert werden und sind entsprechend sensibel für Angriffe oder mißbräuchliche Verwendung.

Nicht zuletzt sind die Regelungen des Gesetzgebers zu berücksichtigen, so fordert dieser z. B. in Deutschland von den Fest- und Mobiltelefon-Netzbetreibern die Einrichtung von Zugriffs-

möglichkeiten auf die Vermittlungseinrichtungen und Gesprächsinhalte für autorisierte staatliche Behörden. Aktuell besteht Unklarheit bezüglich der für die Internet Telefonie anzuwendenden Gesetzesgrundlagen [EEC97]. Die Situation wird durch den möglichen transnationalen Charakter der Kommunikationsbeziehungen auch bei Gesprächen zwischen nationalen Teilnehmern zusätzlich kompliziert. Für zukunftssichere Lösungen sollten mögliche Forderungen wie z.B. die nach einem Key Escrow für die eventuell vorgesehene Audiodaten-Verschlüsselung in jedem Falle bereits frühzeitig berücksichtigt werden.

Bei der Entwicklung von Protokollen und Systemen für Internet-Telefonie werden Sicherheitsaspekte bisher nur unzureichend beachtet. So findet sich in den meisten Protokollen oder Protokollentwürfen unter dem Stichpunkt „Security" eine Formulierung wie „authentication and security issues ... are to be addressed in a future version of this document" [Davis98] oder allgemeine Aussagen, daß die Probleme zu berücksichtigen sind.

# 3 Internet Telefonie Architekturen und Standards

Im Gegensatz zu klassischen Telekommunikationsnetzen, in denen die Verarbeitungs- und Signalisierungsfunktionen im wesentlichen in den Knoten der Netzwerkbetreiber lokalisiert sind, verwenden Protokolle für die Internet Telefonie, wie das von der ITU vorgeschlagene H.323 [ITU98a] und das von der Internet Telephony (IPTEL) Working Group der IETF [IETF98b] favorisierte Session Initiation Protocol (SIP) [Handley98] mit seinen telefoniespezifischen Erweiterungen, eine stark dezentrale Architektur. Dieser Ansatz resultiert einerseits aus dem Fehlen zentral verwalteter Instanzen im Internet, andererseits aus der Zielvorstellung, einen kurzfristig nutzbaren und dennoch variablen und gut skalierbaren Gesamtrahmen zu schaffen.

In einer allgemeinen Architektur für Internet Telefonie unterscheiden wir mit den End- und Netzsystemen zwei Grundkomponenten. Endsysteme sind Computer sowie konventionelle oder spezielle IP-Telefone, die von einem Anwender direkt benutzt werden, und automatisierte Systeme, wie z.B. Voice-Mailboxen.

Eine Reihe von Diensten, wie das Auffinden des Benutzers und des Ortes (IP-Adresse) seiner momentanen Erreichbarkeit anhand eines symbolischen Namens ("User Location"), die Auswahl eines geeigneten und kostengünstigen Gateways beim Übergang zwischen konventionellem und IP-basiertem Netz ("Gateway Location") [Rosenberg98] oder auch die klassischen Funktionen einer TK-Anlage ("Call Distribution", "Behavior-on-busy"), müssen unabhängig von der augenblicklichen Verfügbarkeit einzelner Endsysteme vielen Anwendern permanent zur Verfügung stehen. Sie können daher von den Endsystemen, die zwischenzeitlich unerreichbar oder abgeschaltet sein können, nicht erbracht werden. Vielmehr werden diese Aufgaben in den uns bekannten Internet Telefonie Architekturen von Netzsystemen erfüllt. Die Netzsysteme übernehmen die primäre Aufgabe, Signalisierungsinformationen entgegenzunehmen, zu verarbeiten, zu speichern und an andere End- bzw. Netzsysteme weiterzuleiten. Im Falle von Gateways dienen sie zusätzlich der Verbindung von Teilsystemen und zur Wandlung oder Abbildung der genutzten Datenformate.

Ein Ausschnitt der resultierenden Gesamtarchitektur und mögliche Interaktionen zwischen den einzelnen Komponenten, hier zum Zwecke der Signalisierung beim Gesprächsaufbau, sind in Abbildung 4 dargestellt.

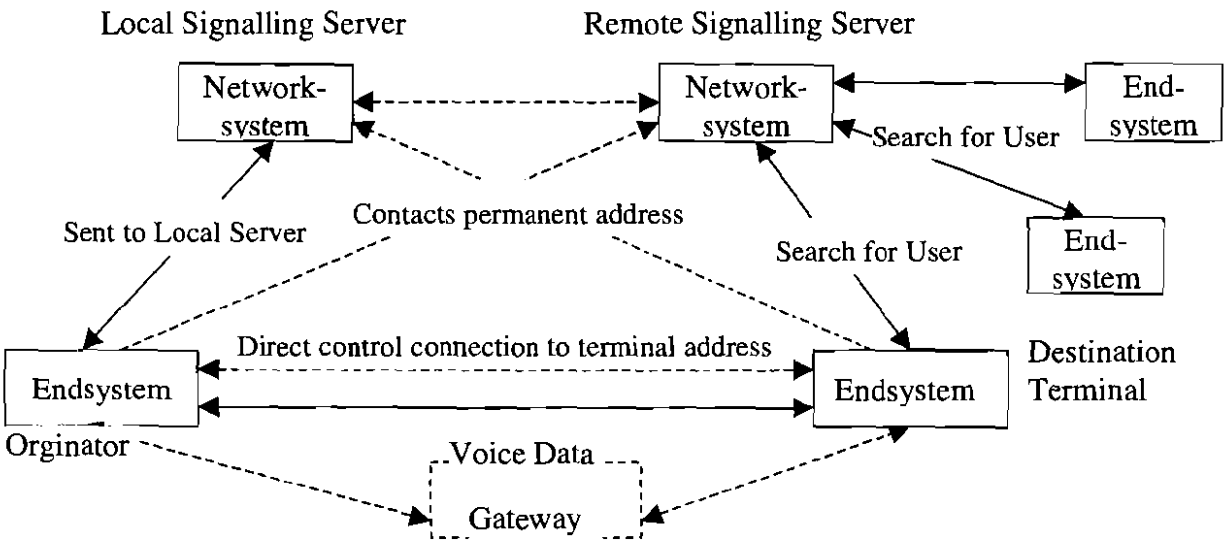


**Abb.4:** Interaktionen beim Gesprächsaufbau innerhalb der Internet Telefonie Architektur

Die zwei wichtigsten Protokollvorschläge für Internet Telefonie orientieren sich an diesem Architekturrahmen. Sie beschreiben jeweils eine Menge von unterschiedlich komplexen Datenübertragungs- und Signalisierungsverfahren und deren Zusammenwirken.

Die ITU hat die H.323 Protokollfamilie standardisiert. Die H.323 Protokolle sind sehr komplex, besitzen einen großen Signalisierungs-Overhead und sind bisher nicht durchgängig und interoperabel implementiert. Die IETF Working Groups (iptel, pint) diskutieren daher als Alternative zu H.323 das Session Initiation Protocol (SIP) als Signalisierungsprotokoll. Beiden Vorschlägen gemein ist das Vorhandensein der oben beschriebenen Netzsysteme. In der H.323 Architektur werden diese als Gatekeeper und Gateways bezeichnet, in der alternativen SIP Welt erfüllen Proxy Server, Redirect Server, Registrars und ebenfalls Gateways ihre Aufgaben.

Allgemein senden Endsysteme Informationen an Netzsysteme, die diese geeignet auswerten, speichern und zur Erfüllung ihrer Aufgaben benutzen. So zeigt z. B. ein Nutzer im Rahmen einer Registrierung (in H.323: H.225.0 RRQ, in SIP: Register-Request) seine aktuelle Terminaladresse an. Wie in Abbildung 4 dargestellt, sendet der Orginator beim Verbindungsaufbau eine Signalisierungsnachricht an seinen lokalen Signalisierungsserver. Dieser kennt entweder die aktuelle Terminaladresse des Gerufenen oder leitet die Signalisierung weiter an einen anderen Signalisierungsserver, der nun das Endsystem benachrichtigt. Die Bestimmung des zugehörigen Servers ist Aufgabe eines entsprechenden Protokolls (z.B. Gateway Location Protocol [Rosenberg98] oder Gatekeeper Routing Protocol [Davis98]). Die Datenverbindung zur Übertragung der Sprachdaten wird dann direkt zwischen den Endsystemen oder über ein zwischengeschaltetes Gateway aufgebaut. Es ist unmittelbar klar, daß sich auch bei der Kommunikation mit oder zwischen Netzsystemen sicherheitsrelevante Fragestellungen ergeben. Nach einer kurzen Darstellung möglicher Basismechanismen werden wir in Abschnitt 5 eine Erweiterung der vorgestellten Architektur vorschlagen.

# 4 Sicherheitsmechanismen

Zur Erfüllung der grundsätzlichen Sicherheitsanforderungen Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit sind verschiedene kryptographische Verfahren nutzbar. So bietet insbesondere die Nutzung von Ende-zu-Ende-Verschlüsselung zwischen den beteiligten Kommunikationspartnern einen Schutz vor unberechtigtem Zugriff und erlaubt es, die Authentizität eines Partners zu überprüfen. Eine zentrale Rolle spielt dabei die geeignete Bereitstellung oder Aushandlung der zu verwendenden Schlüssel.

Da es sich bei den Internet Telefonie Anwendern um eine heterogene und offene Benutzergruppe handelt, sollten Sicherheitsmechanismen auf Public Key Verfahren, für die Gesprächsdatenverschlüsselung auf symmetrischen Verfahren basieren. Mit deren Hilfe ist es möglich, daß mehrere Kommunikationsteilnehmer, die zunächst über keine Informationen übereinander verfügen, ihre Authentizität nachweisen, vertraulich Sitzungsschlüssel vereinbaren und nachfolgend gesichert miteinander kommunizieren. Public Key Verfahren basieren auf der Verwendung eines öffentlichen (Public Key) und eines zugehörigen privaten Schlüssels (Private Key), von denen nur der private geheimgehalten wird, während der öffentliche Schlüssel allgemein bekannt sein kann. Sie setzen als zentrale Vorbedingung ein Vertrauen in die Authentizität der Public Keys voraus. Die Richtigkeit der Beziehung "Entität - zugehöriger Public Key" muß geeignet überprüfbar sein. Dies ist durch Nutzung von Zertifikaten auch in einem transitiven und für eine große Anzahl von Nutzern skalierbaren Prozeß möglich. In diesem Verfahren leistet eine dritte Instanz, eine sogenannte Certification Authority (CA), eine digitale Signatur über den Identifikator eines Objekts, dessen Public Key und möglicherweise zusätzliche Informationen, wie z. B. den Gültigkeitszeitraum des entstehenden Zertifikats. Die Bindung der Zertifizierungsinstanz an den zugehörigen Public Key kann wiederum von anderen Zertifizierungsinstanzen, die eine baum- oder netzartige Zertifizierungsstruktur bilden, beglaubigt werden. Die Überprüfungskette kann abgeschlossen werden, wenn für einen Zertifikator, z.B. durch persönlichen Austausch der Information oder durch Publikation in einem allgemein zugänglichen Medium, Sicherheit über dessen zugehörigen Public Key besteht.

Aktuell existiert eine Reihe von Vorschlägen zur Realisierung von Public Key Infrastrukturen (PKI), die neben Voraussetzungen für die standardisierte Abspeicherung und den Zugriff auf Zertifikate auch technische und administrative Regelungen für deren Erteilung und Rückziehen zur Verfügung stellen müssen. Dabei seien insbesondere die Simple Distributed Security Infrastructure (SDSI), die Simple Public Key Infrastructure (SPKI) [IETF97a] und die X.509 basierte Public Key Infrastructure using X.509 (PKIX) [IETF97b] genannt.

Aufgrund des, trotz der Initiativen einiger Betreiber, aktuellen Fehlens umfassender, staatlich, gemeinnützig oder kommerziell betriebener Zertifizierungsinfrastrukturen nutzen eine Reihe von Anwendungen und Protokollvorschlägen insbesondere im Internet auch die von PGP [Garfinkel95] zur Verfügung gestellten und auf ein "Web-of-Trust" aufbauenden Dienste. Entsprechende Paare aus einem ein Objekt beschreibenden Identifikator (z.B. Email-Adresse) und zugehörigem Public Key werden auf einer Vielzahl von Servern allgemein zur Verfügung gestellt.

Die Darstellung der kryptographischen Grundlagen der Verfahren, einer Taxonomie existierender Ansätze und der national zugrunde liegenden rechtlichen Bestimmungen ist nicht

Anliegen des Beitrages. Diese können z.B. in [Branchaud95] [Schneier96] [Fischer98] und [BGBL97] geeignet nachgelesen werden.

# 5 Integration von Sicherheitsmechanismen in die Gesamtarchitektur

Bisher wurden ausgehend von den vorhandenen Szenarien und deren Risiken die Anforderungen der Kommunikationsteilnehmer an und die grundsätzliche Notwendigkeit von Sicherheitsunterstützung für die Internet Telefonie aufgezeigt. Ziel ist es nun, einen Rahmen für die Integration von allgemeinen sicherheitsrelevanten Mechanismen in die Systemarchitektur für Internet Telefonie zu definieren.

Die Gewährleistung der Vertraulichkeit der Gesprächsdaten ist mittels symmetrischer Verschlüsselungsverfahren, nach Austausch oder Aushandlung entsprechender Session Keys, relativ einfach durch Software oder Hardwareverschlüsselung im Datenpfad zwischen den Codecs der verwendeten Anwendungen realisierbar, wie in Abb. 5 dargestellt. Dabei ist zu beachten, daß die Verarbeitungszeit für die Verschlüsselung zu einer zusätzlichen Verzögerung führen kann, die die Qualität der Sprachübertragung reduzieren kann. Entscheidend ist zudem die Ergänzung der Signalisierungsprotokolle. Diese sollten sowohl durch Berücksichtigung im Layout der auszutauschenden Protokolldaten als auch durch Erweiterbarkeit der jeweiligen Protokoll-Maschinen primär eine Authentifizierung der Kommunikationsteilnehmer mittels unterschiedlicher Strategien erlauben.

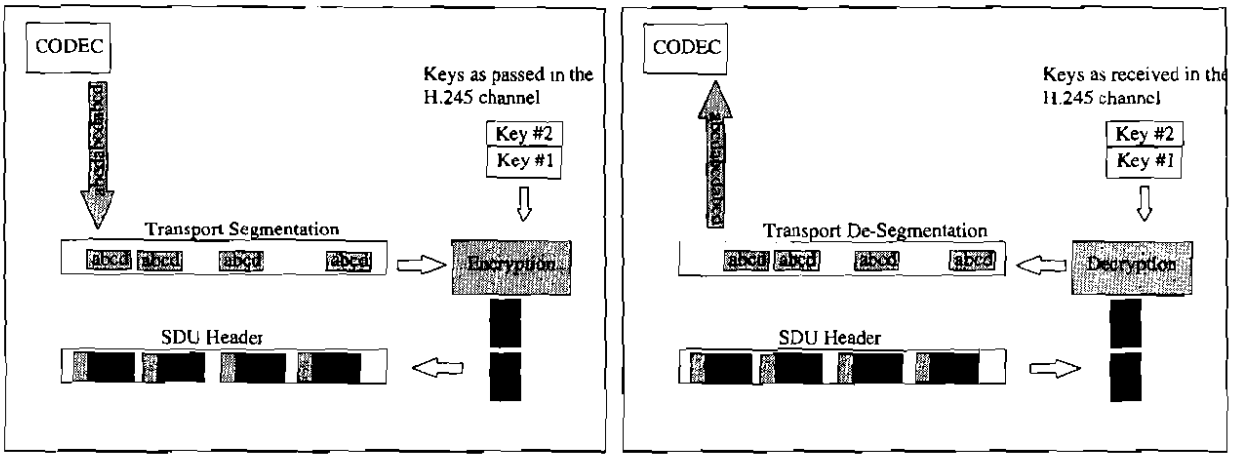


**Abb. 5:** Ver- bzw. Entschlüsselung von RTP-Paketen nach H.235

Für die Arbeit in einem offenen und nicht nur von einem Betreiber, mit einem möglichen Virtual Private Network und ausgezeichneten Zugangspunkten, genutzten Gesamtsystem ist es sinnvoll, alle Komponenten mit einem zertifizierten Public Key auszustatten und eine Anbindung an eine Public Key Infrastruktur vorzusehen. Wir schlagen daher die in Abbildung 6 gezeigte Ergänzung der IP Telefonie Architektur vor. Dabei stellen spezielle Netzsysteme allen Komponenten einen Zugriff auf einen Verzeichnisdienst für Zertifikate zur Verfügung. Die aus verschiedenen Certification Authorities gebildete Public Key Infrastruktur sollte die öffentlichen Schlüssel für End- und Netzsysteme zertifizieren und einen Verzeichnisdienst zum allgemeinen Zugriff auf Zertifikate und Revocation Lists bereitstellen.

Diese Aufgaben sind nicht spezifisch für IP-Telefonie-Umgebungen, sie können im Rahmen eines allgemein nutzbaren und etablierten Dienstes erbracht werden. Die Verteilung von Zertifikaten und Revocation Lists kann z. B. über einen globalen Directory Dienst nach dem Standard X.500, in dem die Informationen verteilt gehalten werden, erfolgen. Das X.509-Directory Authentication Framework [ISO93] definiert Konzepte für den Aufbau eines entsprechenden Netzwerkes von CAs und ihrer Verzeichnisdienste. Mittels des Lightweight Directory Access Protocols (LDAP) [Wahl97] erhält der Anwender einen transparenten Zugriff auf die Verzeichnisse und kann Zertifikate abfragen.

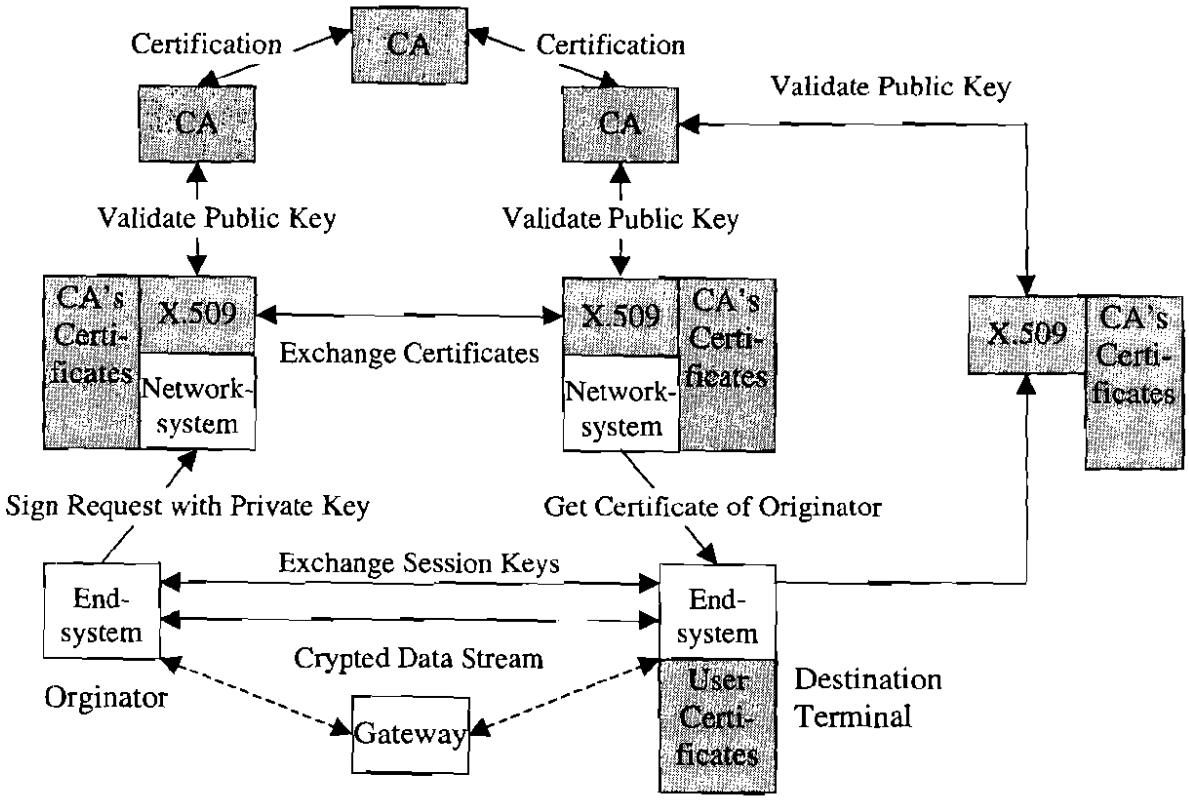


**Abb. 6:** Erweiterte Internet Telefonie Architektur

Unser modularer Ansatz erlaubt den einheitlichen Zugriff auf unterschiedliche Public Key Infrastrukturen, zu denen jeweils ein geeignetes Interface zur Verfügung zu stellen ist. Wichtig ist die Integration in die vorgestellte Gesamtarchitektur und den Protokollablauf. Dies schlägt sich in folgenden Forderungen nieder:

- Übermittelt ein System einen Request oder Informationen an ein anderes, so hat es diese Daten mit seinem privaten Schlüssel zu signieren.
- Empfangene Daten sind nur anzuerkennen, wenn deren Unversehrtheit und die Authenzität des Absenders überprüft wurde.
- Eine entsprechende Überprüfung erfolgt unter Nutzung der dafür vorgesehenen Netzsysteme vorzugsweise mit Hilfe von Zertifikaten, die bei einer Public Key Infrastruktur abfragbar sind.

- Die Autorisierung (als eine von der Authentifizierung zunächst unabhängige Leistung) kann durch so gesicherte Nachfrage bei entsprechenden Servern realisiert werden.

Registriert sich z. B. ein Endsystem an einem Netzsystem, so signiert es seinen Request unter Verwendung seines privaten Schlüssels. Das Netzsystem verfügt entweder bereits über den zertifizierten öffentlichen Schlüssel des Endsystems, erhält diesen unmittelbar oder auf Anforderung von einem anderen bereits vertrauenswürdigen Kommunikationspartner, z. B. einem anderen Netzsystem, oder fragt ihn von einem Verzeichnisdienst einer CA ab. Für mindestens eine Instanz der Zertifizierungshierarchie ist die allgemeine Kenntnis seines Zertifikates zwingend und z. B. im Programmcode oder durch initiale Konfiguration sicherzustellen. Zusätzlich sollten aus Performancegründen bereits bekannte zertifizierte Schlüssel lokal zwischengespeichert und nur nach einem bestimmten Zeitraum auf ihre Gültigkeit überprüft werden. Nach Verfügbarkeit des öffentlichen Schlüssels des Endsystems kann das Netzsystem die Authentizität dieses überprüfen. Ein analoges Vorgehen wird für alle weiteren sensitiven Signalisierungsaktionen genutzt.

# 6 Sicherheitsspezifische Protokollelemente

SIP sieht zur Realisierung der von uns identifizierten Anforderungen in allen Request Headern bereits ein Feld Authorization vor, in dem die PGP-Signatur der Nachricht transportiert werden soll. Die textbasierte und bewußt auf Erweiterbarkeit ausgelegte Implementierung des Protokolls bietet jedoch auch sehr gute Möglichkeiten für die Umsetzung zusätzlicher Protokollelemente und Funktionalitäten.

H.235 [ITU98b] beschreibt den Rahmen für Sicherheitsmechanismen für H.323 Kommunikation. Dort sind ebenfalls Public Key Verfahren zum Schutz von Punkt-zu-Punkt und Multipoint Konferenzen vorgesehen. Dabei wird zum einen die Verschlüsselung der per RTP übertragenen Sprachdaten, wie in Abbildung 5 dargestellt, beschrieben. Zum anderen werden aber auch Optionen für die Gewährleistung von Authentifizierung, Integrität, Vertraulichkeit und Nichtabstreitbarkeit angeboten [Newman98]. H.235 sieht als Basis einen per TLS oder IPSEC gesicherten Signalisierungskanal zu einem bekannten Port vor. Die Authentifizierung erfolgt dann im Rahmen der Signalisierung durch den Austausch von Zertifikaten über diesen gesicherten Signalisierungskanal. Im zweiten Signalisierungsschritt ist dann ein Austausch der Verschlüsselungsfähigkeiten der Endsysteme sowie gegebenenfalls der Austausch von Sessionschlüsseln vorgeschlagen. Der Standard H.235 ist unseres Erachtens unzureichend, da er nur Protokollmechanismen zum Austausch von Zertifikaten und Schlüsseln zwischen den Endsystemen beschreibt. Die Netzsysteme werden nicht einbezogen und zudem sind keine Verfahren zur Verifizierung der Zertifikate und Verteilung der Schlüssel angegeben.

# 7 Ausblick

Voraussetzung für den Einsatz der vorgestellten Verfahren ist, daß alle Beteiligten über entsprechend zertifizierte Public Keys verfügen. Dies kann z. B. für neue Infrastrukturkomponenten bei deren Installation durch ihren Betreiber sichergestellt werden, wenn dieser über mindestens eine entsprechend als vertrauenswürdig zertifizierte Instanz verfügt. Deutlich schwieriger ist die Situation für die Endsysteme. Da sich CA-Infrastrukturen erst im Aufbau befinden, können entsprechende Zertifikate z. B. zweckgebunden von Dienstanbietern vergeben werden. Die genutzten Applikationen (User Agents) sollten sicherheitsrelevante Funktio-

nen und die eventuell notwendige Interaktion mit dem Anwender entweder unmittelbar integrieren oder diese an zur Erweiterung vorgesehene Agenten delegieren. Für eine Übergangszeit ist auch die Interaktion mit Systemen, die die sicherheitsspezifischen Protokollerweiterungen nicht unterstützen, möglicherweise unter Einschränkung des nutzbaren Funktionsumfanges, sowie die Nutzung anderer Mechanismen wie z. B. PINs oder TANs, die geeignet durch externe Mechanismen ("Out-of-Band") ausgetauscht werden können, vorzusehen. In einem Szenario mit konventionellen Endgeräten mit deren in der Regel beschränkten Eingabe-, Signalisierungs- und Verarbeitungsmöglichkeiten kommen die entsprechenden Operationen nur auf einer Teilstrecke der Übertragung und unter Kontrolle des Internet Telephony Gateways zum Einsatz.

Aufbauend auf die im Beitrag dargestellten Architekturüberlegungen werden von den Autoren im Augenblick praktische Implementierungen zur Einbindung sicherheitsrelevanter Dienste sowohl in das H.323- als auch das SIP-Protokollszenario vorgenommen und die Anbindung an Verzeichnisdienste sowie der entstehende Kommunikations- und Verarbeitungs-Overhead evaluiert.

## Literatur


[BGBL97] Verordnung zur digitalen Signatur (Signaturverordnung - SigV); BGBl. I S. 1870,1872, Juli 1997

[Branchaud95] M. Branchaud, S. Handa: "Re-Evaluating Proposals for a Public Key Infrastructure", Law/ Technology Journal, 1995

[Davis98] R. Davis: A Framework for a Peer Gatekeeper Routing Protocol, IETF Internet-Draft, November 1998

[EEC97] EEC: "Status of voice communications on Internet under community law and, in particular, under Directive 90/388", May 1997

[Fischer98] S. Fischer, A. Steinacker, R. Bertram, R. Steinmetz: "Open Security", Springer-Verlag Berlin Heidelberg, 1998

[Garfinkel95] S. Garfinkel: "PGP: Pretty Good Privacy", O´Reilly, Sebastopol, 1995

[Handley98] M. Handley, H. Schulzrinne, E. Schooler: "SIP: Session Initiation Protocol" IETF Internet- Draft, April 1998

[IETF97a] Simple Public Key Infrastructure (spki) Charter http://www.ietf.org/html.charters/spki-charter.html

[IETF97b] Public-Key Infrastructure (X.509) (pkix) Charter http://www.ietf.org/html.charters/pkix-charter.html

[IETF98a] PSTN and Internet Internetworking (pint) Charter http://www.ietf.cnri.reston.va.us/html.charters/pint-charter.html

[IETF98b] IP Telephony (iptel) Charter
http://www.ietf.cnri.reston.va.us/html.charters/iptel-charter.html

[ISO93] ISO / CCITT, ISO 9594-8/X.509, The Directory: Authentication Framework, Dec. 1993

[ITU98a] ITU-T Recommendation H.323 V.2 "Packet-Based Multimedia Communication Systems", Genf, 1998

[ITU98b] ITU-T Draft Recommendation H.235 "Security and Encryption for H. Series (H.323 and other H.245 based) Multimedia Terminals", Genf, 1998

[Kumar95] V. Kumar: "Mbone: Interactive Multimedia on the Internet", Macmillan Publishing, November 1995

[Newman98] E. Newman: Security for H.323-Based Telephony, White Paper, http://www.databeam.com/newsroom/articles/h323security-cti.html

[Rosenberg98] J. Rosenberg, H. Schulzrinne: "Internet Telephony Gateway Location", Proc. Of Infocom, (San Francisco, California), March/April 1998

[Schneier96] B. Schneier: "Applied Cryptography", Second Edition, John Wiley & Sons, New York, 1996

[Schulzrinne 97] H. Schulzrinne: "Re-engineering the telephone system" in Proc. Of IEEE Singapore International Conference on Networks (SICON), (Singapore), Apr. 1997.

[Schulzrinne98] H. Schulzrinne, J. Rosenberg: "Internet Telephony: Architecture and Protocols – an IETF Perspective" Computer Networks and ISDN Systems, 1998

[TIPHON97] "Draft summary minutes, decisions, actions from 1st TIPHON meeting" http://www.iihe.ac.be/scimitar/journal/J0697/tiphon_report.htm

[Wahl97] M. Wahl, T. Howes, S. Kille.: "Lightweight Directory Access Protocol (v3)", RFC 2251, Dec. 1997