Mehrseitige Sicherheit in der Telecommunications Information Networking Architecture

Sebastian Staamann, Technische Universität Berlin
Uwe G. Wilhelm, Eidgenössische Technische Hochschule - Lausanne

28. Februar 1997

1 Motivation

Die Telecommunications Information Networking Architecture (TINA) [BaBI_93] [NiDC_95] [TIN3_95] [TIN2_95] ist gedacht als Basis für die schnelle und kostengünstige Entwicklung und Einführung von Informations- und Kommunikationsdiensten. Deren Spektrum umfaßt die Funktionalität so verschiedener Dienste wie des heutigen Telefons, komplexer Konferenzdienste, des World Wide Web und von Video-on-demand. TINA ermöglicht Multimedia- und Mehrparteienkommunikation. Es werden sowohl vermittelte Kommunikation als auch Verteilung von Information unterstützt.

Als Geschäftsmodell für TINA dient der Supermarkt. Der *Konsument (consumer)* kauft von einem *Verkäufer (retailer)* die jeweilige Dienstnutzung. Zur Verfügung gestellt werden die Dienste gegen Bezahlung von verschiedenen, miteinander konkurrierenden, *Dienstanbietern (third party service providers)*. Die Übertragung und Vermittlung von Datenpaketen und Datenströmen erfolgt über Netze von ebenfalls miteinander im Wettbewerb stehenden *Verbindungsanbietern (connectivity providers)*. Der Verkäufer nutzt zur Diensterbringung für den Konsumenten die Dienste von Dienst- und Verbindungsanbietern. Die Konzepte für Subskription und Bezahlung erlauben dabei eine große Variabilität. Als Branchenbuch zum Auffinden eines Dienstes nach Dienstmerkmalen dient ein *Vermittler (broker)*. Ein TINA-System ist offen, d.h. jeder Interessierte, dessen Endgeräte Schnittstellen anbieten, die zu den von TINA spezifizierten Referenzpunkten konform sind, kann sich anschließen und in einer oder mehreren der genannten Rollen im TINA-System agieren.

In einem solchen System kann nicht davon ausgegangen werden, daß die Beteiligten sich gegenseitig vollständig vertrauen. Die Architektur muß Mittel bereitstellen, mit deren Hilfe die Beteiligten ihre jeweiligen Sicherheitsinteressen durchsetzen können. Haben traditionelle Auffassungen von Sicherheit in der Regel ausschließlich den Schutz des Informations- oder Kommunikationssystems vor Beeinträchtigung oder Mißbrauch durch zugelassene Benutzer und Außenstehende zum Inhalt, so muß die TINA-Sicherheitsarchitektur auch den Schutz des einzelnen Beteiligten gegen potentielle Angriffe durch andere Beteiligte, einschließlich Verkäufer, Netzanbieter und Verbindungsanbieter, ermöglichen. Voraussetzungen für eine solche *mehrseitige Sicherheit* [MüPf_97] sind eine geeignete Strukturierung von Information und Funktionalität sowie die Allokation der dabei entstehenden Objekte zu den jeweils betroffenen Beteiligten. Allokation eines Objektes zu einem Beteiligten bedeutet dabei den logischen Besitz und die physische Kontrolle des Objektes durch den Beteiligten. Ein geeignetes Zugriffskontrollsystem muß dem Besitzer die Festlegung der Zugriffsrechte übertragen *(discretionary access control)*. Die Rechte müssen mit genügend feiner Granularität und in Abhängigkeit von Kontextinformation, wie Anwendungskontext des Zugriffs, gegenwärtige Zeit und Zeit des letzten Zugriffs, spezifiziert werden können.

In diesem Beitrag stellen wir die TINA-C Architektur vor und untersuchen sie im Sinne mehrseitiger Sicherheit. Wir stellen detaillierte Anforderungen mit diesem Ziel auf, präsentieren die bisher in den Spezifikationen vorliegenden Ansätze und analysieren mögliche Bedrohungen. Wir fokussieren dabei auf den Schutz des Konsumenten vor dem illegitimen Beobachten seines Aufenthaltes und seiner Nutzung von Diensten. Hauptsächlicher Gegenstand unserer Betrachtung von TINA ist die *Dienstearchitektur (service architecture)*. Wir diskutieren die Allokation benutzerbezogener Information und geben einen Ausblick auf weitere Arbeiten im Interesse mehrseitiger Sicherheit in TINA.

2 Die TINA-C Dienstearchitektur

Die Dienstearchitektur [BeFG_95] [YOWK_95] ist eine der vier, jeweils einem Problemkreis zugeordneten, Teilarchitekturen in TINA (siehe vorhergehenden Beitrag in diesem Buch [WSWZ_97]). In ihr werden Konzepte, Prinzipien und Richtlinien für Konstruktion, Installation und Betrieb von Telekommunikationsdiensten vorgegeben. Sie definiert die Komponenten, aus denen ein Dienst gebildet wird, sowie die Kombination dieser Komponenten und ihre Interaktion. Das maßgebliche Dokument über die TINA-C Dienstearchitektur [TIN3_96] besteht aus einem präskriptiven und einem deskriptiven Teil. Die Umsetzung der Spezifikationen des präskriptiven Teils ist vorgeschrieben für die Konformität eines Produktes zu den TINA-Standards. Der deskriptive Teil enthält überwiegend Verfeinerungen, deren Umsetzung domänenintern oder spezifisch für Anbieter oder Dienste ist. Die Spezifikationen dieses Teils sind nicht verbindlich, sondern als Vorschläge oder Illustrationen für die Realisierung von Diensten zu betrachten.

2.1 Beteiligte, Rollen, Domänen und Referenzpunkte

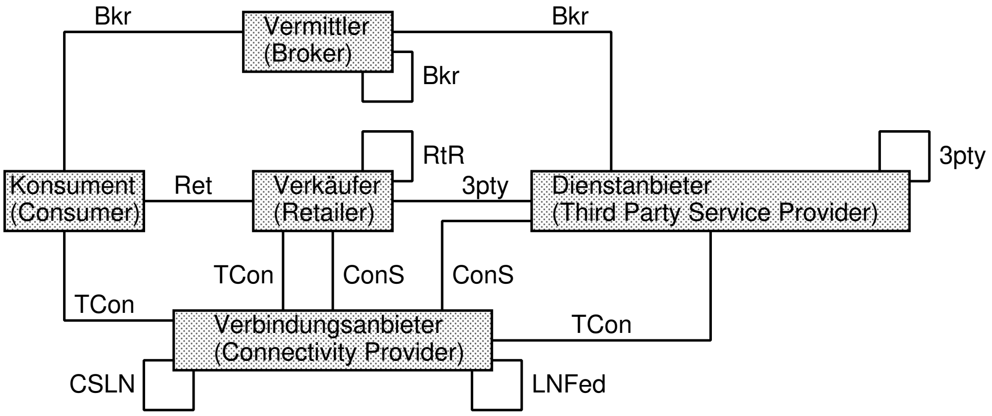
Beteiligte an einem TINA-System sind natürliche oder juristische Personen aus der realen Welt. Im TINA-System agieren die Beteiligten in einer oder in mehreren der schon erwähnten Rollen: Konsument, Vermittler, Verkäufer, Dienstanbieter und Verbindungsanbieter. Jeder Beteiligte ist im TINA-System durch seine Domäne[1] vertreten, die er selbst verwaltet. Diese Domäne enthält die von ihm physisch kontrollierte Hard- und Software.

Die Beziehung zwischen zwei Beteiligten ist durch das Nutzer-Erbringer-Paradigma bestimmt. Der Sinn dieser Beziehung ist die Nutzung *(usage)* der vom Erbringer *(provider)* angebotenen Dienste durch den Nutzer *(user)*. Die Nutzung teilt sich in drei Gebiete: den Zugang *(access)* als Voraussetzung für die Nutzung, die Primärnutzung *(primary usage)* als eigentlichen Grund der Beziehung und die Sekundärnutzung *(ancillary usage)* zu deren Unterstützung, z.B. zum Anpassen seiner persönlichen Kommunikationsumgebung durch den Nutzer in der Erbringerdomäne. Die drei Gebiete sind logisch voneinander getrennt. Die Anwendung des

[1] Natürlich kann eine natürliche oder juristische Person auch, wie schon in heutigen Telefonnetzen, mehrfach, als verschiedene Beteiligte mit jeweils eigenen Domänen, im TINA-System vertreten sein.

Nutzer-Erbringer-Paradigmas auf die Interaktionen schließt nicht aus, daß im Rahmen eines Vertrages zwischen zwei Beteiligten der eine dem anderen gegenüber sowohl als Nutzer als auch Erbringer auftritt und vice versa.

Interaktionen zwischen verschiedenen Beteiligten, d.h. Domänen, erfolgen über Interdomänenreferenzpunkte, im weiteren kurz als Referenzpunkte[2] bezeichnet. Die Referenzpunkte definieren die Interaktion zwischen Beteiligten. Abbildung 1 zeigt die Rollen und die definierten Referenzpunkte[3] zwischen den Rollen.



Bkr	Broker Reference Point
ConS	Connectivity Service Reference Point
CSLN	Client Server Layer Network Reference Point
LNFed	Layer Network Federation Reference Point
Ret	Retailer Reference Point
RtR	Retailer to Retailer Reference Point
TCon	Terminal Connection Reference Point
3pty	Third Party Service Provider Reference Point

Abbildung 1: Rollen und Referenzpunkte in TINA

Im folgenden seien skizzenhaft die schon in der Motivation vorgestellten Rollen und die dazugehörigen Referenzpunkte erläutert. Der Konsument bezieht von einem oder mehreren Verkäufern in einer Art Einzelhandel seine Dienste. Die Interaktion läuft über den Ret-Referenzpunkt. Ein Verkäufer bezieht die von ihm offerierten Dienste in einer Art Großhandel über den 3pty-Referenzpunkt von einem oder mehreren Dienstanbietern. Es ist auch möglich, daß er über den RtR-Referenzpunkt den Dienst von einem anderen Verkäufer kauft. Ähnlich kann auch ein Dienstanbieter den Dienst oder Teile davon[4] über den 3pty-Referenzpunkt von einem anderen Dienstanbieter beziehen. Jede dieser drei Rollen kann über den Bkr-Referenzpunkt vom Vermittler Information über die von anderen angebotenen Dienste beziehen oder sich für durch Merkmale und/oder Namen beschriebene Dienste Adressen von

[2] Neben den Interdomänenreferenzpunkten existieren Intradomänenreferenzpunkte, die vor allem der Portabilität von Softwarekomponenten dienen. Diese werden hier jedoch nicht betrachtet.

[3] Zum Zeitpunkt des Schreibens dieses Beitrags sind die Referenzpunkte als solche definiert, jedoch ist noch keine Spezifikation des Inhalts erhältlich.

[4] Es ist ein explizites Ziel von TINA, die Komposition von Diensten zu unterstützen.

Anbietern geben lassen. Dieser Referenzpunkt wird wahrscheinlich im Sinne eines fairen Wettbewerbs Gegenstand rechtlicher Bestimmungen sein.

Den Transport der Inhaltsdaten eines Dienstes, z.B. eines Audio-Stroms, übernimmt ein Verbindungsanbieter. Das Herstellen der Verbindungen zwischen den angegebenen Netzzugangspunkten, z.B. ein Strom zwischen den *Stream Interfaces* der Anwendungen (UAPs, siehe vorhergehender Beitrag [WSWZ_97]) zweier Konsumenten, kann als Dienst von Verkäufer oder Dienstanbieter über den ConS-Referenzpunkt angefordert werden. Der Abbau einer solchen Verbindung kann außer über den ConS-RP ebenfalls über den TCon-Referenzpunkt, dies auch durch den Konsumenten als Administrator der Domäne eines Endpunktes, veranlaßt werden. Die Referenzpunkte LNFed und CSLN dienen der Kooperation verschiedener Verbindungsanbieter, und zwar entweder nach den Modellen Client-Server (CSLN) oder Föderation (LNFed).

Die Domäne eines Beteiligten in einer Rolle muß nicht alle definierten Referenzpunkte dieser Rolle anbieten. Auch kann ein Beteiligter, d.h. eine Domäne, in mehreren Rollen agieren, z.B. als Verkäufer und als Dienstanbieter. In diesem Fall könnte der Verkäufer den über den Ret-Referenzpunkt dem Konsumenten angebotenen Dienst in seiner zusätzlichen Rolle als Dienstanbieter selbst erbringen. Der 3pty-Referenzpunkt würde also vom Verkäufer für die Erbringung des dem Konsumenten angebotenen Dienstes nicht gebraucht. Wenn die Domäne alle Dienste selbst erbringt und die Dienste nicht anderen Dienstanbietern zur Nutzung angeboten werden, kann der 3pty-Referenzpunkt in dieser Domäne entfallen.

Die hier beschriebenen Referenzpunkte sind letztlich Referenzpunkte zwischen Dienstkomponenten in verschiedenen Domänen. Die Interaktionen der als *Computational Objects (COs)* oder *Computational Object Groups (CO Groups)* im DPE (siehe [WSWZ_97]) realisierten Dienstkomponenten auf Anwendungsebene sind in den Referenzpunkten spezifiziert; die Interaktionen zwischen den Domänen auf der Ebene des DPE, über das *Kernel Transport Network (KTN)*[5], sind nicht Bestandteil der Referenzpunkte auf Anwendungsebene. Die Autoren erwarten, daß für die DPE-Interaktionen die CORBA-Spezifikationen [OMG2_95] maßgeblich sein werden.

Jede noch so komplexe Transaktion mit beliebig vielen Beteiligten setzt sich letztlich aus Interdomänen-Interaktionen nach dem Nutzer-Erbringer-Paradigma zusammen. Ein, eher einfaches, Beispiel möge dies veranschaulichen: Konsumentin Anja und Konsument Bernd wollen miteinander im Rahmen des Dienstes Audio-Konferenz kommunizieren. Beide haben jeweils eine Subskription für diesen Dienst beim Verkäufer DiensteDiscount. DiensteDiscount ist in diesen Beziehungen jeweils Erbringer; Anja und Bernd sind jeweils Nutzer. DiensteDiscount hat den Dienst nicht selbst in seiner Domäne implementiert, sondern beauftragt den Diensteanbieter AudioCom mit der Erbringung. In dieser Beziehung ist DiensteDiscount Nutzer und AudioCom ist Erbringer. Das Erbringen des Dienstes Audio-Konferenz impliziert den Aufbau einer Verbindung zwischen den UAPs von Anja und Bernd, ein Dienst, der in unserem Beispiel von Verbindungsanbieter CityNet erbracht wird. AudioCom ist hier Nutzer, und CityNet Erbringer.

Die allgemeine Anwendung des Nutzer-Erbringer-Paradigmas ermöglicht die Anwendung des im weiteren beschriebenen Sitzungsmodells auf alle Interdomänen-Interaktionen. Eine Nut-

[5]Das KTN ist das Netz, über das alle Daten zwischen operationellen Interfaces transportiert werden.

zung setzt in den meisten Fällen eine Subskription für den Nutzer voraus. *Subskribent (subscriber)* und *Endnutzer (end user)* müssen hierbei nicht identisch sein. Das Management von Subskriptionen (ggf. auch Online-Subskription) steht dem Subskribenten, unabhängig ob mit dem Endnutzer identisch, in Form von Sekundärdiensten zur Verfügung. Die dritte Unterklasse von Nutzern sind die *anonymen Nutzer (anonymous users)*. Sie können nur Dienste nutzen, die kostenlos sind oder die Online-Bezahlung erlauben.

2.2 Das Sitzungsmodell

Das Konzept der Verbindung von Teilnehmern in bisherigen Kommunikationssystemen ist in TINA im Interesse größerer Flexibilität durch das Konzept der *Sitzung (session)* ersetzt. Allgemein ausgedrückt ist eine Sitzung die temporäre Beziehung zwischen Ressourcen zur gemeinsamen Erfüllung einer Aufgabe. Eine Sitzung hat einen Zustand, der während ihrer Lebensdauer wechseln kann. Sie ist ein Informationsobjekt[6], ihre Implementierung erfolgt in Form von Dienstkomponenten, Computational Objects oder CO Groups und kann über mehrere Domänen verteilt sein. Allgemeine Operationen auf Sitzungen sind u.a.: terminieren *(terminate)*, unterbrechen *(suspend)* und reaktivieren *(resume)*.

Die verschiedenen Sitzungen betreffen drei Gebiete: den Zugang des Nutzers zum Erbringer, die Nutzung des Dienstes (Primär- und Sekundärnutzung) und die Verbindungen zwischen Nutzern. Die einzelnen Sitzungen können wiederum andere Sitzungen enthalten oder durch Verbindung mehrerer anderer Sitzungen gebildet werden. Abbildung 2 zeigt anhand des Beispiels einer Kommunikation zweier Teilnehmer die Sitzungen in TINA und ihr Verhältnis zu den Domänen.

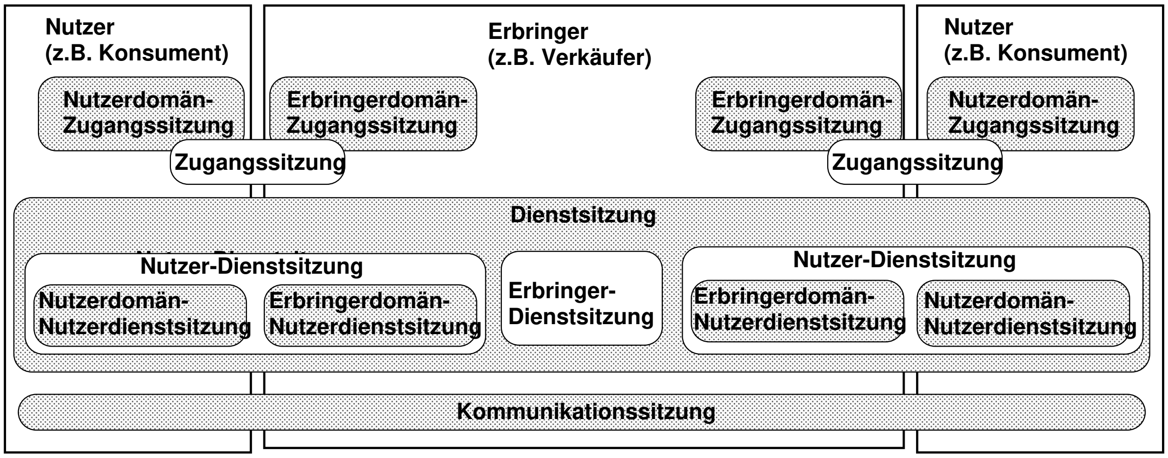


Abbildung 2: Sitzungen in TINA

Die *Zugangssitzung (access session)* ist der zeitlich begrenzte Zugang eines Nutzers zu den Diensten eines Erbringers, vergleichbar der Login-Sitzung eines Benutzers in einem Mehr-

[6] Ein Informationsobjekt ist ein mit der Technik der objektorientierten Modellierung (OMT) [RBPE_91] gebildetes Objekt. Diese Strukturierung erfolgt aus der Informationsperspektive *(information viewpoint)* [TIN1_95]. Ein Informationsobjekt kann auf ein oder mehrere Computational Objects *(computational viewpoint)* [TIN1_96] abgebildet werden.

benutzercomputer als Voraussetzung für das Benutzen der Programme. Sie wird etabliert, indem die Nutzerdomän-Zugangssitzung und die Erbringerdomän-Zugangssitzung kooperieren. Die Nutzerdomän-Zugangssitzung wird vom Nutzer kontrolliert und repräsentiert die für den Nutzer in der Nutzerdomäne verfügbaren Möglichkeiten. Sie enthält neben diesen technischen Beschränkungen die vom Nutzer bestimmten Politiken zu Aspekten wie u.a. Sicherheit und Gebührenberechnung. Die Erbringerdomän-Zugangssitzung enthält die entsprechenden Politiken des Erbringers. Basierend auf diesen, an die Beteiligten gebundenen, Politiken werden Kontexte für die Interaktionen ausgehandelt. Diese Kontexte sind Bestandteil der Zugangssitzung.

Die Zugangssitzung ermöglicht den, den Bedürfnissen und Möglichkeiten des Nutzers angepaßten, Zugang zu den Diensten. Sie bedeutet die, für ihre Dauer feste, Zuordnung eines Nutzers zu einem Endgerät, d.h. zu einer Domäne. Das Konzept der Zugangssitzung unterstützt Nutzermobilität. Der Nutzer kann von beliebigen Endgeräten aus und über beliebige Netzzugangspunkte eine Zugangssitzung mit dem Erbringer aufbauen. Eine offensichtliche und besonders herausgestellte Aufgabe der Zugangssitzung ist der Aufbau und das Aufrechterhalten einer sicheren Bindung der Domänen von Nutzer und Erbringer, was zuerst die Authentikation beinhaltet. Die zwischen Nutzerdomäne und Erbringerdomäne zu vereinbarende Authentikation ist ein Beispiel für einen Teil des Sicherheitskontextes. Die durch die Authentikation, in der Regel mit Aushandlung eines Sitzungsschlüssels verbundene, erreichte sichere Bindung kann dann auf *Dienstsitzungen (service sessions)* übertragen werden.

Eine Dienstsitzung ist eine Instanz eines Diensttyps. Sie enthält Information zur Aushandlung von Dienstqualität, Sicherheitskontext, zur Benutzung von Kommunikationsressourcen und zu den beteiligten Nutzern. An ihr beteiligt sind ein Erbringer und mindestens ein Nutzer. instanziiert wird eine Dienstsitzung in der Regel von einer Erbringerdomän-Zugangssitzung. Der Zugang zu einer Dienstsitzung erfolgt von einer etablierten Zugangssitzung aus. Die Dienstsitzung aggregiert zwei Klassen von Sitzungen, die Erbringer-Dienstsitzung und die Nutzer-Dienstsitzung. Die erste enthält die globale Sicht der Dienstsitzung, einschließlich aller Nutzer. Sie ist ist genau einmal in jeder Dienstsitzung vorhanden. Die Nutzer-Dienstsitzung ist die Sicht des Nutzers auf die Dienstsitzung; von ihr existiert eine pro Nutzer. Sie aggregiert wiederum zwei verschiedene Sitzungen, die Nutzerdomän-Nutzerdienstsitzung und die Erbringerdomän-Nutzerdienstsitzung. Letztere enthält die für den Nutzer spezifischen Aspekte der Dienstsitzung in der Erbringerdomäne. Erstere enthält Funktionalität und Information für die Unterstützung der Nutzer-Dienstsitzung in der Nutzerdomäne.

Ein an einer Dienstsitzung beteiligter Nutzer kann seine Zugangssitzung beenden, ohne seine Beteiligung an einer Dienstsitzung zu beenden. Die Erbringerdomän-Nutzerdienstsitzung wird in diesem Fall unterbrochen und der Nutzer kann diese nach dem erneuten Etablieren einer Zugangssitzung reaktivieren und seine Beteiligung wieder aufnehmen. Die neue Zugangssitzung kann an einem beliebigen anderen Endgerät und über einen beliebigen anderen Netzzugangspunkt erfolgt sein. Dieser Aspekt der persönlichen Mobilität wird als *Sitzungsmobilität (session mobility)* bezeichnet. Das skizzierte Konzept der Dienstsitzung gilt für alle Dienste gleichermaßen, gleich ob Primärnutzung (z.B. Video-on-demand oder Audio-Konferenz) oder Sekundärnutzung (z.B. Anpassen der persönlichen Kommunikationsumgebung oder Online-Subskription).

Die *Kommunikationssitzung (communication session)* repräsentiert eine allgemeine dienstorientierte Sicht auf die Verbindungen zwischen Stream Interfaces. Eine Kommunikationssitzung kann beliebig viele Verbindungen handhaben. Sie wird entweder durch eine Erbringer-Dienstsitzung oder durch eine Erbringerdomän-Nutzerdienstsitzung gesteuert. Parameter sind die gewünschten Endpunkte und Dienstqualitäten. An dieser Stelle sei daran erinnert, daß in TINA alle Inhaltsdaten eines Dienstes (z.B. Videoströme, Audioströme, Hypertextdokumente) ausschließlich über Verbindungen zwischen Stream Interfaces transportiert werden, wohingegen die Information zur Steuerung des Dienstes (z.B. Zurückspulen bei Video-on-demand) über operationelle Interfaces des Dienstes fließt.

2.3 Das Nutzerprofil

TINA unterstützt Mobilität und die Personalisierung von Diensten. Hierfür wird in der Erbringerdomäne Information über den Nutzer gehalten. Diese ist in dem Informationsobjekt *Nutzerprofil (user profile)* enthalten. Das Nutzerprofil enthält alle von der Erbringerdomän-Zugangssitzung benutzte Information für Autorisierungsentscheidungen (z.B. mag eine Subskription nur für bestimmte Endgeräte gültig sein) sowie über Beschränkungen und Anpassungen von Zugangs- und Dienstsitzungen. Das Nutzerprofil aggregiert folgende Objekte mit Information über den Nutzer:

- **Nutzungskontext** *(usage context)*: beschreibt eine Konfiguration aus Netzzugang und Endgerät einschließlich dessen Ausstattung, auf die der Nutzer für Zugangs- und Dienstsitzungen beschränkt ist. Der Nutzungskontext ist temporär (Mobilität), für jede bestehende Zugangssitzung besteht ein Nutzungskontext.

- **Dienstprofil** *(service profile)*: ist eine für den Nutzer spezifische Beschreibung eines Dienstes. Diese Beschreibung besteht im komplexesten Fall aus den vom Erbringer definierten Beschränkungen des Dienstes, den Beschränkungen durch den Subskribenten und den vom Endnutzer gesetzten Präferenzen. Das Nutzerprofil kann mehrere Dienstprofile enthalten.

- **Sitzungsbeschreibung** *(session description)*: spezifiziert eine existierende Dienstsitzung, die der Nutzer reaktivieren oder in die er eintreten kann. Eine Sitzungsbeschreibung wird erzeugt, wenn der Nutzer eine Dienstsitzung bzw. seine Teilnahme daran unterbricht, wenn er eine Dienstsitzung für einen späteren Zeitpunkt ansetzt *(scheduling)*, oder wenn er zur Teilnahme an einer schon existierenden Dienstsitzung eingeladen wird. Das Nutzerprofil kann mehrere Sitzungsbeschreibungen enthalten.

- **Registrierung** *(registration)*: nötige Information, um auf eine Anforderung, in eine Dienstsitzung einzutreten, zu reagieren. Eine solche Anforderung erfolgt u.a. bei einer Einladung zu einer Dienstsitzung oder wenn eine vorher angesetzte Dienstsitzung beginnt. Die Registrierung bestimmt, in Abhängigkeit von Parametern wie Diensttyp oder Zeit die Reaktion, wie z.B. Ablehnen der Einladung oder Auslieferung der Einladung in einer bestimmten Domäne. Ein Nutzerprofil kann beliebig viele Registrierungen enthalten.

Keines der Objekte des Nutzerprofils ist in TINA verbindlich spezifiziert, weder hinsichtlich der enthaltenen Information noch hinsichtlich der Logik, wie diese ausgewertet wird. Relationen zwischen den Objekten sind wahrscheinlich, z.B. können Dienstprofile Abhängigkeiten von Nutzungskontexten enthalten. Die Unterstützung von Mobilität und Personalisierung von Zugang und Dienstauslieferung ist im Prinzip gewährleistet, detaillierte Spezifikationen existieren jedoch nicht. Hier sind in unserer Untersuchung die Ergebnisse eines diesem Thema gewidmeten TINA-C auxiliary projects [EMPS_96] berücksichtigt.

2.4 Die Dienstkomponenten und ihre Allokation

Implementierungen von Diensten in einem TINA-System bestehen aus Dienstkomponenten. Die Dienstearchitektur definiert die Dienstkomponenten der Zugangssitzung[7], die an allen Diensten beteiligten Dienstkomponenten der Dienstsitzung, sowie die generischen Dienstkomponenten aller Dienste. Abbildung 3 gibt anhand des Beispiels der Konferenz mit zwei Teilnehmern einen Überblick über die Dienstkomponenten, Interaktionen und die Zuordnung zu Sitzungen und Domänen. Die einzelnen Dienstkomponenten, einschließlich der Bedeutungen der Akronyme, werden anschließend grob erläutert. Die dargestellten Objekte sind Dienstelemente, nicht einzelne Computational Objects. Die dargestellten operationellen Interfaces sind eigentlich Gruppen von operationellen Interfaces, die hier zur graphischen Vereinfachung zusammengefaßt sind.

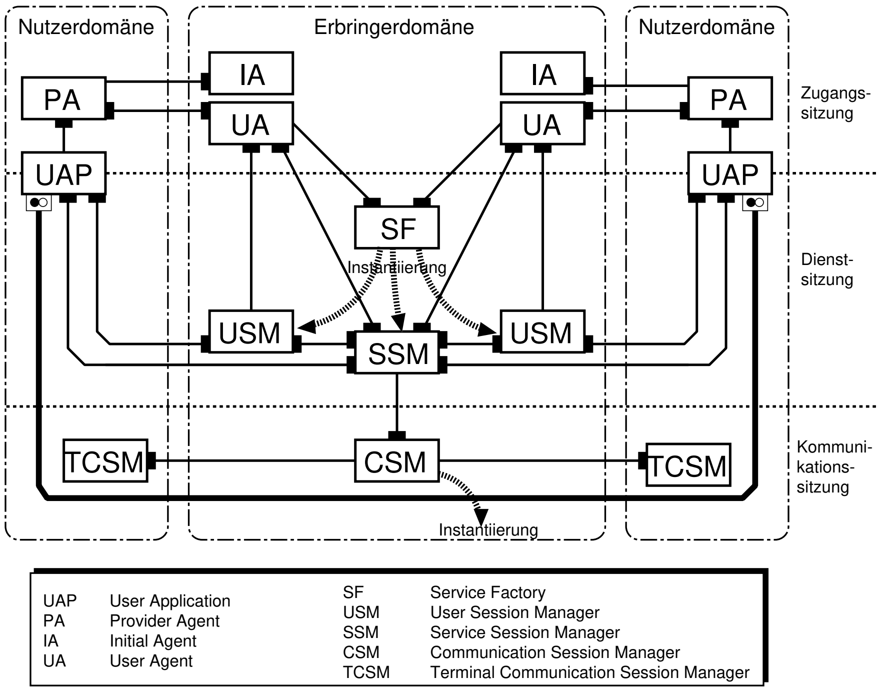


Abbildung 3: Dienstkomponenten in TINA

Komponenten für die Zugangssitzung:

- **UAP**: modelliert Anwendungen in der Nutzerdomäne. Die an der Zugangssitzung beteiligte UAP dient hier vor allem als Schnittstelle des Nutzers (User Interface) zum PA. In der Abbildung ist die Funktionalität für den Zugang in die UAP für die Dienstnutzung integriert.

[7]Der Zugang zum Erbringer wird in TINA als grundlegender Dienst aufgefaßt.

- **PA**: unterstützt die Nutzerdomän-Zugangssitzung. Er ist dienstunabhängig. Beim Aufbau einer Zugangssitzung kooperiert der PA mit dem IA in der Erbringerdomäne, um eine sichere Beziehung zwischen beiden Domänen herzustellen. Dies bedeutet im wesentlichen Authentikation und Erhalt der Referenz des zuständigen UA in der Erbringerdomäne. Im Verlauf der Zugangssitzung leitet er die Anforderungen des Nutzers zum Erzeugen einer neuen Dienstsitzung oder zum Eintreten in existierende Dienstsitzungen von der UAP zum UA weiter und in der entgegengesetzten Richtung die Einladungen zu existierenden Dienstsitzungen vom UA zur UAP, die den Nutzer dann benachrichtigt. Er unterstützt die anonyme Nutzung von Diensten und das Laden von Software aus der Erbringer- in die Nutzerdomäne. Dem Erbringer ermöglicht der PA den Zugriff auf Information über die Hardware- und Softwarekonfiguration des Terminals.

- **IA**: ist der initiale Zugangspunkt zur Erbringerdomäne. Er ist unabhängig von Dienst und Nutzer. Die Referenz des IA ist die Referenz, die ein Nutzer bekommt (z.B. von einem Vermittler), um einen Erbringer zu kontaktieren. Der IA unterstützt das Etablieren einer Zugangssitzung zwischen Nutzer und Erbringer, indem er dem Nutzer die Referenz eines zuständigen UA in der Erbringerdomäne liefert. Dabei gibt es zwei Möglichkeiten. Erstens, der Nutzer ist in der Erbringerdomäne bekannt, d.h. es gibt einen exklusiven UA für ihn, und er will als dieser im System handeln. In diesem Fall findet eine Authentikation zwischen Nutzer und Erbringer statt und der IA händigt dem PA die Referenz seines UA aus. Im zweiten Fall ist der Nutzer bisher nicht bekannt oder er will anonym bleiben. Dann findet keine Authentikation statt, der Nutzer erhält die Referenz eines anonymen UA.

- **UA**: repräsentiert den Nutzer in der Domäne des Erbringers. Er unterstützt die Erbringerdomän-Zugangssitzung. Der UA ist dienstunabhängig und existiert solange, wie der Nutzer beim Erbringer bekannt ist. Der UA hält zusammen mit dem PA die Zugangssitzung aufrecht, er hält als einzige Dienstkomponente in der Erbringerdomäne die Referenzen von dessen PA. Er ermöglicht dem Nutzer, eine neue Dienstsitzung zu erzeugen, indem der UA auf Anforderung vom PA hin die SF dieses Diensttyps beauftragt, SSM und USM zu erzeugen. Ein Nutzer kann in existierende Dienstsitzungen eintreten, indem sein UA die entsprechende SF beauftragt, den nötigen USM zu erzeugen. Der UA dient als Zugangspunkt des Nutzers zu dessen unterbrochenen Dienstsitzungen bzw. Nutzer-Dienstsitzungen. Er ermöglicht die Auswertung und Aktualisierung von Nutzungskontext und Dienstprofilen. Es handelt sich bei dem UA um einen abstrakten Komponententyp, instanziierbar sind nur die folgenden Untertypen mit zusätzlichen, spezifischen Merkmalen:

  - **namedUA**: Ein *named user agent* repräsentiert in der Erbringerdomäne einen authentisierten Nutzer. Er hält den vom Nutzer bestimmten Teil der Dienstprofile und dessen Registrierungen. Der namedUA nimmt Einladungen, in existierende Dienstsitzungen einzutreten, entgegen und liefert diese an den PA des Nutzers aus. Zusätzlich kann er Aktionen im Auftrag des Nutzers ausführen, wenn dieser nicht in einer Zugangssitzung ist[8]. Dies kann u.a. das Initiieren einer Zugangssit-

[8] Die Beschränkung der Möglichkeit von Aktionen auf die Zeit, wenn der Nutzer nicht eingeloggt ist, d.h. keine Zugangssitzung hat, erscheint uns überflüssig und hinderlich für das Filtern einkommender Einladungen zu Dienstsitzungen und die Festlegung entsprechender Reaktionen im voraus durch den Nutzer (vergleiche [EMPS_96] [GKGF_95] [DFRR_97]).

zung, basierend auf Information aus einer Registrierung, sein. Der namedUA kann, den Wünschen des Nutzers folgend oder entsprechend dem Nutzungskontext, eine zusätzliche, benutzerspezifische, Authentikation unterstützen.

  – **anonUA**: Ein *anonymous user agent* repräsentiert in der Erbringerdomäne einen anonymen Nutzer. Der anonUA existiert nur für die Dauer der Zugangssitzung, ebenso die vom Nutzer dabei gesetzten Präferenzen für einzelne Dienste. Im Unterschied zum namedUA können unterbrochene Sitzungen nur in der selben Zugangssitzung reaktiviert werden (keine Mobilität). Ein möglicher und kostenfreier Dienst, zu dem der anonUA den Zugang ermöglicht, ist Online-Subskription, durch die ein namedUA für den bis dahin in der Erbringerdomäne nicht bekannten Nutzer erzeugt werden kann.

Komponenten für die Dienstsitzung:

- **UAP**: modelliert Anwendungen in der Nutzerdomäne. Diese an der Dienstsitzung beteiligte UAP kann die Funktionalität der an der Zugangssitzung beteiligten UAP enthalten (wie in Abbildung 3), muß dies aber nicht tun. Die an einer Dienstsitzung beteiligte UAP enthält die Benutzerschnittstelle des Dienstes, sie ist dienstspezifisch und unterstützt die Nutzerdomän-Nutzerdienstsitzung. Sie kann folgende generische, d.h. in allen Diensten potentiell vorkommende, Funktionen unterstützen: Starten und Beenden der Dienstsitzung, Einladen anderer Nutzer zu der Dienstsitzung, Eintreten in eine existierende Dienstsitzung, Unterbrechen und Reaktivieren der Teilnahme an der Dienstsitzung oder auch der ganzen Sitzung. Die UAP kann null[9], ein oder mehr Stream Interfaces haben. Diese können an Stream Interfaces in Erbringer- oder anderen Nutzerdomänen gebunden sein. In einer Nutzerdomäne können eine oder mehr UAPs enthalten sein. Jede dieser UAPs kann einen oder mehrere Dienste unterstützen. Für jede Dienstsitzung kooperiert die UAP mit einem USM[10].

- **SF**: ist eine dienstspezifische Dienstkomponente. Sie erzeugt auf Anforderung durch den UA desjenigen Nutzers, der eine Dienstsitzung ins Leben ruft, die entsprechenden Dienstkomponenten, nämlich den SSM und den USM des Initiators der Dienstsitzung. Für den Fall, daß ein Nutzer in eine existierende Dienstsitzung eintritt, erzeugt sie den USM für diesen Nutzer. In allen Fällen liefert sie die Referenzen der kreierten Dienstkomponenten an den aufrufenden UA zurück, der sie an die entsprechenden UAPs weitergibt.

- **SSM**: unterstützt die Erbringer-Dienstsitzung. Er beinhaltet die zentrale Logik des Dienstes und kontrolliert die von allen Nutzern des Dienstes geteilten Ressourcen aus der Dienstperspektive. Dies ist, was die Kommunikationsressourcen betrifft, im wesentlichen die Steuerung des CSM. Der SSM hält den Zustand der Dienstsitzung als ganzes (aktiv/unterbrochen). Er verwaltet die Teilnehmer und ermöglicht das Hinzufügen,

[9]Manche Dienste, insbesondere Sekundärdienste, benötigen keine Stream Interfaces, z.B. Online-Subskription.

[10]Im Regelfall kooperiert die UAP (Nutzerdomän-Nutzerdienstsitzung) mit dem entsprechenden USM (Erbringerdomän-Nutzerdienstsitzung). Dienste mit nur einem Nutzer (z.B. Video-on-demand) haben möglicherweise keinen USM, sondern nur einen SSM, in den die Funktionalität des USM integriert ist, mit dem die UAP dann direkt kooperiert.

Einladen und Entfernen von Nutzern, außerdem unterstützt er das Management[11] der Dienstsitzung, z.B. die Anwendung von Schemata für die Gebührenberechnung. Weiter kann der SSM Möglichkeiten zu Aushandlungen zwischen den Nutzern, wie etwa Abstimmungen oder Versteigerungen, unterstützen. Der SSM kann null oder mehr Stream Interfaces haben. Diese können jeweils mit Stream Interfaces in Nutzer- oder anderen Erbringerdomänen verbunden sein.

- **USM**: unterstützt die Erbringerdomän-Nutzerdienstsitzung. Für jeden an einer Dienstsitzung beteiligten Nutzer existiert ein USM. Er enthält die nur diesen Nutzer betreffende Information und Funktionalität. Operationen, die nur diesen einen Nutzer betreffen, bearbeitet der USM selbst, für andere kooperiert er mit dem SSM. Der USM kontrolliert die für den Nutzer exklusiven Ressourcen in der Dienstsitzung und hält den Zustand der Nutzer-Dienstsitzung, d.h. der Teilnahme des Nutzers an der Dienstsitzung. Der USM kann, den Präferenzen des Nutzers entsprechend, konfiguriert werden. Dies kann bei der Initialisierung oder während der Sitzung geschehen. Der SSM kann null oder mehr Stream Interfaces haben. Diese können, wie auch beim SSM, jeweils an Stream Interfaces in Nutzer- oder anderen Erbringerdomänen gebunden sein.

Komponenten für die Kommunikationssitzung:

- **CSM**: ist eine dienstunabhängige Dienstkomponente. Er verwaltet auf der Anwendungsebene End-zu-End-Verbindungen zwischen Stream Interfaces *(Stream bindings)*. Die Eigenschaften (Qualities of Service) und die Konfiguration der Stream bindings einer Dienstsitzung werden in der Form eines *Logical Connection Graph (LCG)* beschrieben. Der CSM stellt SSM und USM operationellen Interfaces zur Verfügung, über die, dargestellt in der Form von LCGs, Stream bindings aufgesetzt, modifiziert und entfernt werden können. Der CSM teilt die zu verwaltenden Stream bindings in zwei Teile, Transportteil und Knotenteil. Der Transportteil ist der Teil außerhalb der Nutzerdomänen, der Knotenteil der innerhalb von Nutzerdomänen. Für den zweiten Teil benutzt der CSM den TCSM der jeweiligen Nutzerdomäne.

- **TCSM**: Der ist ebenfalls eine dienstunabhängige Dienstkomponente zur Verwaltung von Stream bindings, jedoch nur innerhalb der Nutzerdomäne. Dafür stellt der TCSM dem CSM ein operationelles Interface zur Verfügung.

Das Dokument zur Dienstearchitektur [TIN3_96] definiert die Dienstkomponenten, ihre Funktion, ihre entsprechenden operationellen Interfaces und ihr Zusammenwirken. Darauffolgende Dokumente[12] spezifizieren detailliert in der TINA Object Description Language (ODL) [TIN4_95] die einzelnen Dienstkomponenten. Vorgegeben wird dabei nur die Schnittstelle der Komponente nach außen, die innere Struktur bleibt dem Implementierer überlassen. Einige Dienstkomponenten offerieren Interfaces, auf die aus anderen Domänen heraus zugegriffen wird, z.B. IA, UA, USM und SSM. Die Menge aller Interfaces der Dienstkomponenten einer Domäne, auf die von einer anderen Domäne aus zugegriffen wird, bildet im wesentlichen den

[11] Unter Management wird in TINA im Zusammenhang mit Dienstsitzungen das dynamische Festlegen von Kontexten für die jeweilige Dienstsitzung verstanden. Dies umfaßt u.a. Sicherheit und Gebührenberechnung.

[12] Zum Zeitpunkt des Schreibens dieses Beitrags sind die Spezifikationen der Dienstkomponenten zur aktuellen Version der Dienstearchitektur noch nicht erhältlich.

Referenzpunkt[13] zwischen diesen beiden Domänen. Eine Dienstkomponente wird in der gleichen Weise spezifiziert wie ein Computational Object, d.h. es werden Syntax und Semantik der nach außen sichtbaren Interfaces vorgegeben. Aufgebaut ist die Dienstkomponente letztlich aus einem oder mehreren COs und/oder CO Groups. Jede Dienstkomponente ist logisch einer Domäne zugeordnet. Der Besitzer der Domäne ist Besitzer der Dienstkomponente. Die Zuordnung der Dienstkomponenten zu Domänen ist in Abbildung 3 mit dargestellt.

Ein CO ist eine Einheit der Verteilung, d.h. das CO ist vollständig in einer Domäne enthalten. Dienstkomponenten und CO Groups sind keine Einheiten der Verteilung, die COs und CO Groups, aus denen sie bestehen, können physisch auf verschiedene Domänen verteilt sein. Jedoch müssen von den eine Dienstkomponente implementierenden COs diejenigen, die die Interfaces der Dienstkomponente zur Verfügung stellen, zur Domäne der Dienstkomponente gehören. Teile der für die Dienstkomponente nötigen Information können jedoch in, zur Dienstkomponente gehörenden, COs verwaltet werden, die nicht in der Domäne der Dienstkomponente sind. Diese Möglichkeit nutzen wir für unseren Ansatz für die Allokation nutzerbezogener Information in der Domäne des Nutzers.

3 Analyse hinsichtlich mehrseitiger Sicherheit

Die bisher verfügbaren TINA-Dokumente zum Thema Sicherheit sind hinsichtlich mehrseitiger Sicherheit ambivalent. Beispielsweise werden einerseits *Privacy* und gewünschte Anonymität der Nutzer ausdrücklich als Ziele deklariert [TIN2_96], andererseits wird implizit mehr Vertrauen von Nutzern in Erbringer vorausgesetzt als umgekehrt. Es ist jedoch zu berücksichtigen, daß die Bearbeitung des Themas Sicherheit im Vergleich zu anderen Aspekten in TINA noch nicht sehr weit vorangeschritten ist und die vorliegenden Dokumente keine Spezifikationen sind, sondern nur den Status von *Technical Reports* oder *Engineering Notes* haben. Wir werden im weiteren vor allem die Implikationen der allgemeinen TINA-C Architektur für mehrseitige Sicherheit analysieren.

3.1 Anforderungen

In [MüPf_97] wird eine Strukturierung der Sicherheitsanforderungen für IT-gestützte Kommunikationssysteme entsprechend den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit vorgeschlagen, die auf mehrseitige Sicherheit abzielt. Diese berücksichtigt, den in [Pfit_93] formulierten technischen Datenschutzanforderungen an öffentliche Mobilfunknetze folgend, insbesondere den Aspekt der Teilnehmermobilität in modernen Kommunikationsnetzen. Ausgehend von dieser Gliederung postulieren wir im weiteren detaillierte Anforderungen mehrseitiger Sicherheit für TINA. Dabei berücksichtigen wir insbesondere folgende Aspekte:

- Mobilität der Konsumenten
- Vielfalt von Diensten
- Auswahl von angebotenen Diensten, von Verkäufern und von Anbietern durch die Nutzer (Subskriptionen)

[13] siehe Fußnote 3.

- Komplexe Steuerung der Dienstsitzungen durch die Nutzer
- Anpaßbarkeit der persönlichen Kommunikationsumgebung
- Mehrparteienkommunikation
- Teledienste, wie beispielsweise Informationsdienste (z.B. Veranstaltungspläne, Fahrpläne), Tele-Banking und Video-On-Demand
- Wettbewerb verschiedener Verkäufer und Dienstanbieter um Konsumenten und andere Dienstnutzer

Unsere Anforderungen sind unabhängig von den einzelnen Diensten. Sie sollen neben den klassischen Sicherheitszielen sicherstellen, daß kein Beteiligter ohne triftigen Grund in einer mächtigeren Position ist als die anderen Beteiligten. Einzelne Dienste können zusätzliche spezifische Anforderungen haben, denen dann innerhalb der Implementierung des Dienstes Rechnung getragen werden muß.

- **Vertraulichkeit** *(confidentiality)*

  c1 Inhaltsdaten von Diensten, d.h. Streams, sollen vor allen Instanzen außer den vorgesehenen Empfängern *(Stream consumers)* vertraulich bleiben. Empfänger und Erzeuger *(Stream producers)* der Streams können sein: Konsumenten, Verkäufer, Diensteanbieter.

  c2 Verbindungen für Inhaltsdaten, d.h. Stream bindings, dürfen nicht durch Unbeteiligte, einschließlich Verbindungsanbieter, beobachtbar sein. Dies betrifft Beteiligte, Datenumfang, Dienstqualitäten, Zeitpunkt und Dauer der Verbindung.

  c3 Steuerungsdaten von Diensten sollen vor allen Instanzen, außer den an dem Steuerungsvorgang beteiligten Nutzern und Erbringern, vertraulich bleiben.

  c4 Nutzer sollen anonym bleiben können, soweit dies durch Inhalt und Struktur des Dienstes toleriert werden kann. Der Nutzer eines Dienstes muß vor dem Erbringer anonym bleiben können. Außerdem müssen bei Kommunikationsdiensten die beteiligten Konsumenten voreinander anonym bleiben können.

  c5 Niemand darf ohne Einwilligung des Konsumenten dessen momentanen Ort ermitteln können. Dies schließt ein: Verkäufer, Dienstanbieter, Verbindungsanbieter und andere Konsumenten, inklusive momentane oder zukünftige Kommunikationspartner.

  c6 Die persönliche Kommunikationsumgebung eines Nutzers ist vertraulich. Sie darf nicht ausgeforscht werden können. Dies betrifft alle Information im Nutzerprofil (siehe Abschnitt 2.3) und die Subskriptionen des Nutzers für einzelne Dienste.

- **Integrität** *(integrity)*

  i1 Fälschungen von Inhaltsdaten von Diensten, einschließlich Absender, werden erkannt. Unter Fälschung werden auch Verzögerungen, Wiedereinspielen, Unterdrücken oder Änderung der zeitlichen Reihenfolge von Nachrichten verstanden.

i2 Fälschungen von Steuerungsdaten von Diensten, einschließlich Absender, werden erkannt. Unter Fälschung werden auch Verzögerungen, Wiedereinspielen und Unterdrücken von Nachrichten im Rahmen komplexer Aktivitäten zur Steuerung von Diensten mit potentiell mehr als zwei Beteiligten verstanden.

i3 Die persönliche Kommunikationsumgebung eines Nutzers darf nicht unautorisiert verändert werden können. Dies betrifft alle Information im Nutzerprofil und die Subskriptionen des Nutzers für einzelne Dienste.

- **Verfügbarkeit** *(availability)*

a1 Die subskribierten Dienste müssen einem Nutzer zu den vereinbarten Bedingungen jederzeit, soweit nicht anders vereinbart, zur Verfügung stehen.

a2 Behinderungen des Zugangs eines Beteiligten zu Diensten eines anderen Beteiligten durch einen dritten Beteiligten müssen festgestellt werden.

- **Zurechenbarkeit** *(accountability)*

z1 Der Empfänger von Inhaltsdaten eines Dienstes soll einem Dritten gegenüber nachweisen können, daß der Sender die Nachricht gesendet hat.

z2 Der Sender von Inhaltsdaten eines Dienstes soll einem Dritten gegenüber nachweisen können, daß der Empfänger die Nachricht erhalten hat, mindestens jedoch, daß er sie an den Empfänger abgeschickt hat.

z3 Kein Nutzer darf einem Erbringer das vereinbarte Entgelt für die Nutzung von Diensten vorenthalten können, zumindest erhält der Erbringer bei der Nutzung entsprechende Beweismittel. Umgekehrt kann der Erbringer nur Entgelt für entsprechend der Subskription erbrachte Dienste fordern, für die er die entsprechenden Beweismittel vorweisen kann.

Die TINA-Architektur, speziell die Sicherheitsarchitektur, sollte idealerweise diese Anforderungen so unterstützen, daß die Erfüllung von allen Beteiligten, einschließlich Konsumenten, überprüfbar ist, wie in der grundlegenden Arbeit zu mehrseitiger Sicherheit in diensteintegrierenden Kommunikationsnetzen [Pfit_90] gefordert. Im folgenden präsentieren wir den bisherigen Stand der Spezifikation zum Thema Sicherheit und analysieren danach mögliche Bedrohungen.

3.2 Stand der Spezifikation

Die vorliegende TINA-Sicherheitsarchitektur [TIN2_96] unterteilt die Sicherheitsproblematik in die Gebiete Telekommunikationssysteme und -dienste, Managementsysteme, DPE und Sicherheitsmanagement (siehe [WSWZ_97]). Sie geht davon aus, daß das DPE Sicherheitsdienste zur Verfügung stellt, die dann von den, auf dem DPE implementierten, verteilten Anwendungen, d.h. Telekommunikation und Management, benutzt werden. Es wird nahe gelegt, daß das DPE die im Sicherheitsteil des OSI-Referenzmodells [ISO_89] definierten Sicherheitsdienste zu den Gebieten Authentikation, Zugriffskontrolle, Integrität, Vertraulichkeit und Nichtabstreitbarkeit sowie die dafür nötigen Sicherheitsmechanismen enthält. Die Anwendung der Sicherheitsdienste ist nicht näher spezifiziert. Vielmehr wird eine Vorgehensweise beschrieben, wie Dienstentwickler unter Benutzung der vom DPE zur Verfügung gestellten Sicherheitsdienste Sicherheit in TINA Dienste integrieren sollen. Diese besteht aus den Phasen: Abschätzung von Bedrohungen, Angriffspunkten und Risiken, Auswahl von Sicherheitsdiensten, Zuordnung der Sicherheitsdienste zu Schichten, Auswahl von Sicherheitsmechanismen, Auswahl von Algorithmen und letztlich Festlegung von IDL-Schnittstellen für Sicherheitsprotokolle. So vorgehend, sollen dann die Entwickler von TINA Diensten (Kommunikations-, Informations- und Managementdienste) Sicherheit in ihre verteilten Anwendungen integrieren.

Die Entwicklung der DPE-Sicherheitsdienste steht noch aus. Zu erwarten ist eine Adaption der CORBA-Spezifikationen zum Thema Sicherheit [OMG1_95] als Teil der Adaption von CORBA als DPE. Für den Einsatz in TINA sind insbesondere noch folgende Fragen zu klären: die Sicherheit von Interaktionen über die Grenzen von Sicherheitsdomänen und Sicherheitstechnologien hinweg sowie ein globales und unabhängiges Schlüsselmanagement. Diese Probleme werden wir im Rahmen eines Projektes bearbeiten. Nach ihrer Lösung lassen sich die klassischen Anforderungen c1, c3, i1, z1 und z2 durch Benutzung der DPE-Sicherheitsdienste erfüllen. Die Gewährleistung der Sicherheit innerhalb einer Domäne, die ja im allgemeinen Fall selbst nicht auf einen Knoten beschränkt ist, ist damit ebenfalls realisierbar.

3.3 Bedrohungen

Die Anforderungen c2, c4, c5, c6, i2, a1, a2 und z3 lassen sich nicht allein durch die Anwendung der vorgesehenen Sicherheitsdienste des DPE erfüllen. Auch nach der Erfüllung der klassischen Anforderungen existieren noch Bedrohungen der Interessen von Beteiligten. Im folgenden präsentieren wir eine, nach den nicht erfüllten Anforderungen gegliederte, Liste von Bedrohungen.

c2 Die Verbindungen zwischen Beteiligten können beobachtet werden. Der Dienstanbieter kennt als Erbringer der Dienstlogik (SSM) alle Kommunikationssitzungen der Dienstsitzung und damit alle mit ihr zusammenhängenden Verbindungen. Der Verbindungsanbieter erfährt als Parameter (Logical Connection Graph) indirekt die Beteiligten und die Dienstqualitäten. Die Beteiligten kann er aus den im LCG enthaltenen Referenzen der Endpunkte ableiten. Er kennt auch vollständig Datenumfang, Zeit und Dauer der von ihm hergestellten Verbindungen. Auch ein Unbeteiligter, der die Referenzpunkte des Verbindungsanbieters abhört, kann, auch bei End-zu-End-Verschlüsselung der Inhalte, möglicherweise Verbindungen erfahren. Dies kann entweder durch Auswertung der Adreßinformation der einzelnen Pakete des Streams[14] auf unteren Protokollebenen (z.B. bei ATM-Übertragungstechnik), durch inhaltlichen Vergleich der Schlüsseltexte und/oder durch zeitliche Verknüpfung von Datenübertragungen festgestellter Größe geschehen.

c4 Der Erbringer eines Dienstes kommuniziert direkt über operationelle Interfaces mit der Domäne des Nutzers. Aus den dafür nötigen Referenzen der Dienstkomponenten in der Nutzerdomäne (PA und UAP) kann auf die Nutzerdomäne geschlossen werden. Aus der Nutzerdomäne kann der Erbringer durch Auswertung der Zuordnung von Beteiligten zu dieser Domäne bei früheren Dienstnutzungen möglicherweise auf den als Nutzer

[14] Bei den Verbindungen zwischen Stream Interfaces handelt es sich, wie schon erwähnt, um Abstraktionen der Übertragungstechnik aus Sicht der Dienste.

agierenden Beteiligten schließen. Ein Kommunikationspartner kann durch Auswertung der Referenzen zu den Stream Interfaces des Kommunikationspartners oder der Adreßinformation der Pakete des Streams möglicherweise auf das Endgerät des Kommunikationspartners und daraus möglicherweise auf den Partner selbst schließen.

c5 Aus den im Nutzerprofil enthaltenen Informationsobjekten Nutzungskontext und Registrierungen läßt sich der momentane Aufenthaltsort des Nutzers ermitteln. Der Nutzungskontext enthält im Falle einer bestehenden Zugangssitzung die Zuordnungen des Nutzers zu einem Endgerät und des Endgerätes zu einem Netzzugangspunkt. Eine Registrierung kann angeben, an welches Endgerät eine Einladung zu einer Dienstsitzung ausgeliefert werden soll[15]. Aus der Zuordnung des Endgerätes zu einem Netzzugangspunkt läßt sich der Ort des Endgerätes bestimmen, bei immobilen Endgeräten exakt, bei mobilen Endgeräten bis zur Genauigkeit der Größe des Empfangs- und Sendebereiches des Netzzugangspunktes. Der präskriptive Teil der Dienstarchitektur schreibt nicht vor, in welcher Weise das Nutzerprofil auf Computational Objects abgebildet wird. Im deskriptiven Teil wird jedoch eine Implementierung als Teil des namedUA in der Erbringerdomäne nahegelegt (siehe folgenden Abschnitt 4.1). In diesem Fall kann der Verkäufer vollständige Bewegungsprofile des Konsumenten erstellen. Beteiligte an einer Dienstsitzung können den Ort eines Nutzers erfahren, indem sie Referenzen der Interfaces oder Adreßinformation unterer Protokollschichten auswerten (siehe oben).

c6 Die persönliche Kommunikationsumgebung eines Nutzers ist dem Erbringer legitimerweise bekannt. Andere Beteiligte können durch systematisches Einladen des Nutzers zu Dienstsitzungen der vom Erbringer angebotenen Dienste und Auswertung der entsprechenden Reaktionen dessen Subskriptionen ausforschen.

i2 Komplexe Aktivitäten zur Dienststeuerung, wie z.B. das Unterbrechen einer gesamten Dienstsitzung mit all ihren Beteiligten (Beispiel Video-Konferenz), sind mit der Übertragung vieler Nachrichten zwischen den Domänen vieler Beteiligter verbunden. Auch bei Verschlüsselung der einzelnen Nachrichten besteht die Möglichkeit, daß ein aktiver Angreifer durch Abfangen von Nachrichten die Steuerung in seinem Sinne beeinflussen kann.

a1 Ein aktiver Angreifer auf die Übertragungswege zwischen Nutzer und Erbringer kann durch Abfangen oder Modifizieren der übertragenen Daten die Nutzung von Diensten sabotieren.

a2 Der Betreiber des Kernel Transport Network[16] könnte alle Nachrichten zu fremden Erbringern abfangen und nur Nachrichten zu bestimmten, mit ihm liierten, Erbringern an ihr Ziel kommen lassen. Diese Art Angriff kann auch unvollständig erfolgen. Sie führt zu nicht zufriedenstellender Diensterbringung und hat damit geschäftsschädigende Wirkung auf den betroffenen Erbringer. Auf ähnliche Weise kann auch der Zugang zum Vermittler als Lieferanten von Referenzen konkurrierender Erbringer sabotiert werden.

[15] In [EMPS_96] ist im Interesse größerer Flexibilität bei der Auswahl eines passenden Terminals eine weitere Stufe bei der Zuordnung vorhanden. Hier ist die Zuordnung für Registrierungen: Nutzer zu Lokation und Endgeräte zu Lokation. Der Ort ist also sogar direkt als Datum im Nutzerprofil vorhanden.

[16] Der Betreiber des KTN ist im Geschäftsmodell nicht als eigener Beteiligter definiert, vermutlich, weil der Transport der Nachrichten zu den operationellen Interfaces als gratis (vergleichbar Signalisierung in existierenden Netzen) angenommen wird. Zu erwarten ist, daß der Verbindungsanbieter auch dieses Netz betreibt. (u.U. sind beide nur logisch voneinander getrennt.)

z3 Erbringer können bei der Berechnung des Entgelts im Interesse höherer Einnahmen gefälschte Parameter der tatsächlichen Dienstnutzungen (z.B. Dauer von Verbindungen oder übertragene Datenmenge) angeben.

Die Liste von Bedrohungen erhebt keinen Anspruch auf Vollständigkeit. Sie illustriert jedoch, daß im Rahmen der bisherigen allgemeinen Architektur in TINA und der Anwendung der bisher in der Sicherheitsarchitektur vorgesehenen Sicherheitsdienste nicht zwangsläufig die Anforderungen mehrseitiger Sicherheit erfüllt sind. Im folgenden präsentieren wir erste Ansätze zum Erreichen dieses Ziels.

4 Ansätze für mehrseitige Sicherheit

Leitlinien dieser Ansätze sind die Rückgabe der logischen und physischen Kontrolle von Information und Funktionalität an den davon Betroffenen und die Aufteilung nötigen Vertrauens auf mehrere, voneinander unabhängige, Parteien. Mittel sind die Verlagerung der Vertrauensgrenzen auf die Domängrenzen und die Erhöhung des technischen Aufwandes für die Analyse von Kommunikationsverhalten durch die Verknüpfung festgestellter einzelner Übertragungen.

4.1 Allokation

Die TINA Sicherheitsarchitektur [TIN3_96] geht von der Annahme aus, daß sich die Objekte innerhalb einer Domäne gegenseitig vertrauen. Zwischen den Domänen wird kein Vertrauen per se angenommen. Dieser Annahme muß zur Erfüllung der Anforderungen c5 und c6 hinsichtlich des Nutzerprofils entsprochen werden. Bisher ist das nicht der Fall. Das Informationsobjekt Nutzerprofil ist mit seinen zugehörigen Informationsobjekten Nutzungskontext, Dienstprofile, Sitzungsbeschreibungen und Registrierungen auf den namedUA abgebildet. Der präskriptive Teil der Dienstearchitektur siedelt den namedUA in der Erbringerdomäne an (Abbildung 3). Im deskriptiven Teil wird eine Implementierung des namedUA als CO Group vorgeschlagen. Abbildung 4 zeigt die Zusammensetzung des namedUA aus den einzelnen Computational Objects.

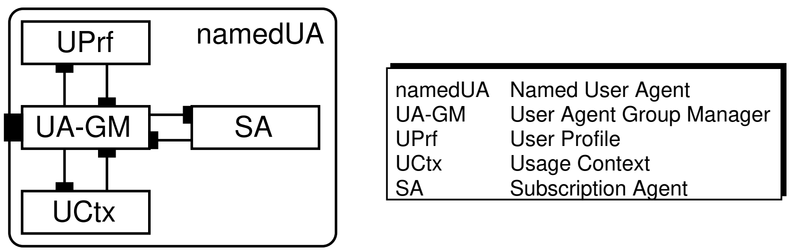


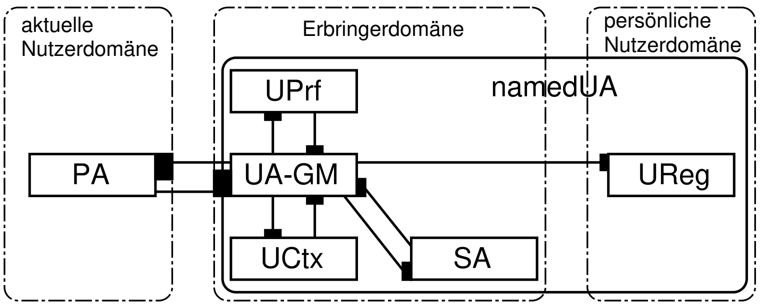
Abbildung 4: Der UA als CO Group

Der UA-GM stellt nach außen die Interfaces des namedUA[17] (siehe Abschnitt 2.4) als *contracts* (siehe [WSWZ_97]) zur Verfügung. Im Falle einer bestehenden Zugangssitzung des Nutzers ist

[17]Der Aufbau des anonUA ist bisher nicht vorgeschlagen worden. Es ist eine ähnliche Struktur wie beim namedUA vorstellbar, wobei jedoch alle Information im anonUA nur die maximale Lebensdauer einer Zugangssitzung hat.

er verantwortlich für die Kooperation mit dem PA in der aktuellen Domäne des Nutzers. Das CO UCtx enthält die Zuordnung des Nutzers zu einem Endgerät und die Zuordnung dieses Endgerätes zu einem Netzzugangspunkt für die bestehende Zugangssitzung. Innerhalb der Erbringerdomäne interagiert der UA-GM mit SF, SSM und USM. Außerdem hält er die Liste der Registrierungen. Registrierungen sind noch Gegenstand der Entwicklung. Im einfachsten Fall, wie zur Zeit im deskriptiven Teil der Dienstearchitektur, bedeutet eine Registrierung die Auswahl eines Endgerätes in Abhängigkeit von einer Bedingung. An dieses Endgerät werden dann Einladungen ausgeliefert. In weitergehenden Entwicklungen [EMPS_96] realisieren die Registrierungen ein Erreichbarkeitsmanagement (vergleiche [DFRR_97]) mit zusätzlicher Auswahl eines Endgerätes. Das CO UPrf dient dem Management der vom Nutzer bestimmten Anpassungen und Einstellungen der Dienstauslieferung. Der SA ist verantwortlich für die nutzerspezifische Information über seine Subskriptionen von Diensten.

In dem vorgeschlagenen Entwurf in TINA enthält der UA-GM die mehr oder weniger frei vom Benutzer programmierbare, ebenfalls rein private Information, wie auf Einladungen zu Dienstsitzungen reagiert werden soll. Im Interesse der Erfüllung der Anforderung c5 allozieren wir die Registrierungen in der Nutzerdomäne. In Anlehnung an [EMPS_96] sind die Registrierungen und die Funktionalität zu ihrer Auswertung in einem selbständigen Computational Object enthalten, dem CO UReg *(User Registrations).* Dieses CO allozieren wir in der persönlichen Domäne des Nutzers. Abbildung 5 zeigt die Allokation und die Beziehung des UA zu persönlicher und aktueller Domäne des Nutzers.



namedUA	Named User Agent	UPrf	User Profile	PA	Provider Agent
UA-GM	User Agent Group Manager	UCtx	Usage Context	UReg	User Registration
		SA	Subscription Agent		

Abbildung 5: Die Allokation der Registrierungen

In zwei Fällen finden Interaktionen zwischen UA-GM und UReg statt, bei Einladungen zu Dienstsitzungen oder zum Setzen von Registrierungen. In beiden Fällen führt der UA-GM Operationen des UReg aus, die von dessen entsprechenden operationellem Interface angeboten werden. Im ersten Fall wird die mit der Einladung verbundene Information als Parameter mit übergeben. In der Nutzerdomäne wird vom CO UReg die Annahme der Einladung durch Auswertung der Registrierungen entschieden und im Fall der Annahme wird die Adresse eines Endgerätes geliefert. Für die Einladungen wird vom UReg eine Authentikationsprüfung des Datenursprungs vorgenommen, wodurch, ein unabhängiges Schlüsselmanagement vorausgesetzt, der Erbringer gehindert wird, durch fingierte Einladungen die Registrierungen auszuforschen. Das Registrieren, d.h. Setzen der Registrierungen, ist von anderen Nutzerdomänen aus möglich. Authentizität, Integrität und Vertraulichkeit der entsprechenden Daten werden durch End-zu-End-Verschlüsselung zwischen aktueller Nutzerdomäne und persönlicher Nutzerdomäne gewährleistet. Der UA-GM leitet die entsprechenden Nachrichten lediglich zum UReg weiter. Regelmäßiges Neuregistrieren verhindert, daß der Erbringer durch Ausbleiben neuer Registrierungen auf den Verbleib des Nutzers am alten, dem Erbringer von der letzten angenommenen Einladung bekannten, Ort schließen kann. Die Unterschiedlichkeit der Schlüsseltexte wird durch Auffüllen des Klartextes mit Zufallszahlen garantiert. Die Absendedomäne der Registrierungen, d.h. der momentane Ort des Nutzers, wird durch die Anwendung anderer Sicherheitsmechanismen, z.B. Mixe, verborgen.

Das Konzept setzt die Existenz einer persönlichen Nutzerdomäne für jeden Nutzer voraus. Diese Domäne ist der Vertrauensbereich des Nutzers, den er dauerhaft physisch unter seiner Kontrolle hat, siehe auch [Walk94] [DFRR_97]. Die momentane Nutzerdomäne muß nicht mit seiner persönlichen Nutzerdomäne identisch sein (persönliche Mobilität). Im privaten Einsatzbereich ist die persönliche Nutzerdomäne durch das oder die Endgeräte des Nutzers in seiner Wohnung realisierbar. Im Organisationsbereich ist diese einfache Lösung in der Regel nicht ausreichend, da keine Nutzerdomäne unter der Kontrolle des Nutzers steht. Hier sind mehrere Lösungen denkbar. Erstens, der einzelne Nutzer kann dasselbe CO UReg verwenden wie im privaten Leben. Zweitens, die COs UReg der Nutzer sind in unabhängig administrierten und physisch gesicherten, z.B. verplombten, Geräten oder Räumen alloziert. Drittens, die URegs werden als nicht änder- oder auslesbare Hardware realisiert. Die Untersuchung dieser Alternativen ist Gegenstand unserer weiteren Arbeiten, ebenso die Integration der Zugriffskontrolle im Anwendungskontext (siehe oben) in das Zugriffskontrollsystem des DPE.

4.2 Pseudonyme

Ein wichtiges Problem für den Datenschutz stellt die Identifikation von Benutzern dar. Oft möchte ein Benutzer für die Inanspruchnahme eines Dienstes nicht seine tatsächliche Identität preisgeben, sondern er möchte Dienste, z.B. Beratungsdienste, anonym nutzen. Da eine anonyme Nutzung oft Probleme hinsichtlich der Verbindlichkeit aufwirft, ist eine Zwischenlösung basierend auf Pseudonymen wünschenswert. Hier authentisiert sich der Benutzer gegenüber einer vertrauenswürdigen dritten Instanz und erhält von dieser ein Pseudonym samt Beglaubigung (Credential). Mit diesem Pseudonym kann der Benutzer sich nun einer anderen Instanz gegenüber authentisieren, ohne daß diese Instanz eine Information über die tatsächliche Identität des Benutzers erhält. Im Falle eines Disputes kann sich jeder an die vertrauenswürdige Instanz wenden, die dann nach einer unabhängigen Prüfung des Sachverhaltes die Verbindung zur tatsächlichen Identität des Benutzers wieder herstellen kann. Ein Protokoll für Benutzerpseudonyme könnte in TINA relativ einfach realisiert werden. Der Pseudonymitätsdienst als Zugangsdienst würde, anders als das Konzept des anonUA, die langfristige Nutzung einer den Wünschen des Benutzers angepaßten Kommunikationsumgebung sowie die Möglichkeit, zu Dienstsitzungen eingeladen zu werden, eröffnen.

4.3 Weitere Ansätze

Die Anforderung i2 läßt sich durch kryptographische Verkettung der einzelnen Interaktionen im Rahmen einer Sitzung erfüllen. Sowohl im Kernel Transport Network als auch bei den

Verbindungen über die Stream Interfaces lassen sich Mixe [Pfit_90] einsetzen. Dies dient der Erfüllung der Forderungen c2, c4, c5 sowie a2 und bewirkt die Aufteilung der Information über Kommunikationsverbindungen auf mehrere unabhängige Parteien, so daß der Nutzer nicht vollständig einem Transporteur vertrauen muß. Durch Einsatz von Mixen läßt sich auch verhindern, daß der Erbringer bei Annahme einer Einladung und bei bestehenden Zugangssitzungen den Nutzungskontext, d.h. den Aufenthaltsort, des Nutzers erfährt. Bei einem entsprechenden Ansatz enthält der Nutzungskontext des Nutzers (CO UCtx) beim Erbringer die persönliche Domäne dieses Nutzers. Diese enthält den tatsächlichen Nutzungskontext und stellt die zusätzliche, geschützte, Verbindung zwischen Nutzer und seiner persönlichen Nutzerdomäne her. Den Bedrohungen a1 und a2 kann durch mehrfache Auslegung von Netzverbindungen mit alternativem Routing, Verbergen von Sender und Empfänger vor dem Transporteur und durch regelmäßiges Senden von getarnten Probenachrichten entgegengewirkt werden. Anforderung z3 kann durch unabhängige Intelligenz in den Endgeräten gekoppelt mit Online-Bezahlung in kleinen Summen unterstützt werden, wobei jede Abbuchung oder Forderung sofort vom Nutzer hinsichtlich ihrer Berechtigung geprüft wird.

5 Ausblick

Die Telecommunications Information Networking Architecture wird bei Erfüllen der in sie gesetzten Erwartungen den umfassenden Rahmen für die Kommunikation und Information in elektronischer Form für Organisationen und Haushalte bilden. Unabdingbar für die gesellschaftliche und kommerzielle Akzeptanz ist der Schutz teilnehmerbezogener Daten vor Mißbrauch und der Schutz von Anbietern gegen jede Art von Behinderung durch Konkurrenten. Die technische Umsetzung dieses Schutzes bedeutet die Anwendung der Prinzipien mehrseitiger Sicherheit auf TINA. Die Sicherheitsarchitektur, wie bisher in TINA ausgearbeitet, sollte deswegen so erweitert werden, daß die Anforderungen mehrseitiger Sicherheit erfüllt werden. Die Allokation von Information und Funktionalität ist dafür eine Grundvoraussetzung. Im Rahmen der CORBA- und TINA-Sicherheitsarchitekturen werden langfristig Sicherheitsdienste zur Erfüllung der klassischen Sicherheitsanforderungen bereitgestellt. Weitergehende Anforderungen im Interesse mehrseitiger Sicherheit lassen sich durch bekannte Konzepte erfüllen. Für die architektonische Einbettung müssen jetzt die Anstöße kommen, da die Festlegung der Spezifikationen in TINA schon weit vorangeschritten ist. Grundpfeiler muß ein von den kommerziellen Anbietern im TINA-System unabhängiges Schlüsselmanagement sein; dieses könnte von unabhängigen Vermittlern mit übernommen werden.

Literatur

[BaBI_93] Barr, William J.; Boyd, Trevor; Inoue, Yuji: The TINA Initiative. In: IEEE Communications Magazine März 1993. S.70-76.

[BeFG_95] Berndt, Hendrik; de la Fuente, Luis A.; Graubmann, Peter: Service and Management Architecture in TINA-C. International TINA Conference, Melbourne, Australia, 13.-16. Februar 1995. S.81-96.

[DFRR_97] Damker, Herbert; Federrath, Hannes; Reichenbach, Martin; Rannenberg, Kai: Persönliches Erreichbarkeitsmanagement. Beitrag in diesem Buch.

[EMPS_96] Eckardt, Tim; Magedanz, Thomas; Popescu-Zeletin, Radu; Schulz, Marco; Stapf, Michael: Personal Communications Support in the TINA Service Architecture -

A new TINA-C Auxiliary Project. TINA'96 Conference, Heidelberg, 3.-5. September 1996. S.55-64.

[GKGF_95] Görk, C.; Kleier, S.; Guntermann, M.; Fröhlich, M.; Bisseling, H.: A European Solution for Advanced UPT: Integration of Services for Personal Communication. International TINA Conference, Melbourne, Australia, 13.-16. Februar 1995. S.603-617.

[ISO_89] ISO/IEC 7498-2: Information Technology - Open Systems Interconnections - Basic Reference Model - Part 2: Security Architecture (auch ITU-T Recommendation X.800). Februar 1989.

[MüPf_97] Müller, Günter; Pfitzmann, Andreas: Mehrseitige Sicherheit - Antwort auf die Digitalisierung, Beitrag in diesem Buch.

[NiDC_95] Nilsson, Gunnar; Dupuy, Fabrice; Chapman, Martin: An Overview of the Telecommunications Networking Architecture. International TINA Conference, Melbourne, Australia, 13.-16. Februar 1995. S.1-12.

[OMG1_95] Object Management Group: CORBA Security. Dezember 1995.

[OMG2_95] Object Management Group: The Common Object Request Broker, Architecture and Specification, Revision 2.0. Juli 1995.

[Pfit_90] Pfitzmann, Andreas: Diensteintegrierende Kommunikationsnetze mit teilnehmerüber- prüfbarem Datenschutz. Berlin; Heidelberg; New York: Springer 1990.

[Pfit_93] Pfitzmann, Andreas: Technischer Datenschutz in öffentlichen Funknetzen. In: Datenschutz und Datensicherung 8/93. S.451-463.

[RBPE_91] Rumbaugh, James; Blaha, Michael; Premerlani, William; Eddy, Frederick; Lorensen, William: Object-Oriented Modeling and Design. Englewood Cliffs: Prentice-Hall 1991.

[TIN1_96] TINA-C Dokument TP_HC.012_3.2_96: Computational Modellling Concepts, Version 3.2. Mai 1996.

[TIN1_95] TINA-C Dokument TB_EAC.001_1.2_94: Information Modellling Concepts. April 1995.

[TIN2_95] TINA-C Dokument TB_MDC.018_1.0_94: Overall Concepts and Principles of TINA. Februar 1995.

[TIN3_95] TINA-C Dokument TB_MH.002_2.0_94: Requirements upon TINA-C Architecture. Februar 1995.

[TIN2_96] TINA-C Dokument TR_EGL.004_2.0_1996: Security Architecture, Version 2.0. März 1996.

[TIN3_96] TINA-C Dokument TB_RM.001_4.0_96: Service Architecture, Version 4.0. Oktober 1996.

[TIN4_95] TINA-C Dokument TR_NM.002_1.3_95: TINA Object Definition Language (TINA-ODL) Manual, Version 1.3. Juni 1995.

[Walk94] Walke, Bernhard: Technik-Akzeptanz und -Verträglichkeit von mobilen Kommunikationsnetzen. ITG-Fachtagung: Herausforderung Informationstechnik. 18.-20. Oktober 1994. VDE-Verlag.

[WSWZ_97] Wilhelm, Uwe G.; Staamann, Sebastian; Wolf, Gritta; Zoellner, Jan: Sicherheit in CORBA und TINA. Beitrag in diesem Buch.

[YOWK_95] Yagi, Hikaru; Ohtsu, Kazuyuki; Wakano, Masaki; Kobayashi, Hidetsugu; Minerva, Roberto: TINA-C Service Components. International TINA Conference, Melbourne, Australia, 13.-16. Februar 1995. S.113-124.