Echtzeitplattformen für eBusiness: Forschungsergebnisse aus dem EU-Projekt INTELLECT

Dipl.-Ing. Kai-Oliver Detken[1]

[1]Detken Consultancy & Internet Technologies (DECOIT)
Zu den Stauwiesen 18, D-28879 Grasberg
Fax: +49-4298-894547, Phone: +49-4298-894548
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Zusammenfassung

Das Forschungsprojekt Intelligent Online Configuration of Products by Customers of Electronic Shop Systems (INTELLECT) startete im Januar 2000 mit einer Laufzeit von zwei Jahren im IST-Programm der Europäischen Union (EU). Das Hauptziel dieses Projektes ist es vorhandene eCommerce-Systeme zusammenzuführen und sie mit einer neuen Oberfläche zu versehen, die Produkte (Waren und Güter) so realistisch wie möglich abbildet (3D-Darstellung). Die Ergebnisse des Projektes sollen sich dabei nicht nur auf eine bestimmte Produktart beschränken, sondern individuell anpassbar sein, um auch für andere Industriesektoren Relevanz zu besitzen. Interaktive Kommunikation und Konfiguration, animierte 3-D-Abbildungen, unterschiedlichen Wahlmöglichkeiten sowie schnelle Zugriffszeiten sind die weiteren Ziele des Projektes, die garantierte Dienstgüten erfordern. Dabei wird die Integration eines interaktiven Help-desk-Systems erfolgen, wodurch der Benutzer durch den eShop geführt wird. Geplant ist, dass der Kunde direkt über das Internet eine Verbindung zu dem E-Shop aufsetzen kann, sodass über Text-Chat, Videokommunikation oder VoIP[1] dem Kunden bei seiner Auswahl bzw. bei der Benutzung des Shops geholfen wird. Dabei ist neben einer Führung durch die Web-Seiten, auch eine Produktberatung über Video-Clips angedacht. Neben der Qualität spielt dabei auch die Sicherheit der Transaktionen eine wichtige Rolle. Durch das 3D-Modul werden die Produkte realistisch abgebildet und konfiguriert. Für die Konfiguration gibt es ebenfalls eine interaktive Hilfestellung.

1 Einleitung

Heutige Online-Shops bieten zahlreiche Produkte den Internet-Benutzern an. Dabei sind sie allerdings meist eine 1:1 Abbildung der vorhandenen Produktkataloge. Die Vorteile, die das Internet bietet werden meistens nicht genutzt. Statische 2D-Abbildungen, schlechter Fotoqualität, kurzer Textbeschreibung, komprimierten Videosequenzen/Sounddateien, lange Ladezeiten, unübersichtliche Darstellung lassen die Endbenutzer oft auf traditionelle Kataloge zurückgreifen, statt neue E-Commerce Medien zu nutzen.

[1] Voice-over-IP

Nahezu alle Shop-Systeme nutzen heute Datenbank-Managementsysteme, um alle relevanten Daten zu speichern und Zugriff auf Produkte, Bestellungen und andere Informationen zu erhalten. Dabei setzt man meist auf Standardschnittstellen zu den gegenwärtig vorhandenen Bestellsystemen, um diese in das E-Commerce System zu integrieren. Die Integration von neuen Standards, Protokollen und Sprachen (z.B. CORBA[2], ODBC[3], JDBC[4]) fällt somit leichter. Auf der anderen Seite haben viele Systeme den Nachteil, dass vorhandene Produktdaten in Formaten (z.B. CAD[5], ERP[6] oder PDM[7] Systeme) vorliegen, die sich nicht einfach auf neue Systeme umsetzen lassen. Hinzu kommen große Sicherheitslücken im Internet, die bislang eine untergeordnete Rolle gespielt haben, da es als reines Forschungsnetz genutzt wurde.

Um die Sicherstellung der Authentizität, Integrität und Vertraulichkeit der übertragenden Daten zu gewährleisten, werden symmetrische und asymmetrische Verschlüsselungsverfahren eingesetzt. Dabei werden die asymmetrischen Verfahren vor der eigentlichen Kommunikation verwendet, um für einen sicheren Austausch der Schlüssel zu sorgen. Anschließend findet dann eine symmetrische Verschlüsselung statt. Schlüssellänge und Kryptoverfahren sind dabei entscheidend für die Sicherheit der Daten verantwortlich. Hier muss man, aufgrund immer schneller Rechnertechnik, die Schlüssellänge erweitern bzw. exponentielle Verfahren einsetzen. Um sicherheitsrelevante Daten nach Außen abzusichern, sind die Daten auf der äußeren Netzebene ebenfalls nur in verschlüsselter Form vorhanden. Der eigentlich neue und zudem noch höchst aktuelle Aspekt ist die Sicherung von Internet-Diensten, wie z.B. die Übertragung sicherheitsrelevanter Daten von einem WWW-Browser zu einem WWW-Server. Das ist gerade beim Aufbau sicherer Intranets entscheidend. Hinzu kommt die Forderung nach sicheren Zahlungssystemen, um den Bereich Business-to-Customer abzusichern. Im Internet-Umfeld sind eine Vielzahl von Entwicklungen vorangetrieben worden, die sich speziell mit der Absicherung von Internet-Diensten beschäftigen. Dabei haben im Grunde alle Lösungen miteinander gemeinsam, dass sie auf keinen Standards beruhen bzw. sich nicht durchgesetzt haben.

Ein wesentlicher Punkt ist die Einfachheit der Bedienbarkeit bzw. die interaktive Hilfe, die momentan selten und wenn schlecht umgesetzt ist. Heutige E-Commerce Systeme scheitern häufig durch zu viele Links, die ein Benutzer benötigt, um letztendlich sein gewünschtes Produkt in den Warenkorb aufzunehmen. Beratend stehen ihm höchsten Chat-Applikationen oder E-Mail zur Seite. Wesentlich verbesserte Interaktion ermöglichen direkte VoIP-Verbindungen und/oder Videokommunikation in ausreichender Qualität. Die Einhaltung der Qualität ist dabei allerdings durch zu geringe Bandbreiten, inhomogene Netze und fehlende QoS[8]-Mechanismen im Internet bislang nicht möglich. Hier müssen Echtzeitplattformen unter Berücksichtigung von Standards aufgebaut werden, die ausreichende Ressourcen garantieren können. Dieser Beitrag geht auf Lösungsansätze ein, die im Rahmen des EU-Projekts u.a. untersucht wurden und implementiert werden sowie weiterreichende Möglichkeiten um Echtzeitqualitäten sowie die Sicherheit für eBusiness-Prozesse zu garantieren. [DeFi00]

---

[2] Common Object Request Broker Architecture

[3] Open DataBase Connectivity

[4] Java DataBase Connectivity

[5] Computer-Aided Design

[6] Enterprise Resource Planning

[7] Product Data Modelling

[8] Quality-of-Service

2 Problemstellung

Die Laufzeitschwankungen im Internet lassen sich bislang nicht vorhersehbar beherrschen. Aufgrund der chaotischen Struktur sind Überbelastungen einzelner Netzknoten an der Tagesordnung. In diesem Fall würden die Datenpakete verworfen und später noch einmal angefordert werden. Das ist bei Sprachverkehr nicht tragbar. Höhere Bandbreiten lösen kurzfristig dieses Problem, haben aber keinen direkten Einfluss auf Jitter, Verzögerungen und Komprimierungsverfahren. Hinzu kommt, dass das Internet einem enormen Wachstum unterworfen ist, wodurch neue Standleitungen und Backbones nach relativ kurzer Zeit wieder die volle Auslastungskapazität fahren. Aus diesem Grund müssen andere Wege gefunden werden, um das Netz besser auszunutzen und Ressourcen sowie Laufzeiten garantieren zu können.

Das Protokoll RSVP[9] ist ein erster Ansatz hierzu. RSVP muss allerdings für jede Verbindung vom Netz angefordert werden, wodurch sich dies ungünstig auf die Gesamtleistung des Netzes auswirken kann. Zusätzlich ist es unklar wie das Netz reagiert, wenn eine große Menge von Teilnehmern RSVP nutzt. Außerdem müssen alle Router auf einem Verbindungspfad RSVP sprechen. Router, die das Protokoll nicht unterstützen, müssen getunnelt werden, was wieder zu neuen Schwachstellen führt. Das heißt, das Netz kann letztendlich die angeforderten Ressourcen verweigern oder diese während einer bestehenden Verbindung zurückfordern. Bei vorhersehbaren Routen durch das Netz lässt sich aber auch mit der jetzigen Form von RSVP und der Realisierung in den Routern (vornehmlich Cisco) die Qualität der Sprachübertragung erhöhen. [BZB+97]

VoIP ist aus Gründen der Laufzeiten und Komprimierung sowie der Dienstintegration von mehreren Faktoren stark abhängig, wenn es erfolgreich eingeführt werden soll:

- Bandbreiten im Backbone des Internet
- Quality-of-Service
- Effiziente Komprimierungsalgorithmen
- Verwendung des gleichen und kürzesten Datenpfades beim Routing
- Integration geeigneter Managementtools
- Billing & Accounting
- Integration in herkömmliche TK-Netze und Web-Szenarien

Diese Anforderungen sind heute noch nicht erfüllt oder nur teilweise umgesetzt worden. Zur Integration von VoIP in bestehende TK-Infrastrukturen und zur Implementierung in Web-Systeme bzw. in die Internet-Umgebung müssen diese Problematiken allerdings noch umgesetzt werden.

Hinzu kommt, dass auch bei VoIP unterschiedliche Herstelleransätze vorhanden sind, je nachdem aus welchem Markt der Hersteller ursprünglich stammt, und verschiedene Standards um die Vorherrschaft kämpfen bzw. noch nicht endgültig verabschiedet sind. Die von der ITU[10] entwickelte Protokollfamilie H.323 ist nicht hundertprozentig für VoIP geeignet, da sie nur wenige Komfortfunktionen definiert und mit mobilen Telefonen mit dynamisch zugeord-

[9] Resource Reservation Protocol, RFC-2205

[10] International Telecommunication Union

neten IP-Adressen nicht zurecht kommt. Aus diesem Grund hat die IETF[11] das Session Initiation Protocol (SIP) als Alternative zu H.323 entwickelt. Es ist Kern einer Familie von Spezifikationen, die die Kommunikation zwischen VoIP-Endgeräten und den sogenannten Gatekeepern festlegt. Hinzu sind weitere Merkmale definiert worden, wie die Interaktion mit unterschiedlichen Gateways und das Media Gateway Control Protocol (MGCP), welches Kontrollfunktionen übernimmt. Welche Alternative sich durchsetzen wird, ist bislang unklar. [RoSc00]

Weiterhin bestehen noch Lücken in den Spezifikationen, die zudem noch nicht alle endgültig verabschiedet sind. Dadurch sind die Hersteller nicht gezwungen auf die gleichen Standards bzw. Ansätze zu setzen, wodurch immer wieder die Kompatibilität und Interoperabilität unterschiedlicher Systeme leidet. Auch diese Probleme müssen angegangen werden, wenn man nicht in die gleichen Engpässe wie in der herkömmlichen TK-Welt geraten möchte.

3 Echtzeitintegration

Um eine Echtzeitplattform zu schaffen, die die Hauptkriterien Security, definierte Qualitätsgüte und Einsatz von Echtzeitapplikationen wie VoIP erfüllt, müssen die genannten Probleme kompensiert werden. Das heißt, es sollte zuerst eine sichere Kommunikationsplattform auf Basis eines Virtual Private Networks (VPN) geschaffen werden. Anschließend ist die Anforderung der garantierten Dienstgüte umzusetzen, die Echtzeitapplikationen sowie sensitive Datendienste unterstützt. Zuletzt können dann Echtzeitdienste wie VoIP integriert werden, ohne die Qualität und die Sicherheit unbeachtet zu lassen.

3.1 Security

Gerade im Bereich E-Business und E-Commerce ist die Sicherheit eines der wichtigsten Kriterien, damit sich solche Lösungen am Markt etablieren können. Um eine sichere Umgebung zu schaffen sind bestimmte Anforderungen zu beachten bzw. ist die notwendige Infrastruktur aufzubauen. Hinzu kommt der Einsatz von Echtzeitanwendungen wie Voice-over-IP (VoIP), die weitere Eigenschaften beinhalten, die überdacht werden müssen. Zwar gelten auch hier die allgemeinen Anforderungen an die Informationssicherheit. Darüber hinaus macht allerdings die Einführung verteilter Systeme und der Einsatz von Netzwerken und Kommunikationseinrichtungen zur Übertragung von Daten (inkl. Sprachdaten) zwischen Anwender und Computer sowie zwischen den Rechnern Maßnahmen zum Schutz der Daten während der Übertragung erforderlich (Computer- und Netzwerksicherheit).

Dabei wird auf folgende Hauptanforderungen Rücksicht genommen:

- **Vertraulichkeit:** Der Schutz der übertragenen Daten vor unbefugter Kenntnisnahme Dritter muss gewährleistet werden.
- **Authentizität:** Eine Mitteilung muss auf Echtheit, Zuverlässigkeit und Glaubwürdigkeit überprüfbar sein.
- **Integrität:** Die Unversehrtheit bzw. Unverfälschtheit von Nachrichten wird durch die Integrität beschrieben.

[11] Internet Engineering Task Force

- **Verbindlichkeit:** Hier wird der Sender oder Empfänger einer Nachricht daran gehindert zu leugnen, dass er die Nachricht gesendet bzw. erhalten hat.
- **Verfügbarkeit:** Die Zugriffssteuerung muss für die Beschränkung oder die Freigabe auf den Zugriff auf Systeme und Anwendungen über Kommunikationsverbindungen definiert werden. [Gore99]

Zur Schaffung einer sicheren Kommunikationsplattform af Basis eines VPN wird als gemeinsamer Nenner das Protokoll IP Security (IPsec) verwendet, welches von der IETF seit 1998 spezifiziert vorliegt und eine sichere Internet-Architektur bereitstellen möchte. Grundlage dieser Spezifikation bildet die Spezifikation RFC-2401. Dabei hat sich die IP Security Protocol Working Group der IETF zur Aufgabe gemacht, Richtlinien für mögliche Implementierungen von IPsec für Hard- und Softwarehersteller zu erstellen und auch zu pflegen. Der Vorschlag legt fest, auf welche Weise Authentifizierung und Verschlüsselung auf der IP-Schicht einzurichten sind. Firewalls, die sich an diese Spezifikation halten, können untereinander chiffrierte Daten austauschen, auch wenn sie von unterschiedlichen Herstellern stammen und verschiedene Verschlüsselungsverfahren verwenden. Dies war bislang nicht möglich, da es sich immer um proprietäre Lösungen handelte.

IPsec ist ein Layer-3-Protokoll, d.h. basierend auf dem OSI-Referenzmodell ist IPsec als Erweiterung von IP in der dritten Schicht, also der Vermittlungsschicht anzusiedeln. Die Abb. 1 zeigt dabei die Zuordnungen zwischen OSI-Modell und TCP/IP-Referenzmodell, sowie die grobe Einordnung des IPsec Protokolls. Dabei ist es besonders wichtig darauf hinzuweisen, dass IPsec nur die reine Datenübermittlung schützen kann, die Daten auf dem Quell- und Zielrechner aber unverschlüsselt vorliegen. Damit arbeitet IPsec unabhängig von der jeweiligen Anwendung und deren Verschlüsselungsmethoden. Für den weiteren Schutz der Daten sind dann wiederum Anwendungsprogramme zuständig.

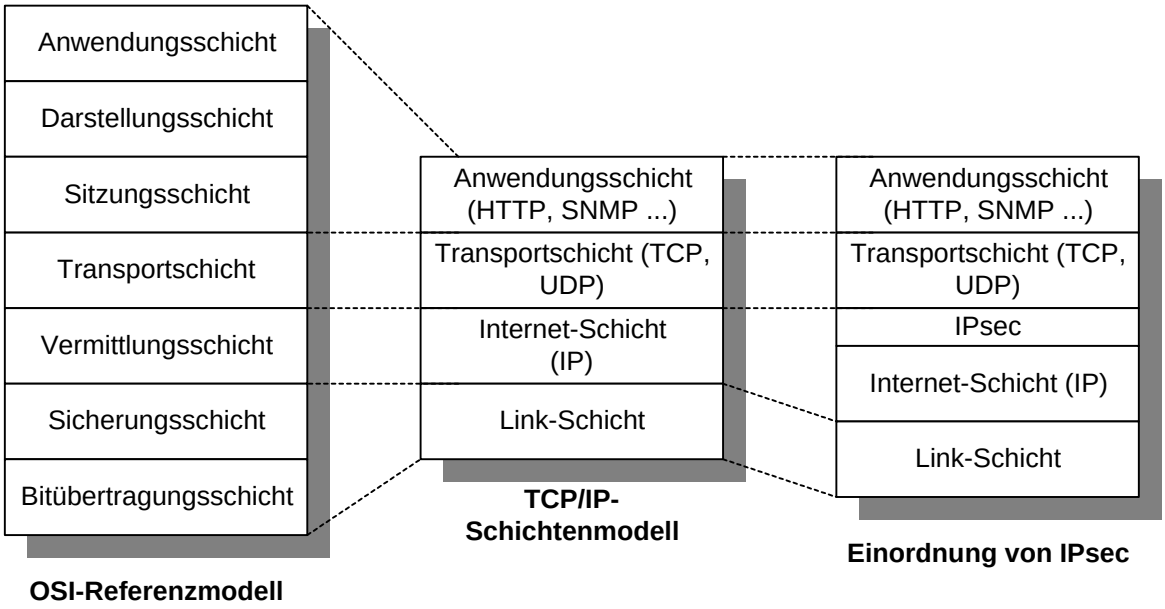

Abb. 1: Einordnung von IPsec ins OSI-Modell

IPsec führt zwei Header ein, die für eine sichere Kommunikation sorgen:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Mit Hilfe des IP Authentication Header (AH) wird die Integrität der übertragenen Daten geschützt und die Authentizität gewährleistet. Auch ohne die Möglichkeit, die Daten verschlüsseln zu können, findet hier eine Sicherung der Datenübertragung statt, indem eine Prüfsumme (z.B. mit Hilfe von MD5 oder SHA-1) der Daten erstellt wird und verschlüsselt in den Authentication Header eingefügt wird. Zum Schutz gegen das Wiedereinspielen (Anti-Replay) von Paketen werden Sequenznummern verwendet.

Der Header Encapsulating Security Payload (ESP) kapselt die zu schützenden Daten ein und gewährleistet bei Bedarf deren Vertraulichkeit durch Verschlüsselung. Außerdem sind Möglichkeiten zum Schutz der Integrität und zur Authentizität der Datenpakete vorgesehen. Wie beim AH können auch hier Sequenznummern zum Schutz gegen das Wiedereinspielen von Datagrammen genutzt werden. Die Vertraulichkeit kann durch ein geeignetes Verschlüsselungsverfahren (z.B. DES oder Triple-DES) gewährleistet werden, der Schutz der Integrität der Daten wird durch eine kryptographische Prüfsumme (z.B. mit Hilfe von MD5 oder SHA-1) garantiert. Nicht durch das ESP eingekapselte Felder eines Pakets können nicht geschützt werden.

Zum Transport der IP-Pakete erhält man zwei verschiedene Modi, den Transport-Modus und den Tunnel-Modus, die sich im wesentlichen durch den Aufbau der Pakete und die Einsatzmöglichkeiten unterscheiden:

- Im **Transport-Modus** werden nur die Daten der Transportschicht geschützt, nicht aber der IP-Header. Bei der Benutzung des ESP ist es nötig, die eigentlichen Nutzdaten in das ESP zu integrieren, da diese hier verschlüsselt werden. Dies wird durch einen Header und Trailer erreicht.
- Im **Tunnel-Modus** wird das gesamte Datenpaket mitsamt seines IP-Headers verschlüsselt und verpackt und mit einem neuen Header versehen. Es ist also möglich, die eigentlich zu schützenden Daten in einem weiteren IP-Paket zu kapseln und damit die so zusammengebauten Datagramme über Gateways zu versenden, die selbst kein IPsec unterstützen. Der Tunnel-Modus erfordert, dass das ursprüngliche Datagramm vollständig neu verpackt wird und daher der Authentication Header und ein neuer IP-Header vorangestellt werden müssen. ESP schließt im Tunnel-Modus das ursprüngliche Datagramm ein, um es insgesamt zu verschlüsseln. Dem so neu entstandenen Paket wird ein neuer IP-Header vorangestellt.

3.2 Quality-of-Service

Zur Erreichung einer garantierten Dienstgüte sind unterschiedliche Ansätze vorhanden:

- Layer 2: ATM[12]-QoS: CBR, VBR und ABR
- Layer 3: IP-QoS: IntServ, RSVP, DiffServ
- Layer 2: IEEE 802.1D

[12] Asynchronous Transfer Mode

Dabei liegt der Schwerpunkt auf dem IP-QoS, da das Internet heute dominiert und man auf dieser Layer-3-Ebene Prioritäten setzen kann. Echtzeitdaten lassen sich heute nicht ohne weiteres über IP-Netze transportieren. Die Voraussetzung dafür ist, dass Ressourcen wie Bandbreite, Bit-Rate oder Verarbeitungsleistung in einer garantierten Qualität zur Verfügung stehen. Das Internet arbeitet jedoch nach dem Best-effort, das keine garantierte Dienstgüte unterstützt. Um dieses Problem in den Griff zu bekommen, wurden QoS-Mechanismen für Multimedia-Anwendungen entwickelt. Sie beruhen auf abgestuften QoS-Niveaus. Solche Ansätze sind die Integrated Services (IntServ) und Differentiated Services (DiffServ).

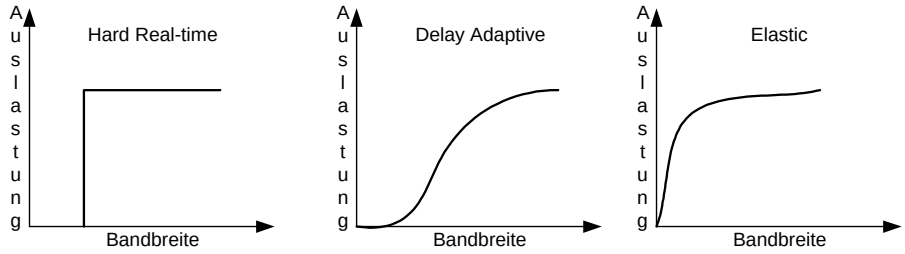

Abb. 2: Unterschiedliche Eigenschaften der Anwendungen

Die Dienstgüteanforderung unterscheidet sich je Anwendung. Dabei steht die Verzögerung einzelner Pakete im Vordergrund, die durch die maximale und minimale Verzögerung begrenzt wird. Echtzeitapplikationen benötigen dabei eine garantierte Verzögerung, während andere Anwendungen weniger anfällig sind. Dabei unterteilt die Integrated Service Group diese Anwendungen in Hard Real-time, Delay Adaptive und Elastic Applications. Die erste Gruppe ist dabei sehr empfindlich gegenüber Störungen, während die zweite Gruppe leichte Verzögerungen toleriert. Die dritte Gruppe sind reine Datenanwendungen, die große Zeitverzögerungen zulassen und das Zwischenspeichern von Daten zulassen.

3.2.1 Integrated Services (IntServ)

Diese ersten Ansätze der IETF um QoS auch in IP-Umgebung umsetzen und nutzen zu können, wurde durch die Arbeitsgruppe Integrated Services (IntServ) ins Leben gerufen. Ziel war es, besonders Echtzeitapplikationen effizienter und mit der maximal möglichen Performance zu unterstützen. Der reine Best-effort sollte durch ein komplexeres Modell abgelöst werden, um die Anforderungen neuer Applikationen erfüllen zu können. Um dies zu ermöglichen, sollten Prioritätsklassen eingeführt werden, die man den unterschiedlichen Anforderungen zuordnen kann. Folgende Annahmen hat man dabei für das IntServ-Modell getroffen:

- Ressourcen müssen explizit verwaltet werden, um die Anforderungen der Anwendungen erfüllen zu können.
- Die Dienstgarantien für Echtzeitapplikationen können nicht ohne Reservierung von Ressourcen erfolgen.
- Die End-to-end-Verzögerungszeiten müssen begrenzt werden, um die dynamische Anpassung an sich ändernde Netzbedingungen gewährleisten zu können.
- Statistisches Aufteilen zwischen Echtzeit- und Datenapplikationen ist vorteilhaft, wenn man über eine gemeinsame Infrastruktur beide Anwendungen nutzen will

Dabei kann die Übertragung über Unicast-Pakete[13] oder Multicast-Pakete[14] stattfinden. Um dies umzusetzen, wird ein virtueller Kanal zwischen den Kommunikationsteilnehmern geschaltet. Ausgehend von den Anforderungen des Datenverkehrs wird ein QoS-Profil mit fest vorgegebenen Verkehrsparametern vereinbart. Dementsprechend werden dann entlang der Route Ressourcen in jeder Übertragungseinrichtung reserviert. Aus den IntServ-Spezifikationen nach RFC-1633 entstanden die folgenden Dienstklassen, die 1997 zum Proposed Standard erhoben worden:

1. **Controlled Load Network Element Service (CL-Service):** hat zum Ziel dem Teilnehmer ein unbelastetes Netz in Zeiten der Überlast vorzutäuschen. Daher wird dieser Dienst auch als geringfügig besser eingestuft, als bei Best-effort. Die Spezifikation RFC-2211 beschreibt diesen Service. Einsatzgebiete sind: Audio-/Videostreaming und Web-basierte Transaktionen. [WROC97a]
2. **Guaranteed Quality of Service (Guaranteed Service, GS):** Dieser Dienst legt die Einhaltung fester QoS-Parameter im Netz fest. Diese Parameter werden vor dem Beginn der Übertragung oder parallel dazu ausgehandelt. Die Spezifikation RFC-2212 legt diese Parameter fest. Einsatzgebiete sind interaktive Dienste, die eine harte Anforderung an QoS haben, wie IP-Telefonie, VoIP und Videokonferenzen. [SPG97]

3.2.2 Differentiated Services (DiffServ)

Neben dem Ansatz der Integrated Services sind die Differentiated Services (DiffServ) der IETF entstanden, um die Probleme der IntServ zu lösen bzw. über einen verbindungslosen Ansatz eine bessere Beherrschbarkeit bzw. Skalierung zu ermöglichen. Der Hauptunterschied zu IntServ besteht somit darin, dass man keine Signalisierung Ende-zu-Ende durchführt. Erste RFCs (RFC-2474, RFC-2475 und RFC-2598) für die Differentiated Services liegen bereits vor. Man möchte hier die bereits gewonnenen Erkenntnisse und Erfahrungen aus ATM einzusetzen, um IP Traffic-Management Funktionalität und Dienstgüte zu implementieren. Im ersten Schritt wird dies durch eine neue Interpretation der TOS-Bits im IP-Header umgesetzt.

Das Konzept von DiffServ ist dabei, dass die Dienste in einige wenige QoS-Klassen unterteilt werden. Für jede so entstandene Dienstklasse wird ein Satz von Behandlungsregeln[15] definiert. Datenpakete, die in das Netz eintreten, werden im DS-Feld des Paketkopfes entsprechend ihrer Dienstklasse markiert und unter Berücksichtigung der dafür definierten PHB weiterverarbeitet. Mehrere unterschiedliche Verkehrsströme mit ähnlichen QoS-Anforderungen werden somit zu einem größeren Verkehrsbündel zusammengefasst (Aggregation), das im Netz auf gleiche Weise behandelt wird. Man spart sich somit die vielen Zustände und deren Verwaltung im Netz. Stattdessen wird die Vorverarbeitung des Verkehrs bzw. die Markierung der QoS-Klasse, das Policy Control und Traffic Shaping nur einmal, nämlich am Eingang in das DiffServ-Netzes vorgenommen. Der Ansatz DiffServ bringt somit eine völlig neue Sicht auf die QoS-Architektur und das Zusammenspiel einzelner Bereiche mit sich.

[13] Unicast = Punkt-zu-Punkt-Kommunikation zwischen zwei Teilnehmern

[14] Multicast = Punkt-zu-Mehrpunkt-Kommunikation zwischen einer bestimmten Gruppe

[15] Per-Hop Behavior (PHB)

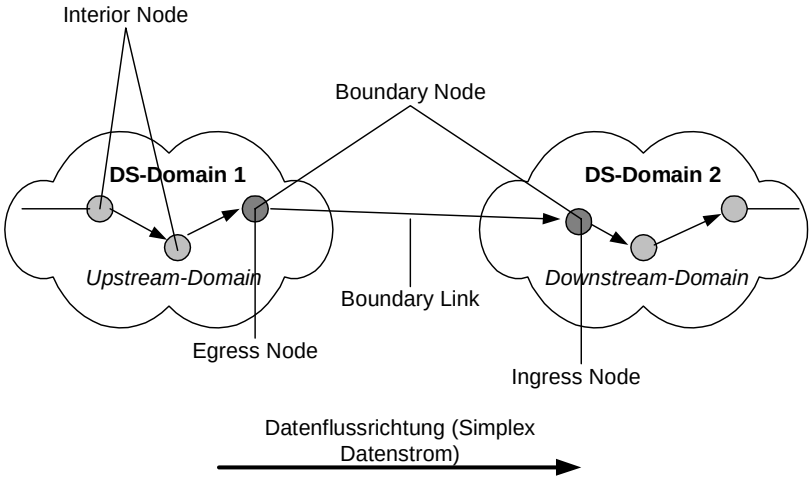

Abb. 3.3: DiffServ-Architektur

Im Mittelpunkt aller DiffServ-Betrachtungen steht eine administrative Einheit, die man als DiffServ-Cloud bzw. DS-Domain bezeichnet. Die administrativen Vereinbarungen und Abkommen spielen hierbei eine übergeordnete Rolle. Man versucht mit der Entwicklung dieses Modells nicht eine einheitliche Behandlung des DiffServ-Verkehrs im Internet zu erzielen, sondern man bildet vielmehr mehrere solche DiffServ-Clouds, innerhalb derer feste Verarbeitungsregeln definiert sind. Darüber hinaus wird die Behandlung der Daten beim Eintritt bzw. beim Verlassen solcher Bereiche in diversen Abkommen festgehalten und entsprechend auf die Datenströme angewendet. Diese Sichtweise ist zwar der gegenwärtigen Internet-Verwaltung ähnlich, aber ist im QoS-Bereich völlig neu. [SEUM01]

3.3 Voice-over-IP

Durch unterschiedliche Codierungsverfahren ist es heute möglich die Sprache stark zu komprimieren, wodurch bis zu 9/10 der Bandbreite eingespart werden kann. Dies ist in der Internet-Umgebung notwendig, um die teilweise schlechten Übertragungsverhältnisse auszugleichen. Nach der Digitalisierung und Komprimierung gelangen die Daten durch ein Übertragungssystem von dem Sender (Quelle) zum Empfänger (Senke). Am Empfänger müssen die digitalen Signale wieder dekomprimiert werden, damit abschließend eine Umwandlung in Analogsignale erfolgen kann.

Bei dieser Bearbeitungsreihenfolge, die nicht abänderbar ist, gilt es eine Reihe von Problemen zu beachten. Dabei tritt bei der paketorientierten Sprachübertragung vor allem die Laufzeit als kritische Messgröße in den Vordergrund. Weitere negative Randbedingungen sind:

- schwankende Verzögerungen
- Verbindungsunterbrechung
- Echoeffekte
- Bitfehler
- Paketverluste
- Fragmentierung
- Reihenfolgeänderungen der Pakete

- Paketverdopplung

Als wichtigste Eigenschaft bei der Sprachübertragung kann die Qualität der Sprache am Empfänger angesehen werden. Um diese zu definieren oder messen zu können, muss man bestimmte Parameter festlegen. Aber selbst dann ist die Bestimmung der Sprachqualität eine schwierige Aufgabe, da sie nur subjektiv erfasst werden kann. Die wichtigsten, aber durchaus nicht alle Aspekte, die für die Sprachqualität entscheidend sind, werden in der Abb. 3.4 dargestellt.

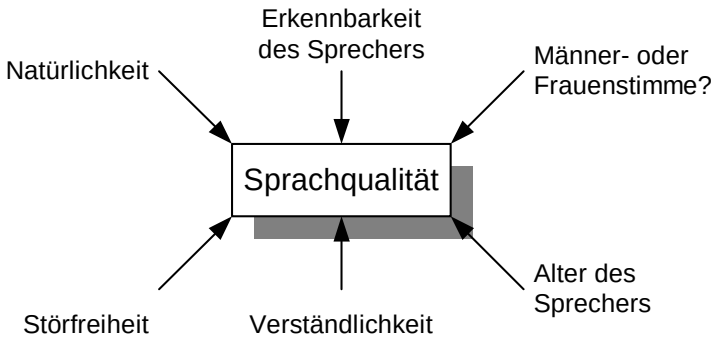

Abb. 3.4: Aspekte der Sprachqualität

Die meisten Messverfahren, die eine Qualität nachweisen sollen, sind dementsprechend subjektiv, da sie von der Beurteilung des Menschen abhängig und demnach Schwankungen unterworfen sind. Bei diesen Verfahren wird eine ausgewählte Sprachprobe von einer gewissen Anzahl von Menschen unter bestimmten Randbedingungen beurteilt. Diese Beurteilungen werden analysiert und statistisch erfasst, um die Ergebnisse einigermaßen reproduzierbar zu halten. Bei den objektiven Messverfahren werden physikalische Messungen und Berechnungen herangezogen, um die Sprachqualität zu ermitteln. Diese sind meistens allerdings nur auf spezielle Fälle anwendbar, da man festgestellt hat, dass technische Messgrößen wie Latenzzeit, Jitter und Paketverluste nicht für eine Beurteilung ausreichen, weil der Zusammenhang zwischen Paketverlust und Einbußen bei der Sprachqualität nicht reproduzierbar ist. Aus diesem Grund kommen meistens die subjektiven Verfahren zum Einsatz.

Die wichtigste Messgröße der Sprachqualität ist die Sprachverständlichkeit, da das Hauptziel der Sprachübertragung darin besteht Informationen zu übermitteln, die im ersten Schritt verständlich beim Empfänger ankommen müssen. Dabei kann die Sprache hervorragend zu verstehen sein, aber einen unnatürlichen roboterähnlichen Klang aufweisen. Dieser kann beim Hören ein unangenehmes Gefühl entstehen lassen. Also darf man die Sprachverständlichkeit auch nicht überbewerten.

Zur Beurteilung der Sprachqualität wird heute das subjektive Verfahren Mean Opinion Score (MOS) eingesetzt. Bei diesem Verfahren wird einer Reihe von Testpersonen (Größenordnung 25) mindestens ein Satz als Sprachprobe dargeboten. Die Testpersonen beurteilen die Sprachproben durch Vergabe von Noten.

3.4 Implementierung

Für den Aufbau einer sicheren Kommunikationsplattform über das Internet wird der Tunnel-Modus verwendet, da er die dazwischenliegende Infrastruktur nicht beachtet bzw. überbrückt. Für eine ganzheitliche Sicherheitsplattform wäre der Transportmodus besser geeignet, der Hop-by-hop arbeitet. Wichtig ist der Einsatz eines Key Managements, um symmetrische Schlüssel sicher über die Netzplattform zu verteilen. In IPsec ist das Protokoll Internet Key Exchange (IKE) dafür definiert worden. IKE arbeitet in zwei Phasen, der Authentifizierungs- und Schlüsselgenerierungsphase. Vorteile des Verfahren sind, dass ohne großen Aufwand neue Schlüssel generiert werden können und dass das Verschlüsselungsverfahren ausgetauscht werden kann. Diese abstrakten Definitionen werden in der RFC-2409 genau beschrieben. Zur symmetrischen Verschlüsselung wird Blowfish empfohlen. Blowfish ist ein Algorithmus, welcher nicht patentiert und frei verfügbar ist. Er wurde von Bruce Schneier entworfen und ist sehr schnell. Blowfish ist für Anwendungen wie die Verschlüsselung von Kommunikationskanälen optimiert worden, bei denen sich der Schlüssel nur selten ändert. Er beinhaltet eine 64-Bit-Blockchiffrierung mit variabler Schlüssellänge von bis zu 448 Bit.

Das DiffServ-Modell besitzt seinen größten Vorteil in der guten Skalierbarkeit der Dienste auf große Netze. Dabei werden im inneren Netz nicht einzelne Datenströme, sondern einige wenige Datenstromaggregate unterschieden. Auf der anderen Seite bietet das IntServ/RSVP-Modell eine wesentlich bessere Granularität des Dienstes als das einfache DiffServ-Modell. Die Anforderungen einer Anwendung sind dabei an keine Verkehrsprofile gebunden. Man kann also nahezu beliebige Werte der Verzögerung und der Bandbreite verlangen. Außerdem bietet RSVP ein sehr leistungsfähiges Signalisierungsprotokoll zur Aushandlung der QoS-Parameter zwischen einem Anwender und dem Netz an. Um die Vorteile beider Modelle zu Nutzen ist beim IETF ein Architekturmodell zur Interoperabilität zwischen IntServ und DiffServ in der Spezifikation RFC-2998 entwickelt worden.

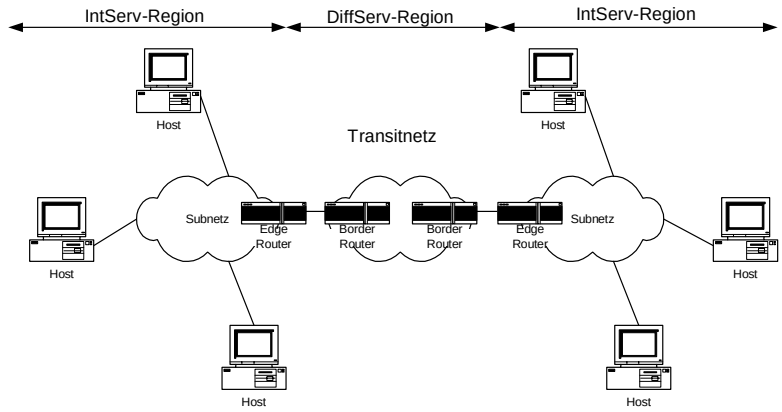

Abb. 3.5: Architekturmodell der IntServ/DiffServ-Interoperabilität

Danach liegt am Rande des gesamten Netzes ein IntServ-Netz und in der Mitte ein DiffServ-Netz vor. Das IntServ-Netz tritt hier als Dienstnutzer (Kunde) der DiffServ-Region auf. Abb. 3.5 zeigt dafür das Architekturmodell. Zur Vereinfachung ist auf beiden Seiten der DS-Domain nur eine IntServ-Domäne eingezeichnet. In der Realität befinden sich an beiden Seiten der DiffServ-Wolke viele IntServ-Domänen. Da die Router in einer DS-Domain auch RSVP-fähig sein können, sowie die Knoten der IntServ-Domäne DS-fähig, ist die Einteilung

des Netzes in DiffServ- und IntServ-Regionen nicht immer eindeutig. Man unterscheidet IntServ- von DiffServ-Regionen nur anhand der Behandlung der Datenflüsse. Werden in einer Region die Datenflüsse auf Microflow-Basis behandelt, so betrachten man diesen Bereich als eine IntServ-Region. Wenn hingegen die Datenflüsse auf einer Aggregat-Basis behandelt werden, so betrachten man diese als eine DiffServ-Region. Die Grenze zwischen der IntServ- und DiffServ-Region ist vom Netzadministrator frei wählbar.

Durch die steigende Anzahl von Online-Shops und die wachsende Zahl der Kunden, die das Medium Internet zum Einkaufen nutzen, steigt auch die Komplexität von eShops und der dahinterliegenden Prozesse. Mitunter tauchen bei dem Benutzer Fragen auf, die daraufhin durch den User Support mittels E-Mail oder Telefon geklärt werden müssen. Diese Lösung ist zum einen langsam und umständlich, zum anderen ist es für den User Support schwierig, am Telefon Unklarheiten zu klären, ohne zu sehen, an welcher Stelle des Online-Shops der Kunde sich gerade befindet.

Die Anbindung eines Call Centers an einen Online-Shop beseitigt die oben beschriebene Problematik und ermöglicht somit eine effizientere Interaktion mit dem Teilnehmer. Durch integrieren eines sogenannten Call-me-Button auf der Webseite eines Online-Shops soll dem Kunden die Möglichkeit gegeben werden, sich direkt über das Internet mit dem User Support zu verbinden. Je nach verfügbarer Hardware und Bandbreite der Internet-Anbindung soll nach Betätigung der Button folgendes automatisch ausgewählt werden:

- Videokonferenzsystem
- IP-Telefonie
- Text-Chat
- Call-back

Der User Support soll bei Etablierung der Verbindung sehen, auf welcher Webseite der Kunde sich befindet, um direkt auf die Frage eingehen zu können und den Anwender zu unterstützen. Es sollte möglich sein, mit einem Remote-Mousepointer auf bestimmte Bildschirmbereiche hinzuweisen, ggf. Aktionen auszuführen. Bei schlechter Verbindungsqualität ist Kommunikation über Texteingabe möglich (Text-Chat). Wenn erwünscht kann der Kunde nach Angabe einer Rufnummer den Support um einen Rückruf bitten, sodass der Betreuungsprozess über Internet oder Telefon fortgesetzt wird.

Voraussetzung für Kompatibilität der Kommunikation zwischen Kunden und Call Center über das Internet muss der H.323 ITU-Standard eingehalten werden. Hiermit ist gewährleistet, dass nicht ein bestimmtes Videokonferenzsystem vorgeschrieben werden muss, sondern dass verschiedene Videokonferenzlösungen genutzt werden können, die H.323 erfüllen. Als Beispiele kann man NetMeeting (Microsoft), CU-SeeMe (Whitepine) oder Cruiser-Produkte (VCON) nennen. [INTE00]

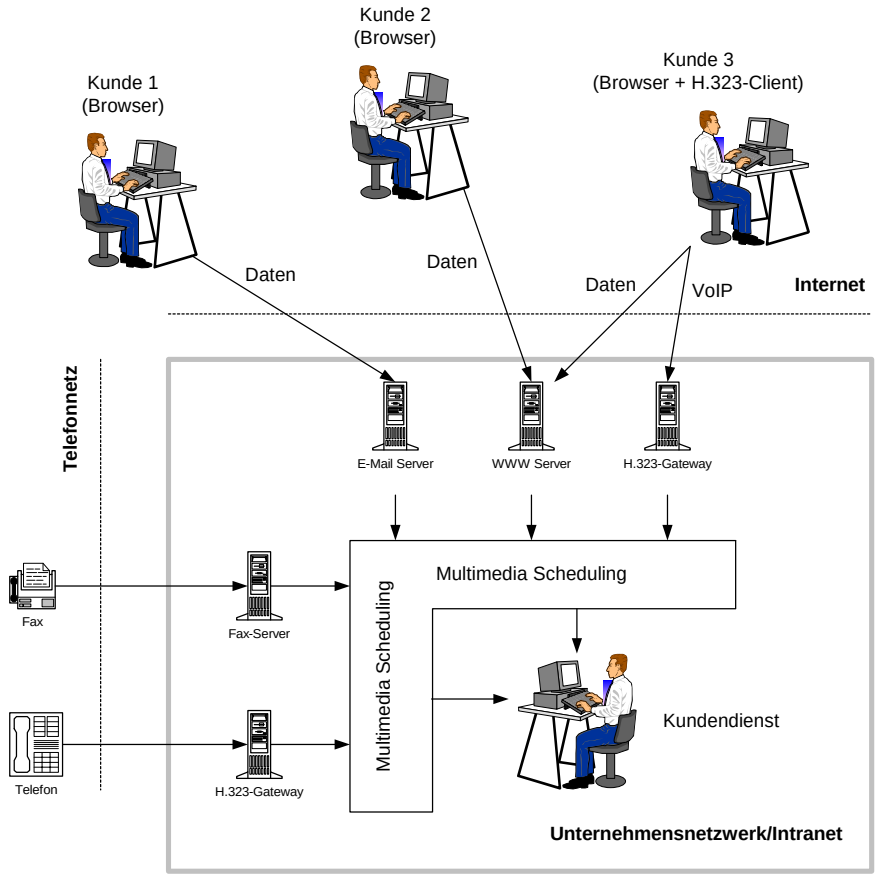

Abb. 1: Web-basierter Call Center

Die Benutzung von Avataren (virtuelle, 3D-animierte Menschen o.ä.) ist eine weitere Möglichkeit, den Support handhabbarer zu gestalten. Weiterhin besteht die Möglichkeit, einen virtuellen Online-Shop zu generieren. In einer dreidimensionalen Einkaufswelt könnte an der Information mittels VoIP und einem Avatar der User Support Prozess beginnen.

Es gibt verschiedene Ansätze, in denen mit Hilfe von Virtual Reality Modelling Language (VRML) 3D-Welten generiert und Avatare verwendet werden können. Beispiele für Software-Produkte, die sich VRML zu Nutzen machen, sind:

- Online-Traveler (Virtuelle 3D-Welten im Internet inklusive VoIP)
- Blaxxun Contact 4.3 (VR-Welt mit sprachsynthetisierten Text-Chat)
- Holodesk Communicator 1.1 (3D-Welten mit VoIP, Text-Chat, Dokumentenablage, Bildbetrachter etc.)

Die Vorteile, die sich durch die Verschmelzung von Daten-, Sprach- und Videokommunikation ergeben, lassen sich nicht nur für einen Call Center darstellen, sondern gelten auch für andere Bereiche. Die folgende Punkte lassen sich dabei auflisten: [Detk00]

- Kostenreduzierung
- Anwenderfreundlichkeit
- Kundennähe
- Kürzere Wege und schnellere Reaktionszeiten

4 Fazit

Zusammenfassend sind folgende Engpässe bzgl. VoIP zu erwähnen:

- Direkte Kommunikation bei E-Commerce-Lösung ist über das Internet bislang nicht vorhanden, da die Möglichkeiten begrenzt sind und keine ausreichende Dienstgüte angeboten wird
- VoIP-Implementierungen sind kaum vorhanden und wenn nur in kleineren Test-/Pilotprojekten verfügbar
- Im Internet und in anderen Datennetzen wird nur Best-effort eingesetzt
- Bislang ist die Sprach- und Bildqualität im Internet von der Tageszeit abhängig, da unterschiedliche Lasten auftreten. Diese Lasten lassen sich in einem heterogenen Umfeld nicht oder nur schwer beherrschen
- Videokonferenzsysteme als eine Möglichkeit Echtzeitdaten zu übertragen haben sich nicht durchsetzen können, da die technische Implementierung unzureichend war, die Handhabung sich unfreundlich gestaltete sowie Multicast zur Gruppenkommunikation ein komplexes Themengebiet darstellt
- Sicherheitsprobleme: keine Verschlüsselung der Sprachdaten wird bislang verwendet oder von den Herstellern angeboten sowie fehlende oder unzureichende Authentifizierung ist vorhanden [Gore99]

INTELLECT ist dabei ein Help-Desk-System integrieren, welches auf den vorhandenen Qualitätsgrad des Internet Rücksicht nimmt, vorhandene Standards und Spezifikationen berücksichtigt und neue Interaktionsmöglichkeiten mittels 3D, Avataren und Online-Führung durch die Web-Seiten bietet. Dabei werden bei der Entwicklung des Systems die Endbenutzer bei INTELLECT von Anfang an mit einbezogen, um größtmögliche Akzeptanz zu erreichen und benutzerfreundliche Software zu entwickeln. Aus diesem Grund werden verschiedene User Groups in unterschiedlichen Ländern (Griechenland, Deutschland, Österreich) gebildet, die kontinuierlich mit Wissen versorgt und die ersten Testplattformen nutzen werden. Nach Ende des Projektes Anfang 2002 wird eine Kommerzialisierung des entstandenen Produkts angestrebt. [DFW+00]

Literatur

[BZB+97] R. Braden, Ed.; L. Zhang; S. Berson; S. Herzog; S. Jamin: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification; RFC-2205; Network Working Group; Category: Standard Track; IETF 1997

[DeFi00] Kai-Oliver Detken, Ioannis Fikouras: Intelligent and Secure 3D-Configuration of Products in Electronic Shop Systems; Proceedings; 16.-19. November 2000; Third International Conference on Telecommunications and Electronic Commerce (ICTEC 2000); Dallas, Texas, USA 2000

[DFW+00] Detken, Fikouras, Wurst, Weber, Kaufmann: Interactive Marketing and Intelligent 3D-Configuration of Products in Electronic Shop Systems; eBusiness and eWork 2000 Conference and Exhibition; Proceedings; 18.-20.10.2000; Madrid/Spain 2000

[DeRe00] Kai-Oliver Detken, Bernd Reder: EU-Projekt INTELLECT: Der Internet-Shop der Zukunft: Einkaufen im Cyber-Shop; NetworkWorld 24,25/00; Computerwoche Verlag GmbH; München 2000

[Detk01] Kai-Oliver Detken: E-Shopping dreidimensional - Call Center und 3D-Welten werten E-Shops auf; ; NET 1-2/01; Hüthig-Verlag; Heidelberg 2001

[Gore99] Christian A. Gorecki: Sichere Sprachübertragung über das Internet; Diplomarbeit an der Universität Bremen; Fachbereich Physik/Elektrotechnik; Prof. Laur; Bremen 1999

[RoSc00] Carsten Rossenhövel; Gabriele Schrenk: Sprachqualität entscheidet – Prüfverfahren für IP-Telefone; NetworkWorld 24/25; Computerwoche Verlag GmbH; München 2000

[INTE00] Software functional specification, in: handbook D07, Internal Document, INTELLECT consortium 2000