Abschlußbericht für Verbundprojekt

VPN Seat

Zuwendungsempfänger:	**Förderkennzeichen:**
IHP Microelectronics	20K0606A
Vorhabensbezeichnung:	
VPN Seat – Drahtloses Virtuelles Netzwerk für die Kommunikation durch den Passagier	
Laufzeit des Vorhabens:	
1.1.2007 bis 31.12.2009	
Berichtszeitraum:	
1.1.2007 bis 31.12.2009	

Autor	:	Im Namen des VPN Seat Projektteams der IHP Microelectronics Peter Langendörfer, Oliver Maye
Projekt-Nr.	:	240101RS
Sicherheit	:	Freigegeben
Version	:	1.1
Datum	:	26.07.2010

INHALTSVERZEICHNIS

INHALTSVERZEICHNIS 2

I. KURZE DARSTELLUNG 3

1 Aufgabenstellung 3

2 Voraussetzungen 3

3 Planung und Ablauf des Vorhabens 3

4 Wissenschaftlicher und technischer Stand 4

5 Zusammenarbeit mit anderen Stellen 6

II. EINGEHENDE DARSTELLUNG 7

1 Verwendung der Zuwendung 7

2 Erzielte Ergebnisse 7
2.1 AP1.1 – Top-Level und Systemanforderungen 7
2.1.1 Systemanforderungen 7
2.1.2 Middleware-Anforderungen 8
2.1.3 Hardware-Anforderungen 8
2.2 AP1.2 – Architektur und Schnittstellen 8
2.3 AP2.1.1 – Entwicklung eines Geräteauswahlverfahrens 10
2.3.1 Voruntersuchung zum Verteilen von Multimedia-Datenströmen 10
2.3.2 Untersuchungen zur automatischen Geräteauswahl 11
2.4 AP2.1.2 – Entwicklung eines Schlüsselauswahlverfahrens 12
2.5 AP2.2.1 – Entwicklung einer einheitlichen Protokollschnittstelle 14
2.6 AP2.2.2 – Einheitliche Service Discovery Protokolle 15
2.7 AP4.1 – Entwicklung der Demo-Anwendung 16
2.8 AP4.2 – Aufbau des Demonstrators 19

3 Notwendigkeit und Angemessenheit der geleisteten Arbeit 20

4 Voraussichtlicher Nutzen 21

5 FE-Ergebnisse von dritter Seite 21

6 Veröffentlichungen des Ergebnisses 22

7 Referenzen 22

I. Kurze Darstellung

1 Aufgabenstellung

Das Ziel des Verbundvorhabens bestand darin, jedem Passagier ein "Drahtloses Virtuelles Privates Netzwerk (VPN)" an seinem Sitz durch Einsatz innovativer Technologien bereitzustellen. In dieses Netzwerk sollen die mobilen Endgeräte des Passagiers und die zum Sitz gehörende, System-Plattform integriert sein. So wird die Verwendung der persönlichen Endgeräte, mit ihren individuellen Einstellungen, bei der Nutzung der Onboard Dienste ermöglicht. Die geplante automatische Integration der Endgeräte in die Infrastruktur nimmt dem Passagier und den Flugbegleitern auch die Last der Konfiguration des Systems ab.
Die IHP GmbH hat sich im Wesentlichen auf die mittleren Schichten konzentriert. Hierbei sollten insbesondere Ansätze für Multi-Standard Protokoll Gateways untersucht und entwickelt werden. Des Weiteren hat sich die IHP GmbH auf die Untersuchung von Konzepten zur Gewährleistung der Datensicherheit und dem Schutz der Privatsphäre konzentriert. Zusätzlich wurde der Architekturentwurf sowie die Integration der einzelnen Komponenten der Partner in den finalen Demonstrator durch das IHP verantwortet.

2 Voraussetzungen

Das IHP hat im Rahmen folgender Projekte an Middleware-Platformen insbesondere für context-sensitive Dienste mitgearbeitet: Wireless Internet: ad hoc, Wireless Internet zellular (beide bmbf gefördert), WINE GLASS (EU 5th Framework).
Sicherheitsaspekte in kontext-sensitiven Plattformen und Hardwarebeschleuniger für kryptographische Verfahren untersucht das IHP in den Projekten: Mobile Internet Business (bmbf) und UbiSecSens (EU 6th Framework).
Darüber hinaus hat das IHP ein eigenes 802.11a Single Chip Modem im Rahmen des Projektes IBMS2 entwickelt und arbeitet zurzeit im Rahmen des WIGWAM Projektes an WLAN Modems im 60 GHz Bereich sowie im EU Projekt PULSERS an UWB Systemen. Außerdem wurde im IHP ein TCP Chip entwickelt.
Das IHP hat also hervorragende Vorraussetzungen ein einheitliches Multi-Standard-Protokoll Gateway, das die gefundenen Dienste und Endgeräte in ein virtuelles, Passagier gebundenes, Netzwerk integriert und in diesem den Datenaustausch regelt, zu entwickeln. Es bringt außerdem die notwendigen Kompetenzen für Arbeiten am Schlüsselaustauschverfahren und zur Dienstvermittlung in das Projekt ein.
Im Rahmen einer Forschungsstudie arbeiteten IHP und Airbus Deutschland GmbH bereits zusammen. Auch mit dem Unterauftragnehmer PhiloTech verbindet IHP eine lange, gemeinsame Kooperationshistorie. Die vorhandenen Kontakte werden genutzt, um ggf. Synergieeffekte zu erzeugen, die sich gemeinsam mit anderen Forschungs- und Entwicklungsvorhaben dieser Unternehmen ergeben können.

3 Planung und Ablauf des Vorhabens

Der zeitliche und inhaltliche Ablauf des Vorhabens verlief insgesamt im Rahmen der ursprünglichen Planungen. Größere Abweichungen in den Einzelpositionen traten in der personellen Ausstattung der Anfangsphase, bei Arbeiten zur Service-Discovery Vermittlung, beim Multiprotokoll-Gateway sowie bei der Ausstattung des Demonstrators auf, konnten jedoch sämtlich durch operative Entscheidungen im Verlauf des Projektes kompensiert werden.

Der Projektstart bei IHP erfolgte zunächst mit einer Person. Die Erweiterung des Projektteams um eine weitere Mitarbeiterin gelang erst mit einer Verzögerung von ca. 6 Wochen. Der Rückstand konnte jedoch bereits im ersten Drittel der Projektlaufzeit wieder aufgearbeitet werden. Im gesamten Projekt kam es zu keinen weiteren personellen Engpässen.

Entgegen erster Annahmen konnte eine dynamische Dienstvermittlung mithilfe der DIANE-Plattform [1] (http://hnsp.inf-bb.uni-jena.de/DIANE) aufgrund der spezifischen technischen Anforderungen nicht erreicht werden. Als hinderlich in diesem Ansatz erweist sich das hohe Abstraktionsniveau, auf dem in DIANE Dienste beschrieben, angeboten und vermittelt werden. Als Reaktion auf die gewonnenen Erkenntnisse wurden proprietäre Lösungen für ein bilaterales Bridging zwischen verschiedenen Service Discovery Protokollen in das Architekturmodell wiederaufgenommen. Der zeitliche Ablauf des Projekts blieb davon unbeeinflusst.

Im Rahmen der Projekttätigkeit zum Multiprotokoll-Gateway wurde erkannt, dass eine dynamische Erweiterung der zum Einsatz kommenden Übertragungsverfahren und Protokolle nicht notwendig ist. Ebenso ist die Anzahl gleichzeitig übertragener Daten- und Medienströme im Flugzeugsitz vorhersagbar klein. Mit dieser verringerten Dynamik des Gesamtsystems und dem häufigen Fehlen von Alternativrouten, lässt sich eine Multiprotokollvermittlung auch ohne XML Beschreibung sogar effizienter konstruieren. Die gewonnenen Erkenntnisse hatten keinen Einfluss auf den zeitlichen Verlauf des Projektes.

Die für den Aufbau des Demonstrators benötigten NFC-fähigen Endgeräte konnten zunächst nicht und später nur mit einem finanziellen Mehraufwand beschafft werden.

4 Wissenschaftlicher und technischer Stand

Service Discovery Protokolle
Es existiert eine Reihe von Ansätzen zum Service Discovery. Diese werden von unterschiedlichen Konsortien und Standardisierungsgremien vorangetrieben. Die für dieses Projekt wichtigsten Service Discovery Protokolle (SDP) sind: UPnP (http://upnp.org), Jini (http://www.jini.org), Service Location Protocol (SLP) (IETF, RFC2608) und Bluetooth SDP (http://www.palowireless.com/). Die Grundfunktionalität dieser Protokolle ist im Wesentlichen gleich. Geräte können Dienste anbieten oder nach Diensten suchen. Einige der Protokolle nutzen zusätzlich zu Broadcast-Nachrichten zentrale Register, die quasi als Vermittler dienen. Obwohl die Grundfunktionalitäten sehr ähnlich sind, sind diese Protokolle zu einander inkompatibel. Deshalb wurden in den letzten Jahren zahlreiche Ansätze untersucht, die eine einheitliche Nutzung der Service Discovery Protokolle ermöglichen sollen. Diese Ansätze lassen sich in zwei Kategorien einteilen:

- Bridging Konzepte: Diese Ansätze versuchen die Interoperabilität von jeweils zwei ausgesuchten SDPs zu erreichen. Abbildung 1 zeigt bereits untersuchte Beziehungen.

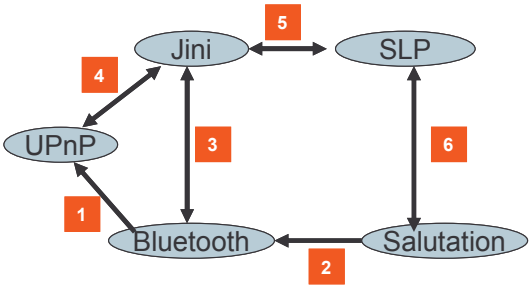

Abbildung 1: Existierende Bridging Ansätze für SDP

- Multi-SDP Ansätze: Die Unterstützung einer gemeinsamen Dienstbeschreibung wurde mehrfach untersucht. Die „Multi-Protocol Service Discovery and Access (MSDA) Middleware Plattform“ [2] bietet eine einheitliche Schnittstelle zum Service Discovery, die durch SDP spezifische Plugins in SLP, Jini oder UPnP Anfragen übersetzt werden kann. Die „Open service discovery architecture“ (Osda) [3] verfolgt einen ähnlichen Ansatz, führt jedoch ein XML basiertes Beschreibungsschema als Zwischensprache ein, das die Komplexität der Adaption an mehrere SDPs verringert. Die Idee „Reflective Middleware for Mobile Computing“ (ReMMoC) [4] verwendet alle bereitstehenden SDPs für die Suche nach geeigneten Diensten. Dabei wird ein SOAP basierter Ansatz für die Realisierung der Schnittstellenunabhängigkeit verwendet. Sichergestellt wird jedoch nur eine syntaktische Übereinstimmung der Suchanfrage und der Suchergebnisse.

Die Integration der räumlichen Nähe wurde in den letzten Jahren ebenfalls für Service Discovery Ansätze untersucht. Die Granularität ist dabei jedoch vergleichsweise grob. Dieses ergibt sich zwangsläufig aus der Genauigkeit, die von heutigen Positionierungssystemen bereitgestellt wird. Ein bekannter Versuch, dieses Problem zu lösen besteht darin, das Service Discovery über eine Infrarot Schnittstelle durchzuführen. So werden nur unmittelbar benachbarte Geräte erreicht. Leider erschweren die physikalischen Randbedingungen – direkte Sichtverbindung – den Aufbau von Gruppen mit mehr als zwei Geräten beträchtlich.

Split Device Ansätze

Ziel der Split-Device Technik ist es, die Komponenten eines multimedialen Datenstroms auch auf physisch verschiedenen Endgeräten darzustellen. So sollen z.B. beim Abspielen eines Videos die Audiodaten auf das Bluetooth-Headset, die zugehörigen Bilddaten jedoch auf das LCD eines Notebooks geleitet werden. Hierzu muß der zugrunde liegende Datenstrom aufgetrennt und auf die beteiligten Geräte (Videoquelle, Audio-, Videorenderer) verteilt werden. Grundsätzlich ist jede Stelle zwischen Datenquelle (Datei) und –senke (Wiedergabegerät) geeignet, um den Strom aufzutrennen und die verschiedenen Medienarten individuell zu behandeln.

Windows Remote Desktop Connection (WRDC) ist eine Technologie, um Windows-Computer über ein Netzwerk miteinander zu verbinden und Applikationen und Daten zur Verfügung zu stellen. Hierbei wird das Video von einer geeigneten Applikation, wie z.B. den Windows Media Player, auf dem Server entpackt, dekodiert und gerendert. Die Übertragung des fertig gerenderten Bildes erfolgt dann per WRDC auf den Client. Sie geschieht also nach dem Eintreffen in der lokalen Senke – eigentlich außerhalb des Video-Datenstroms. Diese Lösung erfordert die maximale Übertragungsbandbreite. Entsprechende Experimente lieferten sehr unbefriedigende Resultate – Das Video spielt stark verruckelt ab.

MaxiVista ist in etwa eine Windows Remote Desktop Connection, jedoch ohne Rückkanal, wie er dort für Maus- und Tastatureingaben benötigt wird. Daher ist diese Lösung etwas effizienter als WRC, insgesamt aber immer noch unbrauchbar für die Videoübertragung.

Bei der Benutzung des DivX Webplayers wird das Video vom Server, z.B. durch eine HTTP Server-Software, lediglich bereitgestellt. Die Übertragung erfolgt vor der Datenquelle, also ebenfalls außerhalb des Videostromes. Dekodierung und Rendering erfolgen vollständig auf dem Client durch eine geeignete Applikation, z.B. Web-Browser mit DivX-Plugin. Abgesehen von der besonders effizienten Art der DivX-Codierung besteht kein prinzipieller Vorteil gegenüber einem mit dem Windows Mediaplayer remote abgespielten Video. Es werden Ton und Video-Daten gemeinsam übertragen. Diese Lösung ist zwar sparsam bei der Verwendung der Netzwerkresourcen, verlangt dem Client jedoch ein Maximum an Rechenkapazität ab.

Ein vielversprechender Ansatz für die IHP-Lösung ist ein Eingriff in das DirectShow Subsystem von Windows. Ein geeigneter Filter kann in die Verarbeitung des Videostromes derart platziert werden, dass clientseitiger Rechenaufwand und Netzwerkbelastung optimal ausbalanciert werden.

Security

Für den Austausch von Schlüsseln in ad hoc Netzen sind in den letzten Jahren einige Protokolle vorgeschlagen worden. Die meisten dieser Ansätze gehen jedoch davon aus, dass es einen

gemeinsamen Vertrauten, wie die Basisstation gibt, wenn es geschlossene Gruppen von Geräten sind oder dass die Gruppe offen ist und benachbarte Endgeräte in diese Gruppe integriert werden sollen. Für dieses Projekt treffen beide Annahmen nicht zu. Die Gruppe der Geräte soll geschlossen sein, die jeweiligen Endgeräte und die Basisstation (Sitz) kennen sich jedoch nicht. In der Literatur wird ein Ansatz diskutiert, bei dem der gemeinsame geheime Schlüssel einer bestimmten Anzahl von Endgeräten aus Umweltdaten wie Temperatur, Geräuschpegel etc. gebildet wurde, und so die physikalische Nähe die Zugehörigkeit zu der geschlossenen Gruppe definiert hat. In einem ähnlichen Ansatz werden dazu Körperdaten genutzt. Beide Ansätze sind interessant, können aber wegen ihrer zu großen bzw. zu kleinen Ausdehnung nicht ohne Veränderung übernommen werden.

Funkmoduln / Antennen / Lokalisierungsverfahren
Im Bereich der Moduln für verschiedene Funkstandards gibt es eine Fülle von standardspezifischen Lösungen für die bisher im kommerziellen Einsatz befindlichen Funktechnologien. Diese Lösungen werden für das vorliegende Projekt als nicht ausreichend angesehen.
Einerseits bieten die bekannten und eingeführten Technologien wie WLAN oder Bluetooth keine oder nur unzureichende Möglichkeiten zur Objektlokalisierung. Die bekannten Verfahren sind zudem entweder in ihrer Auflösungsgenauigkeit bei weitem zu grob oder erfordern aufwändige Kalibrierungen des Systems zur Anpassung an die Einsatzumgebung.
Neue Perspektiven werden durch die Bestrebungen im Bereich Ultra-Wide-Band im Bereich von 3 – 10 GHz eröffnet. Erste Lösungen mit Lokalisierungsgenauigkeiten im Bereich von ca. 10 cm sind bekannt. Der Einsatz von UWB-Chips bzw. Baugruppen in Flugzeugkabinen und die gleichzeitige Integration weiterer Funkstandards zu einer Hardwareplattform ist bisher nicht bekannt und erfordert besondere Maßnahmen unter anderem hinsichtlich gegenseitiger Beeinflussungen, Nutzung von Baugruppen für mehrere Funktechnologien, Management der Funkschnittstellen und Antennenlösungen. Bekannt sind zum Beispiel Lösungen bei denen UWB- und 433-MHz-ISM-Kommunikationshardware in einem Gerät verwendet wird. Bei diesen Geräten werden jedoch keine Ressourcen der jeweiligen Kommunikationsstapel technologieübergreifend genutzt. Lediglich auf Applikations- und Koordinationsebene bestehen funktionale Beziehungen.
Lokalisierungsverfahren für die LDR-UWB-Technologie (IEEE802.15.4a) sind theoretisch beschrieben und bekannt. Nicht alle dieser Verfahren sind jedoch in der Lage, die notwendige Auflösungsgenauigkeit zu liefern.
Es ist zu vermuten, dass der mögliche Datendurchsatz einer reinen LDR-UWB Lösung nicht ausreicht, um den Bandbreitenbedarf von IFE-Anwendungen zu erfüllen. Somit wäre eine Kombination einer LDR- (z.B. gemäß IEEE802.15.4a) mit einer HDR-UWB Lösung (z.B. gemäß WiMedia) eine Realisierungsoption, die sowohl eine hinreichende Lokalisierungsgenauigkeit, als auch einen entsprechend hohen Durchsatz in der Kommunikationsfunktion gewährleistet. Bei der Konzeption sind spezielle Fragen der Interoperabilität und Koexistenz zwischen beiden UWB-Übertragungsstandards zu berücksichtigen.

5 Zusammenarbeit mit anderen Stellen

Die Zusammenarbeit mit dem Projektpartner TES und dem Unterauftragnehmer PhiloTech verlief erwartungsgemäß, produktiv und reibungsfrei. Die Aufteilung in die Hardware spezifischen Aufgaben (TES), Software (IHP) und Anwendungsprogrammierung (Unterauftragnehmer Philotech) hat sich dabei bewährt. Im Demonstrator konnten alle Teilergebnisse integriert und gezeigt werden. Diese Aufteilung der Arbeiten hat eine klare Schnittstellendefinition erfordert, die im Rahmen des Arbeitspaketes Gesamtarchitektur vorgenommen wurde. Bei diesen Arbeiten hat sich das spezifische System-„Know-How“ der Firma Philotech als sehr hilfreich erwiesen. So konnte eine Architektur definiert werden, die keine Zertifizierung hinsichtlich der in der Luftfahrtindustrie üblichen Sicherheitslevel benötigt.

Kooperationsfördernde Kommunikationstechniken wie Telefonkonferenzen, Projekttreffen und Statusmeetings – letztere gemeinsam mit einem Vertreter des Zuwendungsgebers – wurden regelmäßig und effektiv eingesetzt. Unter Ausnutzung synergetischer Effekte wurde das gemeinsam vorhandene Know-how wirkungsvoll in die Projektarbeit eingebracht.

II. Eingehende Darstellung

1 Verwendung der Zuwendung

Die Zuwendung wurde konform zur Antragstellung verwendet. Alle Arbeitspakete des IHP sowie die Unterauftrag der Firma Philotech wurden in vollem Umfang bearbeitet. Für alle anwendungsspezifischen Teillösungen wurden geeignete Lösungen prototypisch umgesetzt. Dies gilt insbesondere auch für die Teilaufgaben, für die während des Projektverlaufes Änderungen in der Zielsetzung notwendig wurden. Darüber hinaus wurde mit dem „Split Device Ansatz“ eine Lösung umgesetzt, die für die angedachten Nutzungsszenarien extrem wichtig ist und die so ursprünglich nicht vorgesehen war. Für die Präsentation der Ergebnisse wurde ein Hardware-Flugzeug Mock-up (Abbildung 13) realisiert, in dem alle angedachten Dienste mit Hilfe der im Projekt entwickelten Soft- und Hardware demonstriert werden können.

2 Erzielte Ergebnisse

2.1 AP1.1 – Top-Level und Systemanforderungen

Im Rahmen des Arbeitspaketes wurden zunächst Top-Level Anforderungen sowie Anforderungen auf Systemebene identifiziert, analysiert und definiert. Die erarbeiteten Resultate wurden im Dokument „VPN Seat - Concept Paper and Top Level System Requirements“ [5] niedergelegt.

Die zugrundeliegende Anwendung ist das Verteilen multimedialer Dienste in einer Flugzeugkabine. Sie erscheint auch im Ergebnis der zurückliegenden Projektarbeit, der dabei gesammelten Erfahrungen sowie nach neuerlicher Prüfung weiterhin sinnvoll und realistisch.

Die meisten der ursprünglich daraus abgeleiteten Anforderungen haben sich bewährt und bestehen weiterhin. Im Folgenden werden daher lediglich die Änderungen zum Ausgangsdokument [5] aufgeführt, die sich durch die inzwischen hinzugewonnenen Erkenntnisse ergeben. In den folgenden Abschnitten diskutieren wir kurz die Anforderungen, zu denen sich während der Bearbeitungszeit des Projektes neue Erkenntnisse ergeben haben.

2.1.1 Systemanforderungen

Req.ID	Name	Ursprüngliche Beschreibung
SRQ_1002	VOIP	The system must run a VoIP application.
SRQ_1203	Cabin I/F	The system must be able to access data services provided by the cabin equipment, such as IFE or the cabin LAN.
SRQ_1303	RFID	The system must be able to read RFID tags.
SRQ_1501	IFE Emulator	An IFE Emulator needs to be established streaming Music & Video.

Tabelle 1 – Ursprüngliche Systemanforderungen, zu denen sich Änderungen ergeben haben.

Für die Vorführung im finalen Demonstrator wurde das Sitz-zu-Sitz Szenario nicht berücksichtigt. Daher erübrigt sich für den Demonstrator die Forderung SRQ_1002 nach einer VoIP-Applikation.

Aus grundsätzlicher, architektureller Sicht und für einen späteren realen Einsatz ist diese Anforderung jedoch weiterhin sinnvoll.
Die tatsächliche Integration eines Unterhaltungssystems (IFE) in den Demonstrator ist für dessen Funktion und Anschaulichkeit nicht kritisch. Die Anbindung an die IFE Programmierschnittstelle ist kein eigentliches Ziel des Projektes. Alternativ kann eine überschaubare Menge multimedialer Daten auch über das herkömmliche Dateisystem bereitgestellt werden. Insofern sind die Requirements hinsichtlich der Schnittstelle zum IFE – SRQ_1203 und SRQ_1501 – obsolet.
Durch die Unterstützung von NFC und inhaltlicher Überlappung erübrigt sich die separate Forderung nach RFID, so dass das Requirement SRQ_1303 entfallen kann.

2.1.2 Middleware-Anforderungen

Req.ID	Name	Ursprüngliche Beschreibung
MRQ_1003	Bluetooth PAN	The middleware must support the bluetooth personal area networking profile.
MRQ_1202	UDP	The UDP protocol must be supported
MRQ_1301	Stream Server	A streaming server capable of streaming multi media content to a remote client should be provided.

Tabelle 2 – Ursprüngliche Anforderungen an die Middleware mit Änderungsbedarf.

Das Bluetooth PAN Profil ist für den Demonstrator nicht zwingend notwendig. Gleichwohl ist es mit Blick auf einen realen Einsatz durchaus wünschenswert. Die Anforderung MRQ_1003 sollte daher aufrecht erhalten werden.
Ebenso ist das UDP-Protokoll nicht unbedingt notwendig, um das Projektergebnis zu demonstrieren. Es ist jedoch wünschenswert in zukünftigen Anwendungen. Die genannte Anforderung MRQ_1202 sollte daher im Katalog verbleiben.
Ein Streaming-Server wird nach den bisher gesammelten Erfahrungen auf der Seat-Unit nicht benötigt. Die entsprechende Anforderung MRQ_1301 kann daher gestrichen werden.

2.1.3 Hardware-Anforderungen

Req.ID	Name	Ursprüngliche Beschreibung
HRQ-1004	RFID	OSI Layers 1 and 2 should be supported
HRQ-3000	Multi-Standard Antenna Solution	Cost and Space requirements call for an integrated antenna solution

Tabelle 3 – Ursprüngliche Hardwareanforderungen mit Korrekturbedarf.

Wie bereits angemerkt, ist die Forderung nach RFID zusätzlich zu NFC entbehrlich. Mithin kann die entsprechende Anforderung HRQ-1004 an die Hardware aus dem Katalog gelöscht werden.
Ebenso ist die Multi-Standard Antenne für die Funktion des Demonstrators nicht maßgeblich, für eine kommerzielle Anwendung jedoch durchaus wünschenswert. Die Anforderung HRQ-3000 sollte daher aufrecht erhalten werden.

2.2 AP1.2 – Architektur und Schnittstellen

Das System wurde als Systemplattform spezifiziert, welche in den späteren Einsatzraum integriert werden kann und als Basis für den zu erstellenden Demonstrator dient. Sie ist in Abbildung 3 dargestellt. Darüber hinaus kann die vorgesehen Systemplattform auch für andere Einsatzzwecke wiederverwendet werden, was die wirtschaftliche Nutzbarkeit der späteren Resultate deutlich erhöht und besonders dem Sinne des Forschungsprojektgedankens entspricht.
Die allgemeine Systemarchitektur ist in Abbildung 2 dargestellt. Sie beinhaltet eine bestimmte Anzahl sogenannter Sitzeinheiten (Seat Units), die durch ein Ethernet Netzwerk sternförmig miteinander verbunden sind.

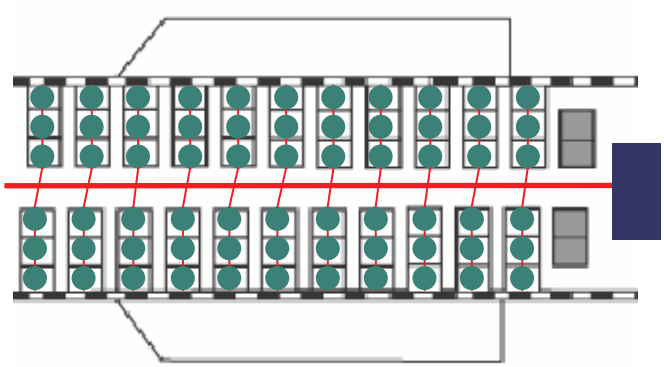

Abbildung 2 Allgemeine Systemarchitektur – Anordnung der Kabinenkomponenten: Sitzeinheiten (grün), Netzwerkinfrastruktur (rot) und Dienstinfrastruktur (blau).

Jeder Sitz, in dem die Nutzung drahtloser VPN-Dienste möglich sein soll, ist mit einer solchen Seat Unit ausgestattet. Aus Sicht des Passagiers fungiert diese als Access Point für die jeweils zur Anwendung kommende Funktechnologie.
Die ausgebrachte Netzwerkinfrastruktur verbindet die Seat Units untereinander und mit der Dienstinfrastruktur der Kabine. Das können zum Beispiel Video-Server, Außenbordkameras oder bestimmte, dafür vorgesehene Sensoren im Flugzeug (Temperatur, GPS) sein.
Für die Durchführung des Projektes wurden keine besonderen Annahmen hinsichtlich der Netzwerkinfrastruktur getroffen. Für eine spätere Produktion ist jedoch wichtig, dass die konkret verwendete Technologie folgende Anforderungen erfüllt:

- Das Netzwerk kann die vorgesehene Anzahl Seat Units auch tatsächlich aufnehmen und
- Es treten keine Interferenzen mit den in den Seat Units verwendeten Funktechnologien auf.

Vier mögliche Applikationsszenarien wurden für den Einsatz in der Flugzeugkabine definiert:

1. Konsumieren von Services mittels vorhandener Hardware
2. Konsumieren von Services mittels mitgebrachter Passagierhardware
3. Intra-Seat Kommunikation
4. Inter-Seat Kommunikation

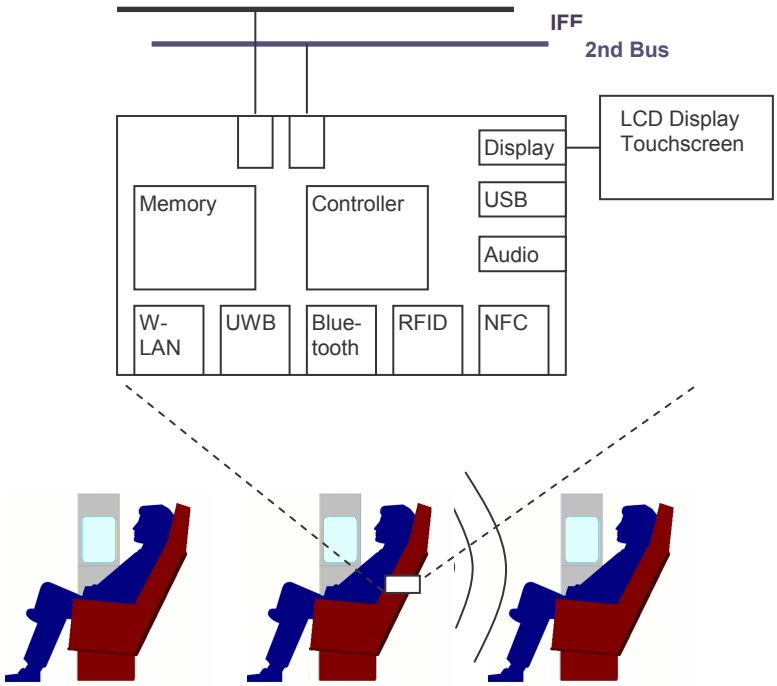

Abbildung 3 – Anwendungskonzept und grobe Systemarchitektur

Das beschriebene System wurde analysiert und als technisch machbar eingestuft. Weitere Details sind im separaten technischen Report „System Architecture“ [6] niedergelegt.

2.3 AP2.1.1 – Entwicklung eines Geräteauswahlverfahrens

Zur Schaffung eines aus Anwendersicht relevanten Demonstrationsfalles wurden zunächst Voruntersuchungen zur verteilten Wiedergabe von Multimedia-Daten unternommen. Im weiteren Verlauf des Arbeitspaketes schlossen sich daran die Aktivitäten zur automatischen Geräteauswahl an.

2.3.1 Voruntersuchung zum Verteilen von Multimedia-Datenströmen

Für das Konsumieren von Diensten mittels vorhandener und mitgebrachter Passagierhardware wurde am Beispiel der Video-Übertragung ein Lösungsvorschlag entworfen. Wird ein Video auf einem Server bereitgestellt, so soll die Audio-Komponente über die Bluetooth-Kopfhörer, die Bildkomponente jedoch über das Notebook-LCD des Passagiers wiedergegeben werden.
Ein Lösungsvorschlag mit minimalen Anforderungen an benötigten Ressourcen wurde erarbeitet. Der Datenstrom wird nach dem MPEG-Splitter aufgetrennt. Der Audio-Teil gelangt noch auf dem Server zum entsprechenden Renderer. Das Ergebnis wird an das als Standard-Audiogerät konfigurierte Bluetooth Headset ausgegeben. Der gesamte Audio-Strom läuft folglich direkt auf dem Server ab. Der Video-Teil wird – noch im komprimierten Zustand – durch einen entsprechenden Server-Filter übertragen (Abbildung 4) und auf dem clientseitigen Notebook dekodiert und gerendert (Abbildung 5). Das folgende Bild zeigt den Filtergraphen auf der Serverseite.

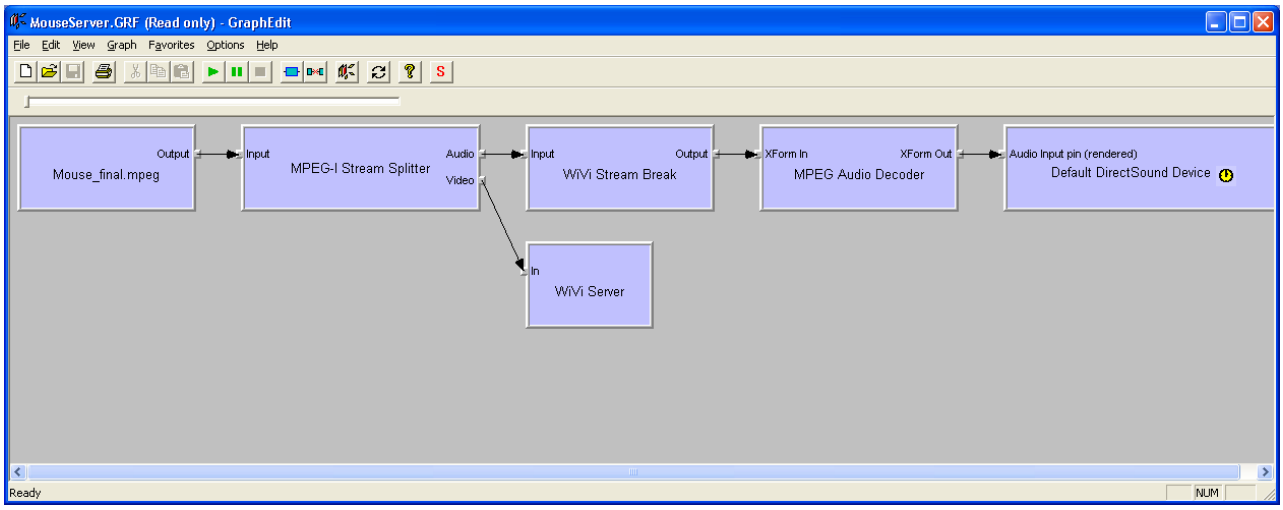

Abbildung 4: Serverseitiger Filtergraph beim Bereitstellen eines Videos. Im Graphen sind die WiVi-Filter unmittelbar nach dem MPEG Splitter Filter angeordnet.

Dieses Verfahren erfordert die geringste Bandbreite. Eine besondere Schwierigkeit stellt hier jedoch die Synchronisation zwischen Video- und Audiodaten dar. In einem ersten Ansatz wurde deswegen auf der Serverseite im verbleibenden Datenstrom eine Strombremse eingesetzt, die den Datenstrom um eine statisch definierte Zeitdauer – die in etwa der Latenzzeit des Netzwerks entspricht – verzögert.

Auf der Clientseite, also dem Notebook, auf welchem die Videodaten angezeigt werden sollen, benötigt man die in Abbildung 5 gezeigte Filterkette.

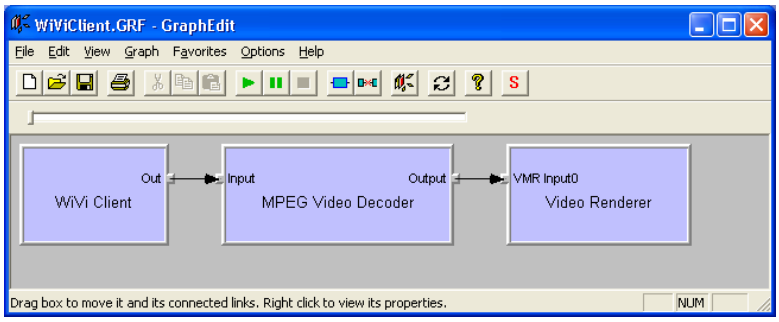

Abbildung 5 Clientseitiger Filtergraph

Um die Machbarkeit dieser IHP-Lösung zu demonstrieren, wurden DirectX-Filter für Windows entwickelt, die den Netzwerkversand eines Datenstroms (WiVi Server und –Client) und ggf. eine Zeitkorrektur (WiVi StreamBreak) übernehmen. Damit ist es schließlich möglich, die Audiodaten auf ein Bluetooth-Headset, die Video-Daten jedoch auf das Benutzer-Notebook zu lenken. Technische Details sind dem technischen Report „Technische Varianten der Videodatenübertragung“ [7] zu entnehmen.

2.3.2 Untersuchungen zur automatischen Geräteauswahl

Aufgrund der im Projekt gewonnenen Erkenntnisse ist davon auszugehen, dass die Geräteauswahl stets durch eine geeignete Benutzerinteraktion unterstützt und letztlich auch legitimiert werden muß. Im Berichtszeitraum wurden nach den notwendigen Vorüberlegungen schließlich konzeptionelle Festlegungen bezüglich der Integration in die Endanwendung getroffen. Demnach kommen zwei Verfahren in Betracht:

- Anmeldung des Passagiers am Sitz mithilfe eines NFC-Tags im Ticket
- Auswahl der automatisch erkannten Geräte und Zuordnung zum privaten Netzwerk

Eine Anmeldung des Passagiers am Sitz könnte dazu dienen, die jeweilige Person (erneut) zu identifizieren. Damit könnten spontane Platzwechsel ermöglicht werden. Sobald der tatsächlich eingenommene Sitz den Passagier erkennt, könnten die jeweils individuell gebuchten Dienste, Filme usw. freigeschaltet werden. Als Identifikationsmedium bietet sich das Ticket an. Ein eingearbeitetes NFC-Tag würde die notwendigen Daten in computerlesbarer Form enthalten. Alternativ könnte auch das NFC-fähige Handy als Datenträger fungieren. Die Anmeldung wird vollzogen, indem der Passagier sein Ticket bzw. Handy an einem NFC-Lesegerät präsentiert, d.h. in unmittelbarer räumlicher Nähe vorbeiführt – s. Abbildung 6. Das Lesegerät ist an einer äußerlich gekennzeichneten Stelle in den Sitz eingebaut und mit der Seat-Unit verbunden.

Eine Realisierung dieses Konzepts wurde im Rückgriff auf vorliegende NFC-Technik (Tag, Lesegerät) erfolgreich implementiert. Das Resultat ist ein Laufzeit-Modul für die Benutzerapplikation. Es erlaubt die Identifikation verschiedener NFC-Tags und die Zuordnung des präsentierten Tags zu weiteren (fiktiven) Fluggast-Daten. Das NFC-Tag kann sich dabei sowohl an einem physischen (Papier-)Ticket, als auch in logischer, virtueller Form auf einem NFC-fähigen Handy befinden.

Abbildung 6 – Datenaustausch per NFC mit einem entsprechend ausgerüsteten Handy

Darüber hinaus erschien es sinnvoll, die automatisch im Umfeld des Sitzes erkannten Geräte dem Benutzer durch die Applikation z.B. in Form einer Auswahlliste zu präsentieren. Hier entscheidet der Benutzer im Einzelfall, ob ein bestimmtes Gerät zu seinem Netzwerk gehören soll, oder nicht. So kann sichergestellt werden, dass ein privates Endbenutzergerät nur an dem Sitz präsent ist, zu dem es gehört. Umgekehrt ist auch Missbrauch vorgebeugt, da die Einbindung eines Gerätes immer auch Interaktion am Gerät selbst erfordert. Insgesamt stellt diese Art Nutzerinteraktion also sicher, dass die mitgebrachten Endgeräte in jedem Fall dem richtigen Sitz zugeordnet werden. In der Verwirklichung dieser Idee entstand ein weiteres Modul für die Benutzerapplikation zur automatischen Erkennung von in der Nähe befindlichen Bluetooth-Geräten. Es erlaubt dem Fluggast die Einzelfall-Entscheidung, ob ein bestimmtes Gerät zu seinem Netzwerk gehören soll, oder nicht.

Beide Verfahren ergänzen einander und können gemeinsam eingesetzt werden. Sie versetzen die Applikation in die Lage, ihre Präsentation z.B. durch eine konkrete Anrede zu personalisieren und geben dem Benutzer die volle Kontrolle über die korrekte Zuordnung seiner Geräte zum Sitz. Im Ergebnis konnten beide Funktionen erfolgreich bei der Abschlußpräsentation demonstriert werden.

2.4 AP2.1.2 – Entwicklung eines Schlüsselauswahlverfahrens

Kryptographische Verfahren sind relativ rechenintensiv. Dieses führt zu zwei Problemen. Erstens können mobile Endgeräte diese Operationen nur für kurze Zeit unterstützen ohne deutliche Einbußen hinsichtlich ihrer Nutzungsdauer in Kauf zu nehmen, d.h. der Nutzer kann sicher oder lange kommunizieren. Zweitens ist uns aus der Airbus-Studie vgl. Kapitel Vorraussetzungen

bekannt, dass die Wärmeentwicklung innerhalb der Kabine ein signifikantes Problem darstellt. Folglich tragen Lösungen, die zu effizienten Implementierungen kryptographischer Verfahren führen, dazu bei, deren Einsatz in VPN Seat Szenarien deutlich zu erleichtern.
Um den Schlüsselaustauschmechanismus auch auf Geräten mit eingeschränkten Ressourcen zu ermöglichen, fiel die Entscheidung auf den Einsatz der Elliptische-Kurven-Cryptographie (ECC). Im Vergleich zu RSA ist ECC ein Public Key Kryptosystem mit kleinerem Schlüssel bei vergleichbarer SIcherheit. Die kleineren Schlüssel verringern die Datenmengen, die übertragen werden müssen.
Um den Stromverbrauch und die damit verbundene Wärmeentwicklung weiter zu reduzieren, kann auch in der Sitzeinheit der Hardwarebeschleuniger für die Kryptooperationen eingesetzt werden. Hier sind besonders die Kurven, die auf binären Feldern basieren, effizient und chipflächegünstig zu implementieren. Das wäre bei einer Massenproduktion der Sitzeinheit die optimale Lösung.

Zunächst erfolgte eine Analyse von Galois-Feld Operationen in der SSL-Implementierung „OpenSSL“. Dabei wurde ein Beschleunigungspotential der vorliegenden Implementation im Vergleich zur Verwendung der iterativen Karatsuba-Methode von etwa 20% ermittelt.
Diese Operationen sind ihrerseits Hauptbestandteil von Signaturverifikation und –Erstellung durch elliptische-Kurven-Methoden. Daher gilt das ermittelte Beschleunigungspotenzial nahezu unvermindert auch für diese Benutzerfunktionen. Durch eine entsprechende Implementation ließe sich also das Benutzerempfinden in diesen Punkten deutlich verbessern. Die folgenden Arbeiten befassen sich mit der weiteren Optimierung der Karatsuba-Multiplikation, um diesen Algorithmus mit minimaler Komplexität in Form eines HW-Beschleunigers implementieren zu können.

Zunächst erfolgte eine Analyse von mehreren Authentifizierungsverfahren der Teilnehmer in ad-hoc Netzen. Die folgenden Probleme wurden entdeckt:

- viele der Verfahren, die bislang als sicher galten, weisen auch Sicherheitslücken auf;
- die Authentifizierung mit RSA oder elliptische-Kurven-Methoden ist zwar sicher aber zeit- und energieaufwendig.

Als mögliche Lösung schlagen wir ein Authentifizierungsverfahren vor, welches auf einer Kombination von asymmetrischer Verschlüsselung und einer Hash-Reihe basiert. Als Veschlüsselungs-Verfahren bieten sich RSA und elliptische-Kurven-Methoden mit kürzeren Schlüsseln für die Initialphase an. Die Hash-Reihe kann auf der Basis von Lamport´s Scheme für die weitere „re-recognition“ der Teilnehmer gewählt werden. Das Ziel ist es eine Art Transitivität der re-recognition bereit zustellen. So kann der Aufbau der Geräte des Benutzers auf das Wiederherstellen und Zusammenführen von Gruppen dieser Geräte zurückgeführt werden, was eine deutliche Reduktion des Aufwandes bedeuten kann. Um den Schlüsselaustausch so effizient wie möglich zu gestalten sollen Verfahren, die auf elliptischer Kurven Kryptographie beruhen eingesetzt werden. Diese bieten eine höhere Sicherheit als RSA bei kürzeren Schlüssellängen und mit geringerem Rechenaufwand. Die aufwendigste Operation in diesen Verfahren ist die Polynom Multiplikation. Die Komplexität dieser Operation nach dem Karatsuba Verfahren wurde während der Projektlaufzeit untersucht. Als weitere Optimierungsmöglichkeit ist die sogenannte Bailey-Multiplikation untersucht worden, um einen Algorithmus mit minimaler Komplexität zu bestimmen.

Im Projektzeitraum wurde eine Methode erarbeitet, die den optimalen Berechnungsweg bzw. Ablaufsplan der Tabellarischen Darstellung des Produktes von n-Bit Polynomen in GF(2n) zeigt. Dabei wurden drei Multiplikationsmethoden untersucht: a) auf der Basis der klassischen Multiplikationsformel, b) vermittels einer iterativen Anwendung der Karatsuba-Methode und c) die Baileys Multiplikationsformeln.

Die iterative Anwendung der Karatsuba-Idee nach dem optimalen Berechnungsplan – im weiteren hier als oIKM bezeichnet – bringt eine durchschnittliche Minderung der XOR- Komplexität der Berechnung um etwa 10% im Vergleich zu den von Paar [8] veröffentlichten Komplexitätswerten.

Die AND-Komplexität ist um ca. 4% verbessert. Für den Vergleich wurden 128-Bit Polynome herangezogen.

Eine weitere Komplexitätsminderung der Multiplikation der n-Bits Polynome kann mit der optimalen Kombination aus oIKM, oIBM und klassischer Multiplikationsmethode erreicht werden. Die erwartete Verringerung der benötigten Chip-Fläche beträgt etwa 20%.
Die Realisierung erfolgte in zwei Stufen. Am Anfang wurden Standard-Kurven, die als sicher identifiziert sind (B-163 und B-233 NIST Kurven), implementiert. Anhand der Ergebnisse, die den Aufwand für die Berechnung zeigen, konnte die Wirkung der Hardwarebeschleuniger quantifiziert werden. Im zweiten Schritt wurde eine weitere Optimierung bezüglich Rechenzeit und Energieverbrauch für die Aufbereitung und Übertragung von Daten - leider nur bei gleichzeitiger Reduktion des Sicherheitsgrades – durch den Einsatz von Kurven mit kürzerem Schlüssel erzielt.
Die Ergebnisse zeigen, dass der oben erwähnte Hardware-Beschleuniger ca. 3 bis 5 Größenordnungen schneller ist, als eine vergleichbare Software-Implementierung.

2.5 AP2.2.1 – Entwicklung einer einheitlichen Protokollschnittstelle

Wegen des angestrebten Einsatzes verschiedener drahtloser Übertragungstechnologien und deren Kommunikationsprotokolle wurde nach Lösungen zur Vermittlung zwischen diesen Protokollen gesucht. Für maximale Transparenz bei der Vermittlung bieten sich die untersten Schichten der Kommunikationsarchitektur an, z.B. MAC Protokoll Layer. Dazu wurden die Parameter der einzelnen MAC-Protokolle in XML beschrieben. Hier wurde insbesondere versucht, die in den Protokollen spezifizierten Parameter auf QoS Parameter abzubilden. Damit soll sich die Tauglichkeit eines Übertragungsweges bzw. Übertragungsprotokolls für einen bestimmten Daten-/Medienstrom mit entsprechenden QoS Anforderungen determinieren lassen. Beispiel-Skripte definieren als XML Schema Description die Syntax einer XML Protokoll Beschreibung. Damit wird eine statische Gültigkeitsprüfung der Beschreibung ermöglicht. Eine entsprechende Protokollvermittlungseinheit kann nun auf deren Basis für gegebene Daten und Medienströme geeignete MAC Protokolle und Übertragungswege auswählen. Abbildung 7 zeigt die entsprechende Architektur. Die XML Beschreibung der QoS und Protokollparameter gestattet zudem die nachträgliche Erweiterung um neue oder zusätzliche MAC Protokolle.

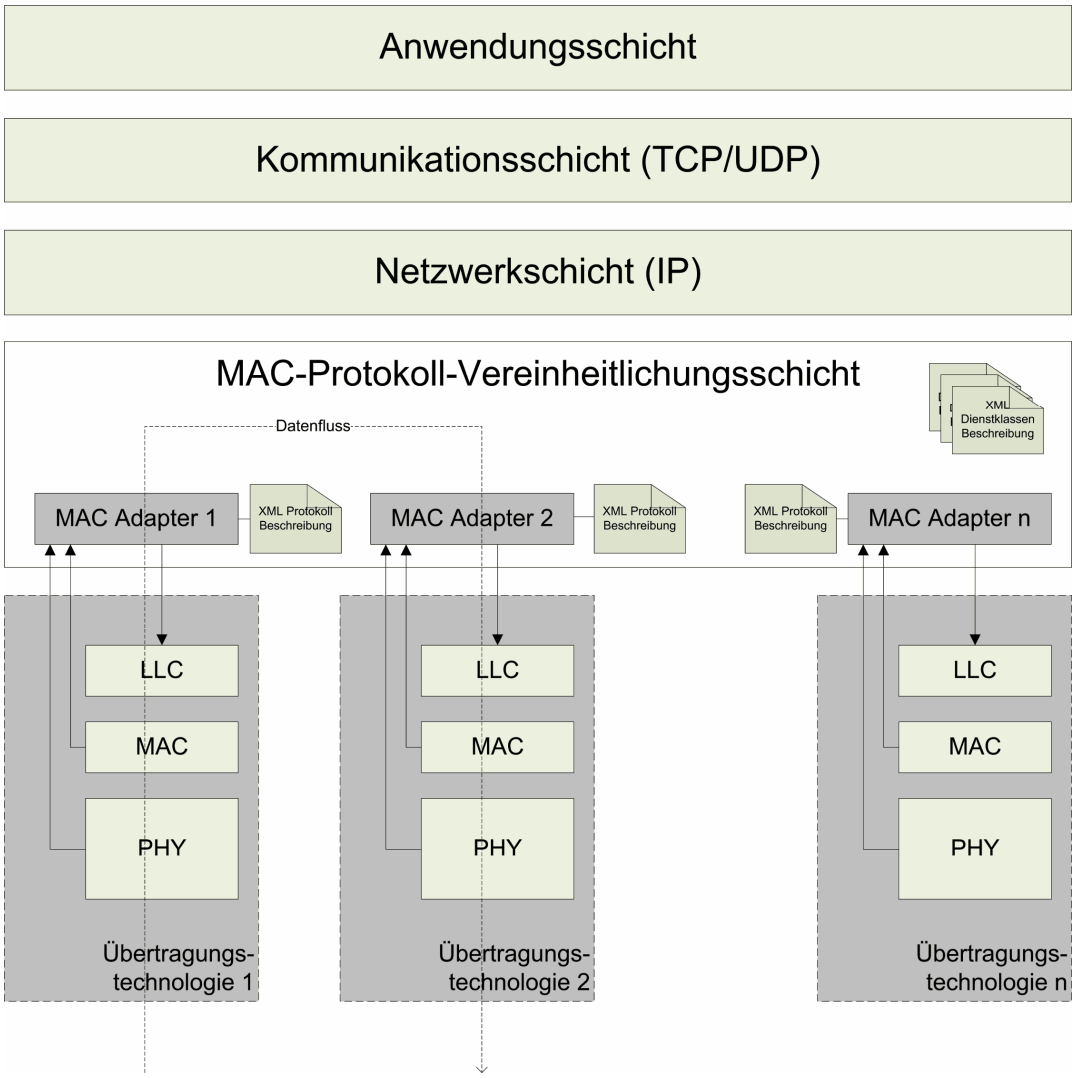

Abbildung 7 – MulitProtokoll Ansatz mit automatischer Übersetzung von QoS Anforderungen zwischen unterschiedlichen Übertragungstechnologien.

Für das VPNSeat Projekt wurde jedoch erkannt, dass die zum Einsatz kommenden Übertragungsverfahren und Protokolle durch die Fähigkeiten der SeatUnit festgelegt sind und eine dynamische Erweiterung nicht notwendig ist. Ebenso ist die Anzahl gleichzeitig übertragener Daten- und Medienströme im Flugzeugsitz vorhersagbar klein. Mit dieser verringerten Dynamik des Gesamtsystems und dem häufigen Fehlen von Alternativrouten (zwischen SeatUnit und Kopfhörer nur Bluetooth), lässt sich eine Multiprotokollvermittlung auch ohne eine derartige XML Beschreibung konstruieren. Insbesondere lässt sich bei direkter Konvertierung die Effizienz verbessern, was unter Berücksichtigung des Energie und Abwärmeproblems von besonderer Bedeutung ist. Sollten in einigen wenigen Fällen dennoch Protokollanforderungsinformationen benötigt werden, so lassen sich diese in den Headerinformationen der darüberliegenden Protokollschichten transportieren und im Einzelfall verarbeiten.

2.6 AP2.2.2 – Einheitliche Service Discovery Protokolle

Hierzu wurde nach Lösungen für eine einheitliche Dienstbeschreibung und daraus resultierenden Möglichkeiten der gemeinsamen Benutzung von Diensten recherchiert. Nach dem ersten Stand der Erkenntnisse ist im Rahmen des DFG-geförderten DIANE-Projektes (Uni Karlsruhe und Uni Jena) ein Ansatz entstanden, der diesem Ziel nahe kommt.

Um den beispielhaften Übergang zwischen zwei Service-Architekturen (z.B. Bluetooth und SLP) mithilfe der DIANE Service Description (DSD) zu demonstrieren, sollten zunächst die benötigten Komponenten entworfen und implemetiert werden.

Im Verlauf des Projektes ausgeführte Experimente stützten weiterhin den Kenntnisstand, dass die DIANE-Platform ein aussichtsreicher Kandidat für eine Basis zur einheitlichen Dienstbeschreibung ist. Die Vermittlung zwischen verschiedenen Service Discovery Protokollen sollte mithilfe der DIANE Service Description (DSDS) realisiert werden. Prototypisch war eine Brücke zwischen zwei bereits verfügbaren Service Discovery Mechanismen, z.B. Bluetooth und NFC vorgesehen.

Letztendlich konnte jedoch eine Umsetzung für realitätsnahe Anwendungen aufgrund der spezifischen technischen Anforderungen nicht erreicht werden. Als hinderlich in diesem Ansatz erwies sich das hohe Abstraktionsniveau, auf dem in DIANE Dienste beschrieben, angeboten und vermittelt werden.
Technisch nutzbare und derzeit verfügbare Repräsentationsformen der DIANE Service Description (DSD) Language liegen auf dem Niveau von Java und OWL. Für die Einbeziehung von Hardware und hardwarenahen Diensten (NFC, Bluetooth, RFID) bedarf es einer individuellen Nebenrepräsentation von DSD. Deren Entwicklung kann – auch in Anbetracht der dann notwendigen Unterstützung durch z.B. automatische Generatoren usw. – im Rahmen der hierfür zur Verfügung stehenden Projekt-Ressourcen nicht mit hinreichender Aussicht auf Erfolg betrieben werden.
Darüber hinaus bedarf es eines weiteren Teils der Dienstbeschreibung – des sogenannten Groundings. Es beschreibt den Zusammenhang zwischen der abstrakten Beschreibung eines Dienstes und der zugehörigen konkreten, ausführbaren Funktion. In DSD gibt es sowohl für die Angebots- als auch für die Anfragebeschreibung ein Grounding. Da Angebot oder Anfrage – und in manchen Szenarien sogar beide – von Endgeräten des Benutzers ausgehen, führt dies zur Notwendigkeit einer vorinstallierten Client-Software, die dieses Grounding übernehmen könnte. Das wiederum steht im Gegensatz zum ursprünglichen Konzept, keine besonderen Anforderungen – über die standardisierten Technologien hinaus – an die Endgeräte des Passagiers zu stellen.

Alternative Konzepte zur einheitlichen Beschreibung von Diensten durch ein gemeinsames Service Discovery Protokoll wurden daher in die Betrachtungen wiederaufgenommen. Dabei gelangten proprietäre Lösungen für ein bilaterales Bridging zwischen verschiedenen Service Discovery Protokollen ins Blickfeld. Im Ergebnis sind das Bluetooth Extended Service Discovery Profile (ESDP) für die Vermittlung zwischen Bluetooth und UPnP sowie anwendungsspezifische Gateways zwischen Bonjour und UPnP als verwertbare Alternativen zu nennen. Aufgrund fehlender Anwendungsmöglichkeiten wurde die Integration in den Demonstrator unterlassen.

2.7 AP4.1 – Entwicklung der Demo-Anwendung

Die Anwendungsentwicklung zeigte im Berichtszeitraum wesentliche Ergebnisse. Das Hauptaugenmerk lag dabei auf einer ansatzweisen Ausprägung möglichst vieler Funktionen. Die entstandene Anwendung läuft auf einer Multistandard Protokoll- und Hardwareplattform, die UWB, WLAN, NFC und Bluetooth als Übertragungstechniken beinhaltet.

Für die Realisierung kamen etablierte Web-Technologien (HTTP) zum Einsatz, die client-seitig lediglich einen Web-Browser, also eine weit verbreitete Client-Software voraussetzen. Die benutzerseitigen Systemvoraussetzungen bleiben damit moderat. Die Anwendung ist nahezu intuitiv bedienbar.

Zunächst wurde eine Webbrowser-fähige GUI erstellt, die es erlaubt, Videos auf der Seat-Unit abzuspielen. Mit den Fortschritten in den anderen Arbeitspaketen konnten schließlich auch die gewünschten finalen Ergebnisse erreicht werden.

Im Rahmen einer Demonstration erlaubt die Anwendung in der Reihenfolge des Gebrauchsflusses zunächst die Identifikation des Benutzers am Sitz. Damit geht im weiteren Verlauf eine Entsprechende Personalisierung (Anrede) einher – Abbildung 8.

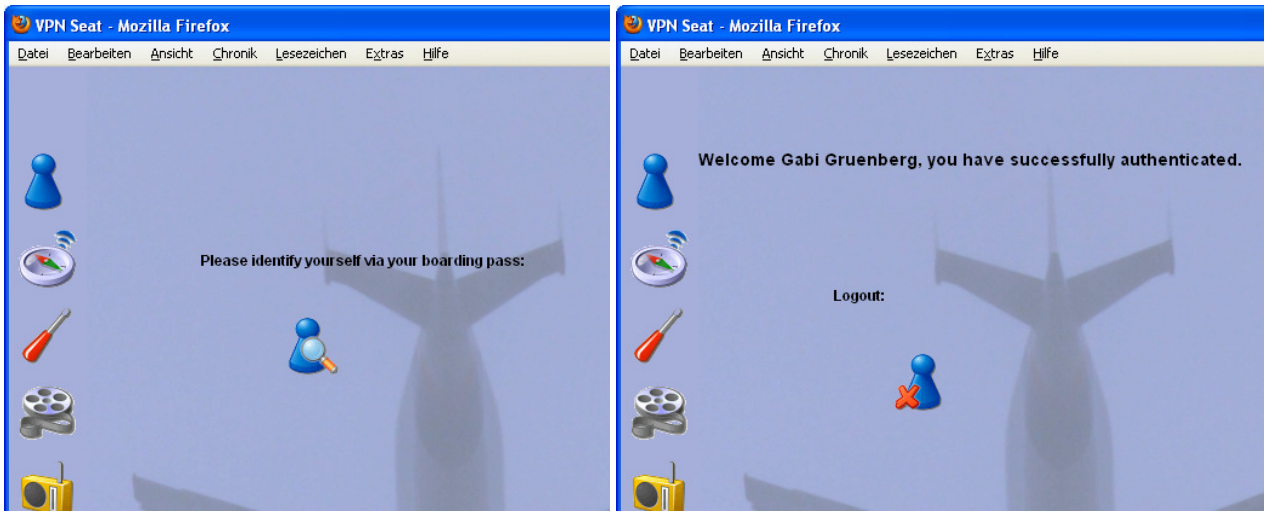

Abbildung 8 – Web-Anwendung bei der Anmeldung eines Benutzers mittels NFC-Tag

Danach wählt der Benutzer die zu ihm gehörenden Bluetooth-Geräte aus. Dabei wird das applikationsinterne service discovery demonstriert - Abbildung 9.

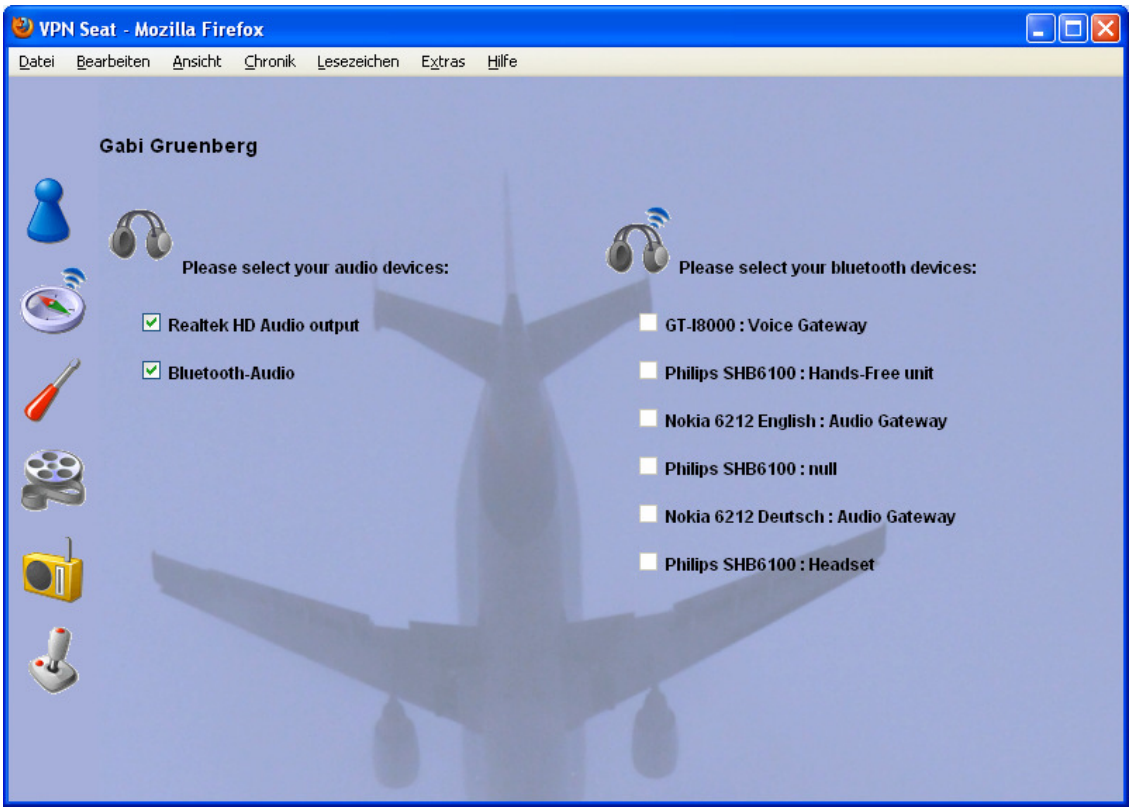

Abbildung 9 – Nachdem die Web-Anwendung automatisch die Bluetooth-Geräte in der Nähe erkannt hat, bietet sie dem Benutzer die Möglichkeit der manuellen Selektion.

Nun ist bereits eine sinnvolle Nutzung der Hauptfunktion möglich. Die Abbildung 10 zeigt die clientseitige Wiedergabe eines aufgetrennten Videostromes in der Split-Device-Technik.

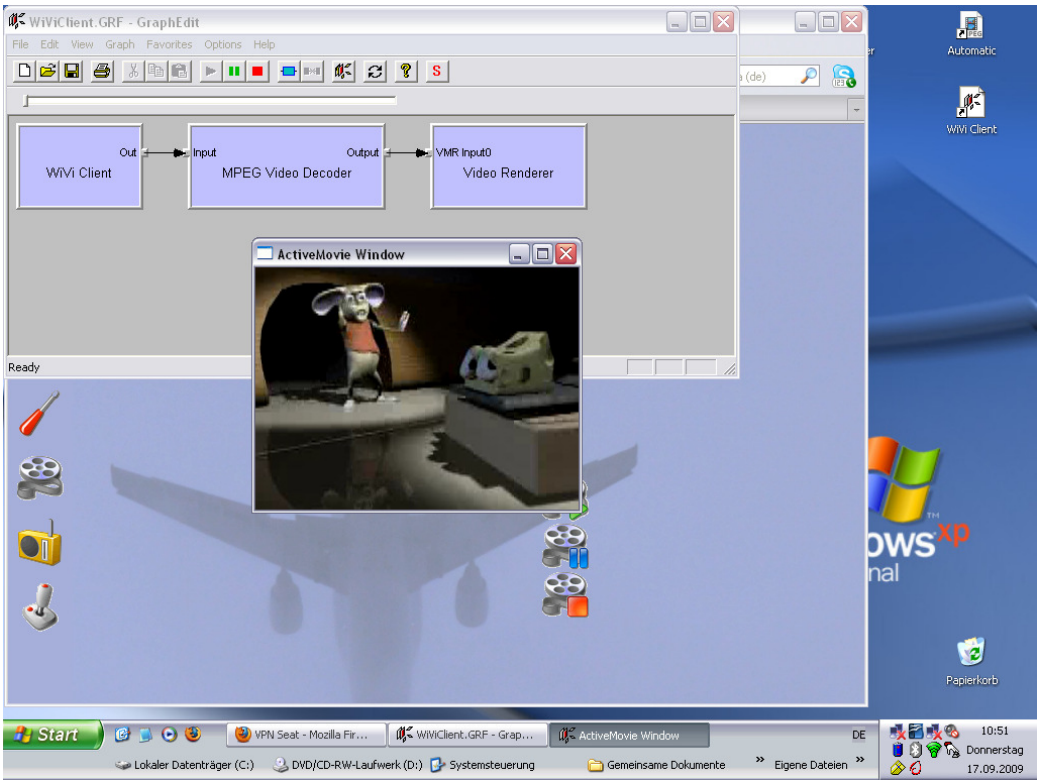

Abbildung 10 – Web-Anwendung beim Abspielen eines Videos.

Die konkrete Verteilung einzelner Medienströme kann in einer entsprechenden Einstellungsseite vorgenommen werden (Abbildung 11).

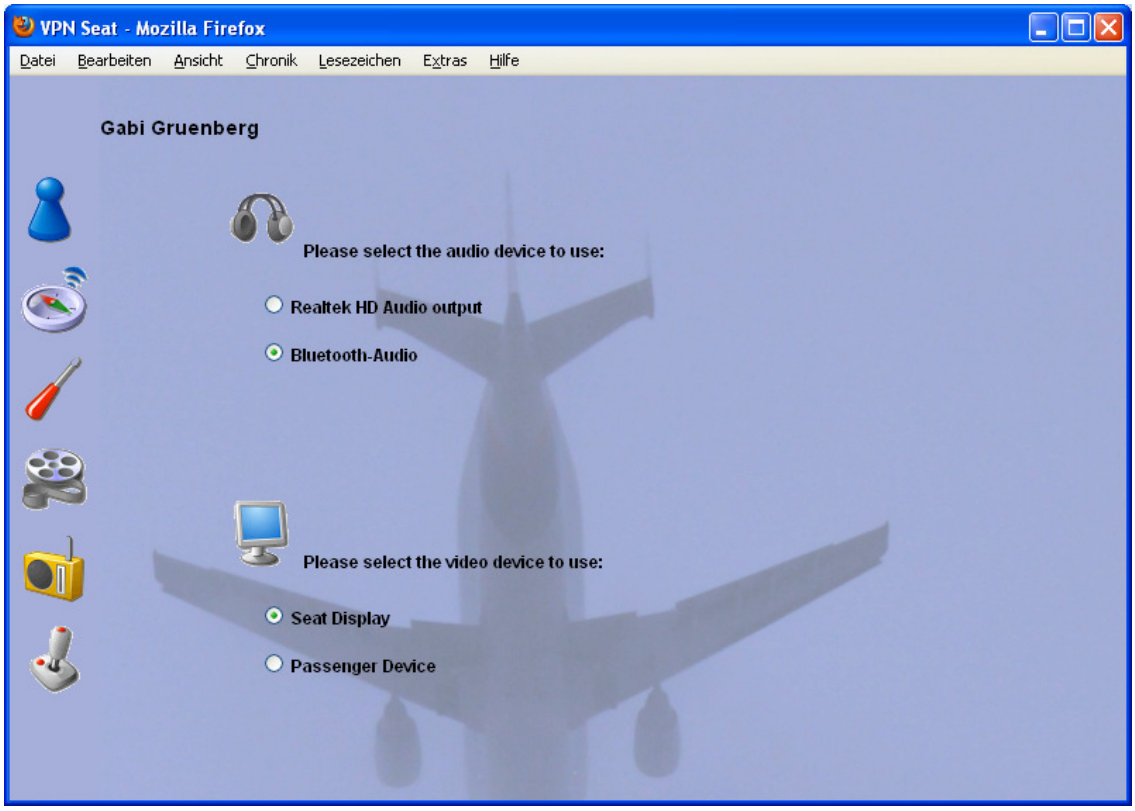

Abbildung 11 – Web-Anwendung des Passagiers. Im Bild die Konfiguration der Ausgabegeräte für verschiedene Medienströme – „Audio device“, „Video device“

Zur Veranschaulichung weiterer Vorteile, die ein Passagier aus der Nutzung einer solchen Seat-Unit potentiell haben könnte, wurde stellvertretend noch ein Spiel – hier Sudoku – in die Applikation integriert (Abbildung 12).

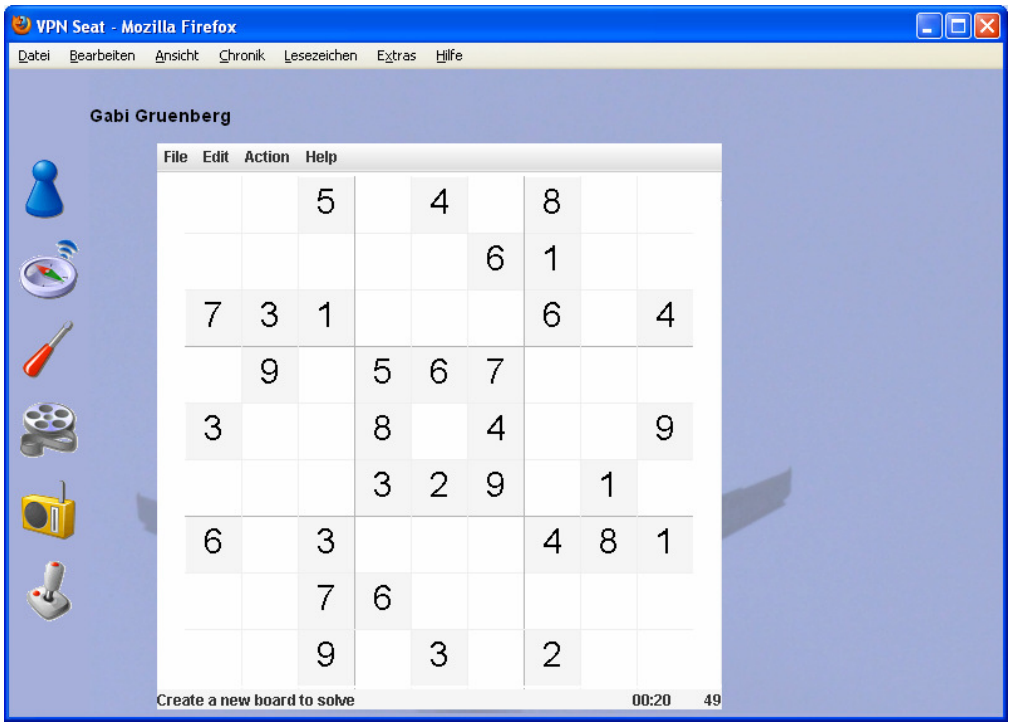

Abbildung 12 - Beispielhafte Implementation eines Spiels.

2.8 AP4.2 – Aufbau des Demonstrators

Hinsichtlich der Konzeption des Demonstrators traten zunächst Schwierigkeiten bei der Beschaffung von NFC-Geräten zu tage. Eine Einbeziehung dieser Technologie in den finalen Demonstrator war fraglich, konnte letztendlich aber doch wenigstens für einen Sitz gewährleistet werden.

Im letzten Projektabschnitt ist der Aufbau des finalen Demonstrators wesentlich vorangeschritten. Die für den realistischen Eindruck notwendige Staffage wurde fertiggestellt und steht für Versuche und Vorführungen zur Verfügung – s. Abbildung 13. Anschließend konnte die technische Ausrüstung in den Demonstrator integriert und in Betrieb genommen werden.

Bereits am Tag der offenen Tür am 5.9.2009 konnte das IHP seinen Gästen einen ersten Eindruck über die Projektergebnisse vermitteln. Der vollständige Demonstrator wurde dem Zuwendungsgeber beim Projektabschlußtreffen am 9.12.2009 erfolgreich präsentiert.

Abbildung 13 - Erste Vorstellung des betriebsbereiten Demonstrators am IHP beim Tag der offenen Tür am 5. September 2009

3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Für die gemeinsame Nutzung der Flugzeug-Infrastruktur im Sinne des Inflight Entertainment Systems mit Geräten des Passagieres gibt es bis heute keine bekannte Lösung. Aus Sicht der Projektpartner ist eine Technologie, die eine Integration der Systeme in eine Gesamtlösung jedoch eine interessante Option, die zum einen wissenschaftlich-technische Fragestellungen aufwirft, die geklärt werden konnten, und zum anderen eine wirtschaftliche Relevanz haben.

Für die im Rahmen dieses Projektes untersuchten Fragestellungen existieren keine allgemein anerkannten oder gar standardisierten Lösungen. Vielmehr wird in einigen Bereichen noch sehr intensiv an ähnlichen bzw. gleichen Fragestellungen geforscht. Die Arbeiten waren also aus wissenschaftlich technischer Sicht notwendig um Aussagen zur Umsetzbarkeit der Basisidee des VPN-Seat Ansatzes machen zu können. Zu allen Arbeitspaketen wurden intensive Untersuchungen sowohl theoretischer Natur, wie Berechnung der Komplexität von Implementierungen kryptographischer Verfahren, als auch experimenteller Art z.B. zur Nutzung generalisierter Service Discovery Mechanismen wie DIANE durchgeführt. Darüber hinaus wurden prototypische Implementierungen für die untersuchten Ansätze umgesetzt und in einen Demonstrator integriert. Die umfänglichen Implementierungsarbeiten haben gezeigt, dass ein System wie das des VPN Seat nicht nur prinzipiell machbar ist, sondern klar aufgezeigt, dass eine Umsetzung auf der Basis heute zur Verfügung stehender Mittel möglich ist.

4 Voraussichtlicher Nutzen

Eine Verwertung der VPN Seat Ergebnisse kann in unterschiedlichen Kontexten erfolgen. Eher langfristig ist die kommerzielle Vermarktung der Ergebnisse zu sehen. Hier gibt es unterschiedliche Einsatzbereiche:

- Flugverkehr,
- Eisenbahnen,
- Reisebusse.

Im Flugverkehr könnten die VPN-Seat Techniken bei „Low Cost“ Airlines zum Einsatz kommen, die ausschliesslich die Software nutzen um ihren Kunden zusätzliche Unterhaltungsdienste anbieten zu können. In Gegensatz hierzu könnten die VPN-Seat Techniken inklusive einer Hardware-Realisierung der Sitzeinheit bei Fluglinien im Business Bereich vermarktet werden. Auch für die Bereiche Eisenbahnen und Reisebusse könnten Einstiegsvarianten die ausschliesslich Software basiert sind, sowie komplexere Installationen, die auch Hardware integrieren anvisiert werden.

Neben dem Vertrieb der Soft- und Hardware könnten zusätzliche Dienstleistungen auf der VPN Seat Plattform angeboten werden.

Hinsichtlich der Vermarktungschancen müssen jedoch folgende Einschränkungen gemacht werden. Die vorliegende Prototypische Lösung ist noch deutlich von einem Vorprodukt entfernt. Hier bedarf es eines signifikanten Aufwandes für die Weiterentwicklung in Richtung Produkt. Der IFE Markt wird von sehr wenigen Firmen dominiert, hier sind kurzfristige Erfolge unwahrscheinlich.

Der Demonstrator wurde bereits der Öffentlichkeit vorgestellt und wird auch in der Zukunft für weitere Projekte sowie in Lehre und Ausbildung eingesetzt. Zur Zeit ist es geplant den VPN-Seat Demonstrator auch im Projekt Easy-A zu Demonstrationszwecke zu verwenden. In diesem Projekt untersucht das IHP 60GHz Technologien zur schnellen drahtlosen Verbreitung von MultiMedia Inhalten. Dieses passt sehr gut zum VPN Seat Demonstrator. Im Rahmen der Weiterverwendung des Demonstrators im easy-A Projekt ist es geplant die EADS Mitarbeiter, des easy-A Projektes für die VPN-Seat Technologien zu begeistern und so evtl. die Techniken an einen Technologiekonzern im Flugzeugbau zu transferieren.

Die VPN-Seat Ergebnisse sowie der Demonstrator wurden bereits für eine Lehrveranstaltung mit der BTU Cottbus genutzt. Im Rahmen dieser Lehrveranstaltungen haben Studenten Verwertungsideen für die VPN-Seat Techniken entwickelt.

Neben der Nutzung der Gesamtidee können auch besonders geeignete Teilaspekte verwertet werden. Hierzu hat das IHP erste Schritte unternommen. Die Betrachtungen zur Komplexität der kryptographischen Operationen haben zu einem neuen Ansatz zur Umsetzung von Hardware-Beschleunigern für diese Operationen geführt, für den das IHP aktuell eine Patentanmeldung anstrebt. Die Anmeldung wird noch 2010 abgeschlossen.

5 FE-Ergebnisse von dritter Seite

Es sind zum momentanen Zeitpunkt keine FE-Ergebnisse von dritter Seite bekannt, die die wesentlichen Projektziele beeinflussen.

6 Veröffentlichungen des Ergebnisses

Während der Projektlaufzeit sind keine wissenschaftlichen Veröffentlichungen entstanden. Nach Abschlusss der Arbeiten sind die Ergebnisse der Untersuchungen zur einheitlichen Protokoll-Schnittstelle jedoch in folgende Veröffentlichung eingeflossen:

> M. Maaser, P. Langendörfer, St. Nowak, Automated Mapping of MAC Parameters into Generic QoS Parameters by Inter-MAC Adaptors, Special Session part of PIMRC, 2010

Desweiteren ist eine Veröffentlichung zur effizienten Implementierung unterschiedlicher elliptischer Kurven geplant, die erfolgen soll, sobald die Patenteinreichung zum gleichen Thema abgeschlossen ist.

7 Referenzen

[1]	“Semantic Service Discovery with DIANE Service Descriptions”, Ulrich Küster, Birgitta König-Ries, Proceedings of the International Workshop on Service Composition & SWS Challenge at the 2007 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2007), Silicon Valley, USA. November 2007
[2]	"Efficient Context-aware Service Discovery in Multi-Protocol Pervasive Environments", Yerom-David Bromberg, Valérie Issarny, Pierre-Guillaume Raverdy, In Proceedings of IEEE International Conference on Mobile Data Management (MDM), 2006.
[3]	"Osda: Open service discovery architecture for efficient cross-domain service provisioning", N. Limam, J. Ziembicki, R. Ahmed, Y. Iraqi, D. T. Li, R. Boutaba and F. Cuervo, Comput. Commun., vol. 30, no. 3, pp. 546-563, February 2007
[4]	"ReMMoC: A Reflective Middleware to Support Mobile Client Interoperability", Paul Grace, Gordon S. Blair, Sam Samuel, In Proceedings of International Symposium on Distributed Objects and Applications, 2003.
[5]	“VPN Seat – Concept Paper and Top Level System Requirements”, S. Hackenberg (TES), O. Maye (IHP), M. Manck (Philotech), 27.4.2007, Customer/company confidential
[6]	„System Architecture“, S. Hackenberg (TES), O. Maye (IHP), M. Manck (Philotech), 15.5.2007, Customer/company confidential
[7]	“Technische Varianten der Videodatenübertragung”, O. Maye (IHP), 18.2.2008, Customer/company confidential
[8]	“Generalization of the Karatsuba Algorithm for Efficient Implementations”, A. Weimerskirch and C. Paar, Technical Report, Ruhr-Universität Bochum, Gemany, 2003, http://eprint.iacr.org/2006/224

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel VPN Seat – Drahtloses Virtuelles Netzwerk für die Kommunikation durch den Passagier	
4. Autor(en) [Name(n), Vorname(n)] Langendörfer, Peter Maye, Oliver	5. Abschlussdatum des Vorhabens 31.12.2009
	6. Veröffentlichungsdatum
	7. Form der Publikation
8. Durchführende Institution(en) (Name, Adresse) IHP GmbH, Frankfurt (Oder)	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 20 K 0606 A
	11. Seitenzahl 22
12. Fördernde Institution (Name, Adresse) Bundesministerium für Wirtschaft und Technologie (BMWi) 10115 Berlin	13. Literaturangaben 8
	14. Tabellen 3
	15. Abbildungen 13
16. Zusätzliche Angaben	
17. Vorgelegt bei (Titel, Ort, Datum)	
18. Kurzfassung Das übergeordnete Ziel des vom BMWi im Rahmen von "LuFo" geförderten Projektes VPNSeat bestand darin, Flugpassagieren ein "Drahtloses Virtuelles Privates Netzwerk (VPN)" am Sitz durch Einsatz innovativer Technologien bereitzustellen. In dieses Netzwerk sollen die mobilen Endgeräte des Passagiers und die zum Sitz gehörende System-Plattform integriert sein. So wird die Verwendung der persönlichen Endgeräte, mit ihren individuellen Einstellungen, bei der Nutzung der Onboard Dienste ermöglicht. Die geplante automatische Integration der Endgeräte in die Infrastruktur nimmt dem Passagier und den Flugbegleitern auch die Last der Konfiguration des Systems ab. Elektronische Geräte des Passagiers (zum Beispiel Notebooks, PDAs oder Mobiltelefone) unterstützen regelmäßig eine Reihe von Funkschnittstellen nach den unterschiedlichsten Standards und Normen. Der VPN-Master im Sitz als Bestandteil der zu entwickelnden Plattform wird diese Funkschnittstellen und verschiedene Kommunikationsdienste unterstützen und somit die Integration und Vernetzung der Geräte des Passagiers ermöglichen. Die Plattform ermöglicht eine Verbindung zur flugzeuginternen Kommunikationsinfrastruktur. Die Herausforderungen hierbei sind einerseits die Geräte- und Diensteauswahl, insbesondere wegen der räumlichen Nähe zu den Nachbarsitzen, die Sicherung der Privatsphäre und die Integration unterschiedlicher Standards im Bereich der drahtlosen Kommunikation und der Kommunikations-Protokolle.	
19. Schlagwörter VPN, Flugzeug, WLAN, BlueTooth, UWB, NFC	
20. Verlag	21. Preis