Ausarbeitung

Milen Koychev

Personalisieren von Diensten

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Milen Koychev

Personalisieren von Diensten

Ausarbeitung im Rahmen der Vorlesung Anwendungen 1
im Studiengang Informatik
am Studiendepartment Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuer : Birgit Wendholt
Zweitbetreuer: Prof. Dr. rer.nat. Kai von Luck

Abgegeben am 19. Juli 2006

Milen Koychev

Thema der Ausarbeitung

Personalisieren von Diensten

Stichworte

Personalisieren, Diente, Benutzeridentifikation, Net-Passport, Liberty Alliance Project, Identitäts-Metasystem, InfoCard, Platform for Privacy Preferences, regelbasierte Personalisierung, kollaboratives Filtern, Feedback-Personalisierung

Kurzzusammenfassung

Die Entwicklung der Kommunikationstechnologien heutzutage fordert die Entstehung eines reichen Dienstangebotes und starker Kunkurenz zwischen den einzelnen Dienstanbieter. Um bestmöglichen Service einem Kunden anzubieten und somit den Konkurenzkampf zu gewinnen, wird das Personalisieren von Diensten eingesetzt.

Diese Ausarbeitung behandelt die Grundaspekte der Personalisierung und bewertet dessen denkbaren Einsatz in dem studentischen Projekt „Flughafen“ im Studiengang Informatik-Master im Wintersemester 2006/2007.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung und Motivation

Die heutzutage existierenden bzw. sich schnell entwickelnden Technologien im Bereich des Informationsaustauschs ermöglichen den Menschen, Dienste und Produkte bequem zu konsumieren bzw. bequem anderen Menschen (in diesem Fall als Benutzer oder Kunden bezeichnet) anzubieten. Diese Entwicklung fördert die Entstehung einer vielfältigen Reihe von Dienst- und Produktangeboten sowie die Konkurrenz zwischen den Dienstbetreibern und Produktanbietern. Um den Wünschen, Erwartungen und Bedürfnissen des Benutzers entgegenzukommen und somit die Existenz aus wirtschaftlicher Sicht eines Dienstangebotes zu sichern, wird die Personalisierung eingesetzt.

Die Personalisierung ist nach [Pashtan05] als der Gebrauch benutzerspezifischer Daten, um die Interaktionen zwischen jedem einzelnen Benutzer und dem Dienstanbieter anzupassen, definiert. Dabei steht der Benutzer im Fokus einer solchen Interaktion. Die Personalisierung verfolgt folgende Ziele:

- **Kundenwünsche im Voraus erraten:** Die Personalisierung lässt zu, die Bedürfnisse der Nutzer festzustellen, zuzuordnen und dauerhaft zu speichern. Dadurch haben die Dienstanbieter die Möglichkeit, auf diese Bedürfnisse einzugehen und entsprechend dem Benutzer das Dienstangebot im Voraus anzupassen und zu planen.
- **Interaktion verbessern:** Die Verbesserung der Interaktion enthält zwei Aspekte. Der erste Aspekt ist, die Kommunikation zwischen den beiden Parteien (Benutzer und Dienstanbieter) zu optimieren. Dieser gewinnt an Bedeutung im Bereich der mobilen Anwendungen. Repräsentativ für solche Anwendungen sind die begrenzten Ressourcen. Die Nutzer setzen mobile Rechner[1] (mobile Clients) ein, um Dienstangebote zu konsumieren. Die Interaktionmöglichkeiten sowie die vorhandenen Rechenkapazitäten bei diesen Rechnern sind knapp. Hinzu muss beachtet werden, dass die mobilen Clients ganz unterschiedliche Ausstattung (Fähigkeiten) haben können. Die Personalisierung bietet Möglichkeiten, trotz der unterschiedlichen und begrenzten Fähigkeiten der mobilen Clients, eine „sinnvolle“ Interaktion durchzuführen. In einem solchen Szenario werden die Informationen an die Fähigkeiten des Benutzers bzw. seiner Ausstattung dynamisch angepasst. Der Zweite Aspekt der Personalisierung in Hinsicht auf die Interaktion ist, den Reiz der Interaktion zu steigern, indem der Benutzer die Möglichkeit hat, bestimmte Eigenschaften selbst zu gestalten. Beispiel dafür sind die personalisierten Web-Seiten der Dienstanbieter (z.B. [amazon] oder [my.yahoo]). Der Benutzer kann das Aussehen der Seite sowie die Inhalte in einem gewissen Rahmen selbst bestimmen.
- **Kundenbindung stärken:** Dieses Ziel kann als Folgerung aus den oben genannten Zielen betrachtet werden. Durch die Personalisierung bestreben die Dienstanbieter, die Kundenzufriedenheit und Loyalität zu steigern und somit den Kunden für sich zu gewinnen.

Diese Ausarbeitung soll einen Überblick über das Personalisieren von Dienstangeboten geben und dessen denkbaren Einsatz in dem studentischen Projekt „Flughafen“ im Studiengang Informatik-Master im Wintersemester 2006/2007 bewerten. Die Arbeit bezieht sich im Wesentlichen auf die im Literaturverzeichnis angegebenen Quellen.

[1] Mobile Rechner wie Personal Digital Assistants (PDA) oder Mobilfunktelefone

2 Grundlagen

In diesem Kapitel werden die technischen Grundlagen zum Thema „Personalisieren von Diensten“ erläutert. Dabei werden die verschiedenen Einsätze bei unterschiedlichen Problemstellungen vorgestellt und bewertet.

2.1 Personalisieren von Diensten

Das Thema umfasst laut Fachliteratur (z.B. [Jagoe03]) folgende drei Unterthemen:

- Benutzeridentifikation,
- Verwalten personalisierter Daten,
- Anpassen des Dienstangebotes.

Die oben genannten Unterthemen werden im Weiteren vorgestellt. Dabei wird mehr auf die Inhalte eingegangen, die für das Projekt im nächsten Semester relevant sein könnten.

2.1.1 Benutzeridentifikation

Ein wichtiger Punkt der Personalisierung ist, die Möglichkeit eines Benutzers sich den Dienstanbietern gegenüber auszuweisen. Dieser Prozess wird in der Fachliteratur als Benutzeridentifikation bezeichnet. In diesem Kapitel wird die Benutzeridentifikation auf Grund von persönlichen Gegenständen, biometrischen Merkmalen und Geheimwissen vorgestellt.

Die Identifikation durch persönliche Gegenstände baut darauf auf, dass der Benutzer durch seinen persönlichen Besitz sich dem Dienstanbieter gegenüber ausweist. Der Benutzer muss diesen immer parat haben, um einen Dienst in Anspruch nehmen zu können. Dieser Besitz kann z.B. ein Radiofrequenz-Identifikation- (RFID) Chip (für weitere Informationen zu dieser Technologie s. [Finkenzeller02]), eine Chip-, eine Smart- und bei vielen mobilen Anwendungen die Sim-Karte sein.

Abbildung 2-1 RFID-Chip

Die Informationen, die diese Gegenstände in sich speichern, reichen um den Benutzer zu identifizieren.

In den letzten Jahren gewinnt die Identifikation durch biometrische Merkmale an Bedeutung [dermalog]. Die Basis dieser Identifikationsart bilden die biologischen Besonderheiten des Menschen wie z.B. Iris- oder Finger-Abdruck. Diese sind bei jedem Menschen eindeutig. Eine solche Identifikationsart weist mehrer Vorteile auf:

- Der Mensch ist von Geburt mit seiner „Identifikation“ ausgestattet.
- Die Fälschungssicherheit ist extrem hoch.

- Die Gültigkeitsdauer ist extrem lang.
- Die Kosten für den langfristigen Betrieb sind gering.

Den Vorteilen stehen auch einige Nachteile gegenüber:

- Die Kosten für die erstmalige Beschaffung und Einrichtung von biometrischen Systemen sind relativ hoch.
- In der Praxis tauchen oft Probleme auf, wenn die biometrischen Merkmale gestört sind: Kleinigkeiten wie Schwielen, Blasen, Verletzungen oder Ähnliches stellen beispielsweise ein Gerät zur Erkennung der Handgeometrie vor echte Schwierigkeiten.

Eine spannende Entwicklung auf dem Gebiet der Biometrie ist der biometrische Reisepass (auch als ePass – elektronischer Reisepass bekannt).

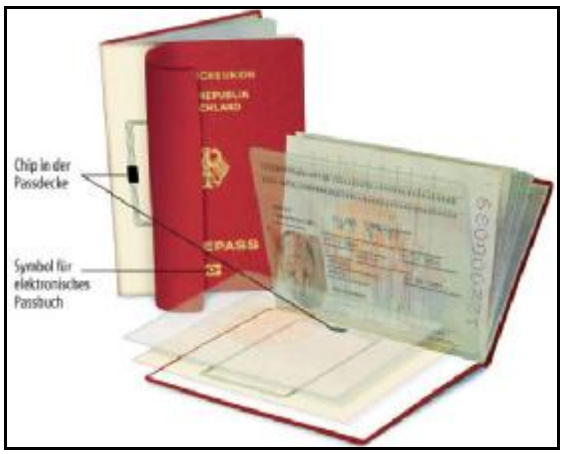

Abbildung 2-2 Biometrischer Reisepass [dermalog]

Er unterscheidet sich von den herkömmlichen Reisepässen dadurch, dass er Personendaten nicht nur in Schriftform, sonder auch in elektronischer Form enthält. Dabei werden neben den ursprünglichen Personendaten auch biometrische Merkmale gespeichert [dermalog]. Somit bindet der biometrische Reisepass die oben beschriebenen Identifikationsarten (Identifikation durch persönliche Gegenstände und durch biometrische Merkmale) zusammen. Momentan existieren viele Pro und Kontra in Hinsicht auf den Einsatz des biometrischen Reisepasses. Die Aussage, ob er sich in der Realität bewährt, wird erst nach seiner Einführung (in Deutschland ab 2007 geplant) möglich.

Eine weitere Identifikationsart ist die Identifikation durch Geheimwissen. Der Benutzer weist sich dem Dienstanbieter gegenüber auf Grund geheimer Informationen aus. Ein sehr verbreiteter Vertreter ist das auf einem Benutzernamen und einem Passwort basierende Loginverfahren. Im Folgenden wird nicht das Loginverfahrten, sondern die Weiterentwicklungen dieses Ansatzes „die zentrale Anmeldestelle“ und „das Indentitäts-Metasystem“ vorgestellt.

Laut [Jagoe03] entstand die Idee der zentralen Anmeldestelle Ende der 90-er Jahre. Zu dieser Zeit bewirkte die Entwicklung des Internets, dass die Desktoprechner bzw. Desktopsysteme an Bedeutung verloren haben. Dabei kam der Trend auf, Softwaresysteme explizit für den Einsatz im Internet zu entwickeln. Das Internet wurde nicht nur als Kommunikationsmedium gesehen, sondern musste auch die Rolle eines großen Betriebssystems übernehmen und bestimmte Dienste den Benutzern anbieten.

Einer dieser Dienste ist die Benutzeridentifikation. Dieser Dienst sollte durch den Identitätsprovider in Form der zentralen Anmeldestelle (s. Abbildung 2-3) realisiert werden.

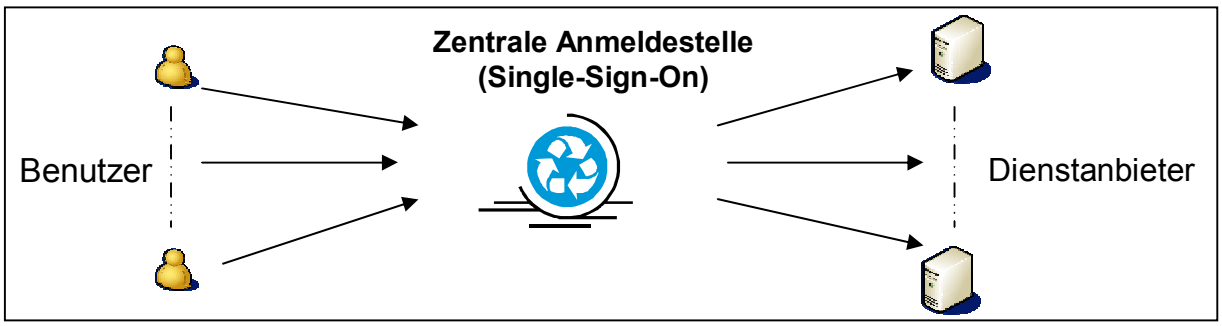

Abbildung 2-3 Zentrale Anmeldestelle - Architektur

Die Architektur dieses Identitätsproviders sieht eine zentrale Instanz vor, die die Identität im ganzen System verwaltet. Die Benutzer des Systems registrieren sich bei der zentralen Instanz mit entsprechenden Benutzerinformationen (z.B. E-Mail-Adresse und Passwort). Der Identitätsprovider speichert die Daten und verwaltet die Identität des Benutzers. Wenn Dienstanbieter an der Identität eines Benutzers interessiert sind, müssen sie diese von der zentralen Anmeldestelle bestätigen lassen. In diesem Fall weist sich der Benutzer der zentralen Anmeldestelle gegenüber aus. Diese bestätigt die Identität des Benutzers dem Dienstanbieter.

Beispiele für solchen Ansatz sind das Microsoft Passport-Netzwerk (auch als Windows Live ID bekannt) [Jagoe03] und das Liberty Alliance Project [projectliberty]. Das Passport-Netzwerk von der Firma Microsoft wurde im Jahr 2000 eingeführt. Dabei hatte Microsoft die Vision, dass sich das Passport-Netzwerk als einziger und zuverlässiger Identitätsprovider für das gesamte Internet durchsetzt. Laut Berichten von Microsoft aus dem Jahr 2004 hat dieses Projekt sein Ziel, als einziger Identitätsprovider fürs Internet zu fungieren, nicht erreicht. Auch das Liberty Alliance Project konnte dieses Ziel verfehlt. Das Internet blieb ein Zusammenspiel unterschiedlicher Insellösungen.

Um die Gründe des „Misserfolgs“ dieses Ansatzes besser analysieren zu können, müssen die folgenden Eigenschaften der zentralen Anmeldestelle-Architektur in Betracht gezogen werden:

- **Einmalige Anmeldedaten:** Es gibt nur einen Datensatz mit Anmeldedaten und dieser wird von einer zentralen Stelle verwaltet. Als positive Konsequenz davon ist die Tatsache zu bezeichnen, dass der Benutzer sich nicht verschiedene Benutzernamen und Passwörter für verschiedne Dienste merken muss.
- **Systemübergreifende Identität:** Der Benutzer wandert mit seiner Identität über das ganze System, dabei haben alle Dienstanbieter die gleiche Sicht auf die Benutzeridentität. Wenn z.B. ein Benutzer bei einem Dienstanbieter durch die Identitätsüberprüfung als Student bekannt ist, wird er bei allen anderen Anbietern auch als Student bekannt sein und muss diese Eigenschaft seiner Identität nicht mehr nachweisen.
- **Standardlösung:** Die Dienstanbieter müssen keine Benutzeridentifikation selbst implementieren, sondern einfach den zentralen Identitätsprovider anbinden. Damit wird der Aufwand für das Erstellen und Betreiben eines Dienstes verringert. In manchen Fällen kann es aber dazukommen, dass die von der zentralen Anmeldestelle angebotene Identität für bestimmte Dienste nicht ausreicht. In solchen Situationen bietet dieser Ansatz keine Möglichkeiten, die

Identitätsüberprüfung anzupassen. Die Benutzeridentifikation muss von dem Dienstanbieter selbst implementiert werden.

- **Eingebaute Sicherheit / Unsicherheit:** Die zentrale Instanz ist eine kritische Stelle, diese muss bestimmte Sicherheitsanforderungen erfüllen. Wenn diese Instanz Sicherheitslücken aufweist, wird die Sicherheit des Gesamtsystems gefährdet ggf. kann nicht mehr sichergestellt werden.
- **Zentrale Benutzerdatenverwaltung:** Für viele Dienstbetreiber ist das Beschaffen von Benutzerdaten ein teurer (im Sinne von aufwändig oder kostenspielig) Prozess. Im Falle der zentralen Anmeldestelle werden die Benutzerinformationen von einer fremden Instanz verwaltet. Die Dienstbetreiben sind nicht immer bereit, diese Informationen einem „Fremden" zu vertrauen. Die Akzeptanz der zentralen Anmeldestelle ist nicht immer und besonders nicht in unternehmenskritischen Bereichen gegeben.

Nach den langjährigen Erfahrungen mit dem zentralen Identitätsprovider und auf Grund der Eigenschaften eines solchen Systems wurde von der Firma Micrrosoft, den Beteiligten am Liberty Alliance Project und weiteren Unternehmen eine neue Vision von einem übergreifenden Identitäts-Metasystem entwickelt. Dieses soll die positiven Eigenschaften der zentralen Anmeldestelle weiter ausbauen und die Nachteile beseitigen (s. [msdn.identity]).

Das Metasystem entwickelt weiter den Gedanken, dass das Internet als ein umfangreiches Betriebsystem betrachtet werden kann. Wobei die Idee der übergreifenden Identität verwaltet durch die zentrale Anmeldestelle nicht in der bisher besprochenen Form verflogt wird. Das Identitäs-Metasystem definiert ein Framework, das dem Benutzer ermöglich, in der heterogenen Welt mit seiner Identität einfach zu operieren. Die Frage, was eine passende Identität ist, wird den Benutzern und den Dienstbetreibern überlassen. Dieses Framework bindet unterschiedliche, vorhandene und zukünftige Identitätstechnologien ein. Dabei werden vom Framework folgende drei Rollen definiert:

- **Benutzer:** Wie in den oben beschriebenen Szenarien ist der Benutzer der Konsument eines oder mehreren Dienstangebote.
- **Dienstanbieter:** Der Dienstanbieter stellt Dienstangebote zur Verfügung. Um Dienstangebote in Anspruch zu nehmen, müssen sich die Benutzer dem Dienstanbieter gegenüber identifizieren. Dabei legt jeder einzelne Dienstanbieter fest, was für ihn eine ausreichende bzw. passende Identität ist.
- **Identitätsprüfer:** Der Identitätsprüfer entspricht mit seiner Funktionalität der zentralen Anmeldestelle – seine Aufgabe ist Benutzeridentität zu überprüfen und zu bestätigen. Besonders dabei ist, dass das Identitäts-Metasystem mehrere Identitätsprüfer vorsieht. Dadurch werden für jede gewünschte Identitätsart ein oder mehrere Identitätsprüfer entwickelt bzw. definiert, die den Dienstanbietern die entsprechende Benutzeridentität bestätigen können. Es besteht die Möglichkeit, dass die Dienstanbieter auch die Rolle des Identitätsprüfers übernehmen können. Dadurch bleiben unternehmenskritische Daten im Rahmen des Unternehmens.

Das Zusammenspiel zwischen den verschiedenen Teilnehmern des Identitäts-Metasystems wird an einem praktischen Beispiel verdeutlicht. Es wird die neueste Entwicklung von der Firma Microsoft im Bereich der elektronischen Identität „InfoCard" kurz vorgestellt.

InfoCard ist eine der Identitätstechnologien, die in dem oben beschriebenen Metasystem agieren können. Dabei basiert diese Technologie auf der Metapher der physischen

Ausweiskarten (wie z.B. Personalausweis, Führerschein usw.). InfoCard unterscheidet zwischen zwei arten von Ausweiskarten:

- **extern ausgestellte Karten:** Solche Karten wurden von einer Institution (z.B. Meldebehörde) für einen Benutzer ausgestellt, um seine Identität zu bestätigen.
- **selbst ausgestellte Karten:** Solche Karten sind vom Benutzer selbst ausgestellt und können auch in einigen Fällen seine Identität nachweisen. Beispiel dafür wäre eine selbst erstellte Visitenkarte, die eine bestimmte Benutzeridentität bestätigt. Es ist offensichtlich, dass diese Identität nicht die Qualitäten einer durch Personalausweis bestätigten aufweist. Wie oben beschrieben überlässt das System den Benutzern und den Dienstanbietern die Entscheidung, welche Identitätsart benutzt werden soll.

Die Karten werden von dem InfoCard-System auf dem Rechner des Benutzers verwaltet. Die Überprüfung der Identität findet durch eine Art „Vorzeigen“ der InfoCard-Karte statt. Das InfoCard-System ist als abgewichstes Subsystem für Microsoft Windows Vista und Microsoft Windows XP entwickelt worden. Das Subsystem bietet Geschützte GUI-Oberfläche (ähnlich wie das Login-Fenster von Windows XP), verschlüsselte Speicherung der Karten auf der Festplatte und verbesserte Antiangriffstechniken.

Im Folgenden wird ein Beispielszenario für den Einsatz der InfoCard-Technologie vorgestellt (s. Abbildung 2-4).

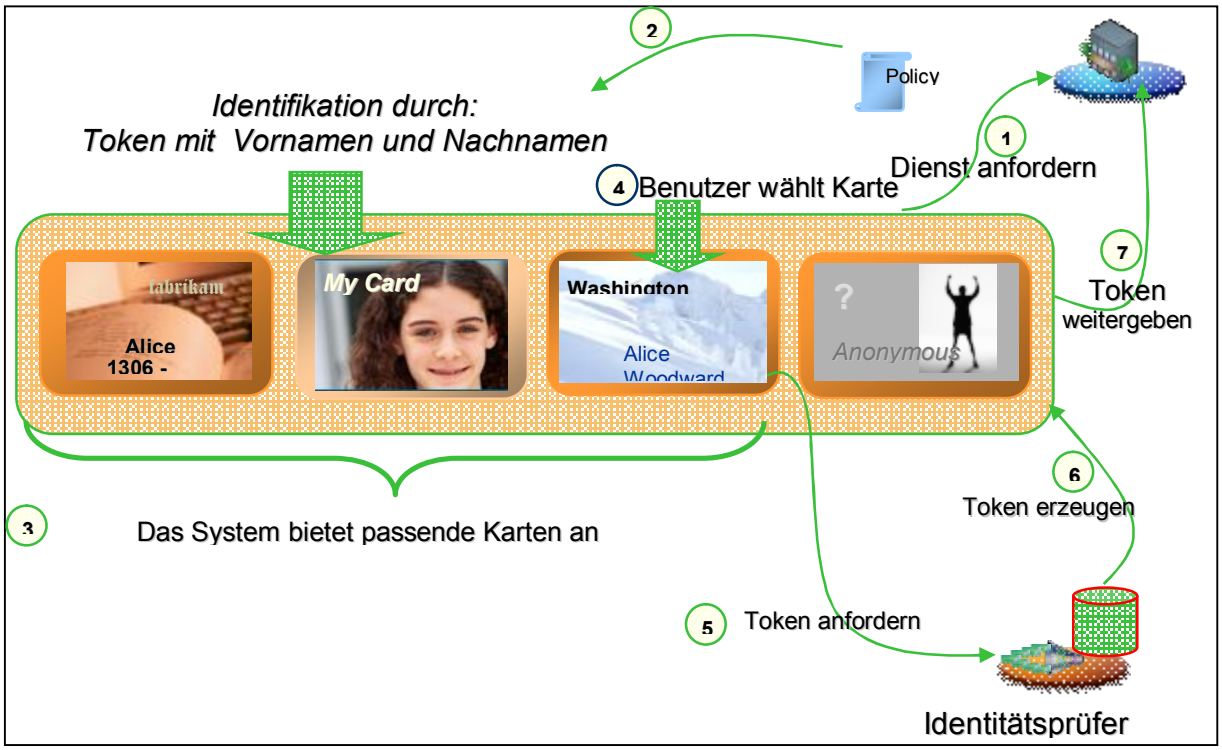

Abbildung 2-4 InfoCard Beispielszenario

Ein Benutzer will einen bestimmten Dienst in Anspruch nehmen. Im ersten Schritt fordert er den Dienst an. Der Dienstanbieter stellt seine Dienste zur Verfügung nur, wenn der Benutzer eine bestimmte Identitätsart nachweisen kann (in diesem Szenario soll die Benutzeridentifikation durch Namen und Vornamen möglich sein). Diese Anforderungen werden vom Dienstbetreiber in einer speziellen Policy beschrieben. Die Policy wird im Schritt zwei an den Benutzer weitergeleitet. Im Schritt drei wählt das InfoCard-System entsprechend

der Policy passende Karten aus dem Karten-Pool aus und bietet diese dem Benutzer zur Auswahl an. Im Schritt vier wählt der Benutzer eine der angebotenen Karten aus. Die Auswahl der Karte ist entscheidend. Die Karte repräsentiert die Verbindung zwischen einem Benutzer und einem Identitätsprüfer. Im Schritt fünf wird eine Anforderung zu dem entsprechenden Identitätsprüfer gestartet, die gewünschte Identität zu bestätigen. Der Identitätsprüfer kontrolliert die Anforderung und anschließend im Schritt sechs schickt die Bestätigung an den Benutzer zurück. Die Bestätigung wird explizit nicht an den Dienst geschickt, da dies ein Sicherheitsrisiko wäre. Der Benutzer soll selbst entscheiden, was er mit seiner Identität macht. Zu Beachten ist, dass weder im Schritt fünf noch im Schritt sechs benutzerrelevante Daten (in unserem Fall Vorname und Nachname) über das Netzt geschickt werden. Diese werden nur vom Identitätsprüfer verwaltet. Die InfoCard-Karte selbst enthält keine Benutzerdaten. Die Antwort des Prüfers bestätigt nur, dass der Benutzer mit dieser Identitätsart sich ausweisen kann. Im Schritt sieben leitet der Benutzer die Bestätigung seiner Identität an den Dienstanbieter und darf in diesem Fall den Dienst in Anspruch nehmen.

Das obere Szenario wurde nur als Beispiel zur Veranschaulichung des Zusammenspiels der einzelnen Komponenten im Rahmen des InfoCard-Systems gewählt. Es sind natürlich weitere Szenarien denkbar, bei denen komplexere Identitätsarten (z.B. Identifikation durch Kreditkarte, Alter, Postadresse usw.) zum Einsatz kommen werden.

Das Identitäts-Metasystem soll die Nachteile der zentralen Anmeldestelle vermeiden, indem ein Framework für unterschiedliche Identitätstechnologien geschaffen wird. Die Vorstellung des InfoCard-System in der Vorlesung AW1 hat eine reiche Diskussion über die Akzeptanz dieses System ausgelöst. Ob das Identitäts-Metasystem und die entsprechenden Technologien (insbesondere das InfoCard-System) sich in der Realität durchsetzen, muss noch festgestellt werden, da diese in naher Zukunft eingeführt werden sollen.

2.1.2 Verwalten personalisierter Daten

Ein weiterer Aspekt des Personalisierens von Diensten ist das Verwalten der personalisierten Daten. Das Verwalten bedeutet in diesem Fall Daten sammeln, speichern und eventuell weitergeben. Ohne die personalisierten Daten ist das Personalisieren von Diensten nicht möglich.

Beim erstellen der personalisierten Datensätzen müssen in vielen Fällen gesetzliche Vorschriften beachtet werden. Diese legen fest, welche Daten unter welchen Bedingungen erhoben, wie lange diese im System gespeichert und ob die Daten an andere Systeme oder Dienstanbieter weitergegeben werden dürfen. Dadurch werden bestimmte Eigenschaften (wie z.B. Sicherheit, Transparenz, Vertrauenswürdigkeit) eines Systems, das Personalisierung enthält, festgelegt. Wie solche Eigenschaften eines Softwaresystems sichergestellt werden können, wird in diesem Kapitel nicht behandelt, da dies den Rahmen dieser Arbeit sprengen wird. Der Leser sollte aber die oben beschriebenen Hinweise im Hinterkopf behalten. Vielmehr wird ein seit einigen Jahren kommender Trend behandelt – das Involvieren des Benutzers in den Personalisierungsprozess.

Das Involvieren des Benutzers bedeutet, dass der Benutzer Kontrolle über die Informationen (z.B. Name, E-Mail-Adresse, Postanschrift, Position usw.) hat, die im Rahmen der Personalisierung von den Dienstanbietern gefordert werden. Dadurch gewinnt der Personalisierungsprozess an Transparenz und das Vertrauen zum jeweiligen Dienstanbieter

kann schneller aufgebaut werden. Beispiel für solchen Ansatz ist das Platform for Privacy Preferences (P3P) Project [w3c.p3p].

P3P ist ein von Word Web Consortium definierter Standard. Er ermöglicht, die Personalisierung der Web-Seiten zu automatisieren und für den Benutzer transparenter zu gestalten. Bei Web-Seiten, die mit P3P ausgestattet sind, hat der Benutzer die volle Kontrolle über seine personalisierten Daten, die von dem Web-Server gespeichert werden. Folgende Informationen werden für den Benutzer durch P3P offen gelegt:

- wer sammelt die Daten,
- welche Daten gesammelt werden,
- für welchen Zweck werden die Informationen gesammelt,
- welche Daten werden weitergegeben,
- wer ist der Empfänger der weitergegebenen Daten,
- wie lange werden die Daten gespeichert,
- wo kann die P3P-Information in menschenlesbarer Form aufgefunden werden?

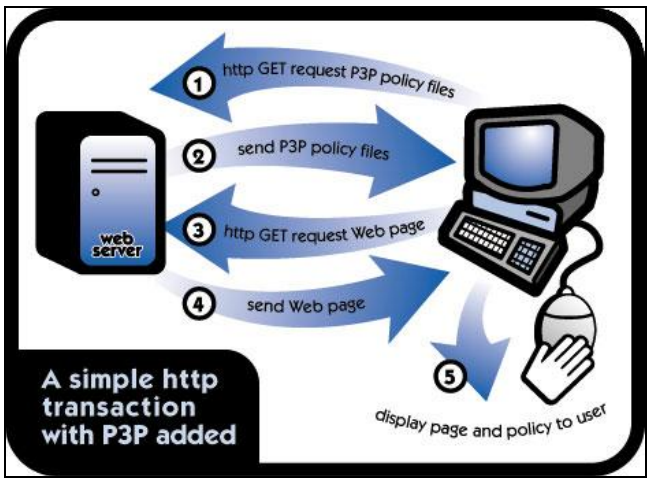

Abbildung 2-5 P3P im Einsatz [Jagoe03]

Bei P3P definiert der Benutzer in einer Policy durch seinen P3P fähigen Browser welche Informationen er den Web-Seiten zur Verfügung stellen will. Der Web-Seitenbetreiber definiert auch welche Informationen er von einem Benutzer der Seite benötigt. Wenn der Benutzer eine P3P fähige Seite anfordert, werden die beiden Polices (des Benutzers und der Web-Seite) verglichen. Im Falle einer Übereinstimmung wird der Vorgang weiter „normal“ ausgeführt. Im Gegenfall wird der Benutzer über die Anforderungen der Web-Seite informiert. An dieser Stelle muss der Benutzer entscheiden, ob und welche der angeforderten Informationen er an die Web-Seite weitergeben wird.

Wie schon oben beschrieben, kann durch P3P nicht nur eine Transparenz und bessere Kontrolle des Personalisierungsprozesses geleistet, sonder auch eine Automatisierung angeboten werden. In der P3P-Policy kann der Benutzer bestimmte Informationen (wie z.B. Vorname, Nachname, Telefonnummer, E-Mail-Adresse usw.) hinterlegen (s. Abbildung 2-6), die automatisch bei einer Nachfrage an die entsprechende Web-Seite weitergegeben werden.

```
<POLICY name="forBrowsers"
discuri="http://www.catalogshop.example.com/PrivacyPracticeBrowsing.html">
<ENTITY>
<DATA-GROUP>
<DATA ref="#business.name">CatalogShop</DATA>
<DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.</DATA>
<DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
<DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
<DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
<DATA ref="#business.contact-info.postal.country">USA</DATA>
<DATA ref="#business.contact-info.online.email">catalog@example.com</DATA>
<DATA ref="#business.contact-info.telecom.telephone.intcode">1</DATA>
<DATA ref="#business.contact-info.telecom.telephone.loccode">248</DATA>
<DATA ref="#business.contact-info.telecom.telephone.number">3926753</DATA>
</DATA-GROUP>
</ENTITY>
<ACCESS><nonident/></ACCESS>
<DISPUTES-GROUP>
<DISPUTES resolution-type="independent"
service="http://www.PrivacySeal.example.org"
short-description="PrivacySeal.example.org">
<IMG src="http://www.PrivacySeal.example.org/Logo.gif" alt="PrivacySeal's logo"/>
<REMEDIES><correct/></REMEDIES>
</DISPUTES>
</DISPUTES-GROUP>
```

Abbildung 2-6 P3P-Policy [w3c.p3p].

Der P3P-Standar ist eine relativ neue Entwicklung, die durch ständig wachsende Anforderungen an den Personalisierungsprozess weitergetrieben wird. Momentan ist P3P nur für den Web-Bereich spezifizier. Es existieren aber die Überlegungen, P3P ähnliche Standards für Bereiche wie „mobile Anwendungen“ und „ortsabhängige Dienste“ zu entwickeln bzw. den P3P-Standard für diese Bereiche anzupassen.

2.1.3 Anpassen des Dienstangebotes

Das Anpassen des Dienstangebotes ist der Kernpunkt bei dem Thema Personalisieren von Diensten. Es wird versucht auf Grund der Benutzeridentifikation und der vorhandenen oder abgeleiteten personalisierten Daten den best möglichen Service einem Konsumenten anzubieten. Dabei werden verschiedene Verfahren in Abhängigkeit von der Situation und der Konsumentengruppe eingesetzt. Die üblichen werden im Weiteren darstellten.

Regelbasierte Personalisierung: Dabei werden aus eigener oder fremder Erfahrung Verhaltensregeln in der Form "WENN DANN" abgeleitet und auf den aktuellen Konsumenten angewandt. Beispielsweise es könnte mittels Data-Mining herausgefunden werden, dass Kunden, die in einem Online-Shop Hemden kaufen, meist auch eine passende Krawatte kaufen (WENN Hemd bestellt DANN Link auf Krawattenkatalog). Einem Kunden, der also in einem Shop ein Hemd bestellt, könnte auch ein Link zu dem Krawatten-Katalog angeboten werden. Ausführlichere Analysen könnten ergeben haben, dass Käufer eines blauen Hemdes meist rote Krawatten bevorzugen, diese Erfahrungen werden das Regelwerk noch mehr spezifizieren (WENN Hemd bestellt in Blau DANN Link auf Krawattenkatalog in Rot).

Kollaboratives Filtern: Dieses Verfahren versucht einen Konsumenten einer Konsumentengruppe mit ähnlichen Interessen zuzuordnen, indem der Konsument nach einer Bewertung des Dienstes (z.B. Kauf eines Buches) gebeten wird. Das System vergleicht die

abgegebene Bewertung mit den schon von anderen abgegebenen Bewertungen und auf diesem Grund findet die Zuordnung zu jeweiligen am besten passenden Konsumentengruppe statt. Im Weiteren findet das Personalisieren von Diensten auf Basis der Gruppeninformationen und nicht auf Basis der Kundeninformationen statt. Bei diesem Verfahren wird zwischen dem offenen und verdeckten kollaborativen Filtern unterschieden. Bei der ersten Variante werden die Eigenschaften der Gruppe, zu der der Konsument zugeordnet wurde, dem Benutzer offen gelegt, bei der zweiten Variante bleiben diese Eigenschaften verborgen.

Personalisierung durch Deduktion: Dieses Verfahren wird in der Fachliteratur (s. [Pashtan05]) auch als Feedback-Personalisierung bezeichnet. Das Verfahren trifft Aussagen auf Basis der vom Benutzer abgegeben Bewertung/en eines konsumierten Dienstes. Dieses Verfahren kann leicht mit dem kollaborativen Filtern verwechselt werden, da beide eine Bewertung des Dienstes enthalten. Im Unterschied zum kollaborativen Filtern, bei dem die Personalisierung auf Basis der Eigenschaften der Gruppe stattfindet, wird die Personalisierung bei der Deduktion auf Basis der abgegebenen Bewertung/en durchgeführt. Beispiel für solchen Ansatz ist der „Personal Video Recorder“. Dieses Unterhaltungsgerät kann Fernsehprogramme aufzeichnen und zeitversetzt wiedergeben. Der Anwender kann dadurch sich ein persönliches Filmprogramm zusammenstellen. Mit der Fernbedienung kann er zudem die betrachteten Sendungen bewerten, und auf der Grundlage der gespeicherten Bewertungen werden ihm weitere Inhalte aus einem „Electronic Program Guide“ vorgeschlagen.

Um eine „gute“ Personalisierung zu erreichen, reicht in meisten Fällen nur eins der oben vorgestellten Verfahren nicht aus, sondern es muss eine sinnvolle Zusammensetzung gefunden werden. Die regelbasierte Personalisierung ist sinnvoll, wenn im System noch keine bzw. wenige personalisierten Daten vorhanden sind. Beispiel dafür wäre der Fall, in dem ein Internet-Shop zum ersten Mal online geschaltet wird. Das definierte Regelwerk (aus Data-Mining oder anderen Shops) kann übernommen werden. Nachteil dabei ist, dass das Regelwerk starr ist, und die Änderungen der Kundenwünsche oder Kundengruppen nicht betrachtet. In einem weiteren Schritt, nachdem der Online-Shop personalisierte Daten gesammelt hat, kann es zum kollaborativen Filtern oder zur Deduktion übergegangen werden. Zu beachten ist, dass der Einsatz des kollaborativen Filterns bei einer großen Dienstdatenbank und wenigen Nutzern nicht effektiv funktionieren wird, da viele Dienste unbewertet bleiben. Die Deduktion kann in den Startphasen des Verfahrens auch eine sprunghafte bzw. für den Benutzer unpassende Personalisierung des Dienstangebotes hervorrufen.

2.2 Fazit

Nachdem die technischen Grundlagen in diesem Kapitel beschrieben und erläutert worden sind, ist es offensichtlich, dass ein erfolgreiches Personalisieren ein Zusammenspiel verschiedener Systeme und Verfahren ist. Bei der Wahl der einzelnen Systeme und Verfahren muss auf jeden Fall der Kontext eines Dienstangebotes in Betracht gezogen werden.

3 Zusammenfassung und Ausblick

In diesem Kapitel wird das im WS2006/2007 stattfindende Projekt mit dem Namen „Flughafen“ vorgestellt. Danach werden die Grundlagen aus dem Kapitel 2 kritisch in Hinsicht auf dessen Einsatz beim Projekt „Flughafen“ betrachtet.

3.1 Projekt „Flughafen“

Im Projekt „Flughafen“ soll das Dienstangebot eines beliebigen Flughafens jedem Fluggast angepasst werden. Der Fluggast soll seinen Interessen (z.B. Einkaufen), seinen Bedürfnissen (z.B. Fax ausdrucken lassen) oder seinen Vorlieben (Kaffeetrinken, Rauchen) auf dem für ihn unbekannten Flughafengelände mit Hilfe unseres Systems nachgehen können. Der Flughafen wird über ein „Indoor Navigationssystem“ (s. [Kutak06]) und einem Verzeichnis (s. [Napitupulu06]) für die vorhandenen Dienste verfügen. Wenn diese Voraussetzungen erfüllt sind, wird die Personalisierung des Angebotes in einem weiteren Schritt erfolgen.

3.2 Personalisieren von Diensten im Projekt „Flughafen“

Jeder Fluggast, der das Personalisieren von Diensten auf dem Flughafen in Anspruch nehmen will, wird mit einem mobilen Rechner (PDA oder Smartphone) ausgestattet.

Im ersten Schritt wird sich der Fluggast durch den Besitzt dieses Rechners (durch spezielle Seriennummern der Rechner) dem System gegenüber identifizieren. Da die Entwicklung der Betriebsysteme für mobile Rechner voranschreitet, ist es auch zu erwarten, dass das InfoCard-System auf mobilen Geräten verfügbar sein wird. Ob dieses System einfach in das geplante Projekt angebunden werden kann und ob dieser Ansatz tragfähig ist, wird die Entwicklung des Systems währen der nächsten Monaten offenbaren.

Den Fluggast in den Personalisierungsprozess hinein zu beziehen, empfinde ich als positive Eigenschaft des Projekts. Momentan ist kein allgemeingültiger Standard (wie z.B. P3P für Web-Seiten) dafür definiert. Dies fordert entweder eine eigene Entwicklung, oder Verzicht auf diese Eigenschaft. Die Entscheidung darüber werden wir erst im WS2006/2007 treffen können, nachdem die genauen Rahmen des Projekts festgelegt worden sind.

Das Dienstangebot wird im Projekt „Flughafen“ auf Basis der vom Fluggast in Anspruch genommenen Diensten personalisiert. Ob ein Dienst in Anspruch genommen wurde, wird auf Grund der Position des Dienstes und des Fluggastes festgestellt (mehr zu dieser Methode s. [Kutak06]). Bis zum WS2006/2007 werden wir (ich und mein Team: Edyta Kutak, Jan Napitupulu) über kein Regelwerk für eine regelbasierte Personalisierung verfügen. Aus diesem Grund planen wir den Einsatz vom verdeckten kollaborativen Filtern. Dabei müssen wir dafür sorgen, dass dieses Filtern nicht mit einer leeren Menge an personalisierten Daten startet. Eine Lösung für dieses Problem haben wir noch nicht. Es wird eventuell eine Modifikation des im Kapitel 2 vorgestellten Verfahrens benötigt.

3.3 Fazit

Das Projekt „Flughafen“ bietet einige Herausforderungen, mit denen wir uns im nächsten Semester auseinander setzen werden. Ein Grundwissen für die Durchführung des Projektes haben wir im Rahmen der Vorlesung Anwendungen 1 aufgebaut. Nun steht uns die spannendste Phase bevor – die Umsetzung der bisher erworbenen Kenntnisse.

Literaturverzeichnis

[amazon] Web-Seite des Online-Buchladens Amazon, http://www.amazon.de, (Stand 07-2006)

[dermalog] Anbieter von biometrischen Identifikationssystemen http://www.dermalog.de, (Stand 07.2006)

[Finkenzeller02] Klaus Finkenzeller, „RFID-Handbuch“, Carl Hanser Verlag München, September 2002 ISBN 3-446-22071-2.

[Jagoe03] Andrew Jagoe, „Mobile Location Services“, Pearson Education Inc., 2003, New Jersey, 2003, ISBN 0-13-008456-5

[ibm.epal] Enterprise Privacy Authorization Language Spezifikation, http://www.zurich.ibm.com/security/enterprise-privacy/epal/, (Stand 07.2006)

[Kuatk06] Edyta Kutak, AW1, 2006, Vortrag und Ausarbeitung zum Thema „Entwicklung eines Location Tracking System für die Indoor Navigation“

[msdn.identity] Definition eines Identitäts-Metasystema http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/identitymetasystem.asp, (Stand 07.2006)

[msdn.infocard] Beschreibung des InfoCard-Ansatzes http://msdn.microsoft.com/winfx/reference/infocard/default.aspx, (Stand 07-2006)

[Napitupulu06] Jan Napitupulu, AW1, 2006, Vortrag und Ausarbeitung zum Thema „Indoor Map Server“

[Pashtan05] Ariel Pashtan, „Mobile Web Services“,Cambridge University Press, Cambridge, 2005, ISBN 0-521-83049-4

[projectliberty] Web-Seite des Liberty Alliance Projects, http://www.projectliberty.org, (Stand 07-2006)

[w3c.p3p] Platform for Privacy Preferences (P3P) Spezifikation, http://www.w3.org/TR/P3P, (Stand: 07.2006)