BAYERISCHER FORSCHUNGSVERBUND
WIRTSCHAFTSINFORMATIK

BAMBERG • BAYREUTH • ERLANGEN-NÜRNBERG • REGENSBURG • WÜRZBURG

Universität Erlangen-Nürnberg

Lehrstuhl Prof. Dr. Dr. h. c. mult. Peter Mertens

Thomas Franke, Dina Barbian

Platform for Privacy Preferences Project (P3P) - Grundsätze, Struktur und Einsatzmöglichkeiten im Rahmen des Franken-Mall-Projekts

Herausgeber:

Prof. Dr. Dieter Bartmann
Prof. Dr. Freimut Bodendorf
Prof. Dr. Otto K. Ferstl
Prof. Dr. Armin Heinzl
Prof. Dr. Dr. h.c. mult. Peter Mertens
Prof. Dr. Elmar Sinz
Prof. Dr. Rainer Thome

Äußere Laufer Gasse 13/15, 90403 Nürnberg, Tel. +49 911-5302 151, Fax +49 911-5302 149, zeier@forwin.de, http://www.forwin.de

FORWIN-Bericht-Nr.: FWN-2000-010

Zusammenfassung

Die Franken-Mall beschäftigt sich zum einen mit der Individualisierung des elektronischen Einkaufs mithilfe von Produktberatungskomponenten, „intelligenten“ Einkaufsagenten und anderen Mehrwertdiensten. Das zweite Standbein der Franken-Mall besteht aus einem regionalen Informations- und Beratungssystem im Freizeitbereich, das sowohl Einheimische als auch Touristen individuell bei der Gestaltung ihrer Freizeit unterstützen soll. Um die für beide Bereiche sehr wichtige Personalisierung umsetzen zu können, ist es nötig, Profildaten der Kunden zu sammeln und zu speichern. Der Bericht stellt das Platform for Privacy Preferences Project (P3P), einen Standard zur Kundenprofilierung im WWW, vor und untersucht ob es sich für diesen Zweck eignet. Des Weiteren wurde die Einsetzbarkeit einer multifunktionalen Chipkarte als Benutzeragent im Rahmen des P3P-Konzepts geprüft.

Stichworte

Electronic Shopping, Freizeitberatung, multifunktionale Chipkarte, P3P, Personalisierung

Abstract

On the one hand, the “Franken-Mall“ supports the individualization of electronic shopping, with the help of advising tools, „intelligent“ shopping agents and other surplus value services. The second core issue of the “Franken-Mall“ is a regional Tourism and Spare Time Advising System, which is intended to support both local citizens and tourists in planning their leisure activities. In order to realize the personalization, which is quite important in both areas, it is necessary to collect and store customer profile data. This report presents the Platform for Privacy Preferences Project (P3P), a WWW-standard for user profiling, and examines, if this is suitable for this purpose. Furthermore, the applicability of a multifunctional chipcard as a user agent within the P3P-concept is considered.

Keywords

electronic shopping, tourism advising system, multifunctional chipcard, P3P, personalization

Inhalt

1 Einleitung

1.1 Projekthintergrund

Der vorliegende Bericht wurde im Rahmen des Forschungsprojekts „Franken-Mall – Regionaler elektronischer Marktplatz und regionales Informations- und Beratungssystem im Freizeitbereich für Mittelfranken“ erstellt. Dieses Vorhaben ist ein Teil des Konzepts, mit dem der Städteverbund Nürnberg-Fürth-Erlangen-Schwabach-Bayreuth an dem 1998 vom **B**undes**m**inisterium für **B**ildung und **F**orschung (BMBF) ausgeschriebenen Media@Komm-Wettbewerb teilgenommen hat.

Zu den Zielen, die mit dieser Ausschreibung verfolgt werden sollen, zählen:

1. die Schaffung eines integrierten Konzepts für das Angebot sowohl öffentlicher als auch privater Dienstleistungen,
2. die Nutzung von modernen Multimedia-Technologien sowie
3. der Einsatz der Digitalen Signatur.

Aus diesen Ansprüchen lassen sich drei Zielgruppen ableiten, an die sich das Konzept wendet. Im Einzelnen sind dies [NIK99, S. 4]:

1. Kommunen als Anbieter öffentlicher Dienstleistungen (z. B. elektronisches Bürgerbüro),
2. Bürger als Anwender und Kunden der Anbieter sowie
3. Privatunternehmen, die als Nutzer kommunaler aber auch als Anbieter privater Dienstleistungen auftreten können.

Die „Franken-Mall“ positioniert sich in diesem Spektrum als sog. „private-public-Teilprojekt“, da sie sowohl private als auch kommunale Dienste beinhaltet, wie man der Abbildung 1 entnehmen kann.

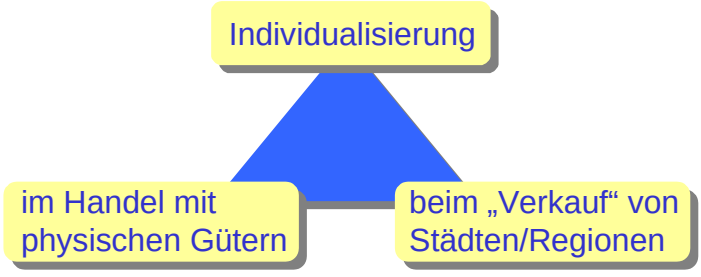

Abbildung 1: Grundgedanke des „Franken-Mall“-Projekts

Im Mittelpunkt steht das Prinzip der Individualisierung, d. h. das Angebot von Dienstleistungen, die möglichst passgenau auf den einzelnen Anwender zugeschnitten sind. Dieser Leitgedanke wird in zwei unterschiedlichen Bereichen weiter verfolgt: Zum einen im sog. Shopping-Modul, das den Handel mit physischen Gütern mithilfe von Produktberatungskomponenten, „intelligenten" Einkaufsagenten und anderen Mehrwertdiensten unterstützen soll, und zum anderen in einem Online-Freizeitberatungssystem für Einheimische und Touristen, welches sich mit dem Marketing und „Verkauf" von Regionen und Städten befasst.

1.2 Aufbau des Berichts

In Kapitel 2 dieses Berichts wird zunächst auf die Wichtigkeit des Datenschutzes und des verantwortlichen Umgangs mit persönlichen Informationen der Kunden eingegangen. Als eine Initiative, die dies zu unterstützen versucht, setzt sich der Abschnitt anschließend mit dem **P**latform for **P**rivacy **P**references **P**roject (P3P) des **W**orld **W**ide **W**eb **C**onsortium (W3C) auseinander. Kapitel 3 geht im Folgenden darauf ein, inwieweit sich die Prinzipien und Technologien des P3P auf die „Franken-Mall" übertragen lassen. Ein gesonderter Abschnitt wird mit Kapitel 4 der Fragestellung gewidmet, ob eine multifunktionale Chipkarte, deren Einsatz das mittelfränkische Konzept vorsieht, als Benutzeragent im Sinne des P3P ausgestaltet werden kann. Den Abschluss bilden eine Zusammenfassung der gefundenen Ergebnisse sowie ein Ausblick auf weitere Arbeiten im „Franken-Mall"-Projekt.

2 P3P – Platform for Privacy Preferences Project

2.1 Überblick und Grundsätze

Um die in Abschnitt 1 angesprochene Individualisierung von Dienstleistungen erreichen zu können, ist es nötig, dass der Anwender seine Bedürfnisse und Präferenzen einem Beratungssystem gegenüber bekannt gibt, welches diese dann etwa in Form eines Benutzermodells strukturiert ablegt. Dabei sind fast immer auch personenbezogene Daten des Interessenten betroffen; häufig ist es sogar so, dass das Beratungsergebnis umso besser wird, je mehr die Anwendung über den Einzelnen weiß. Hieraus ergibt sich speziell für die Online-Beratung ein erhebliches Konfliktpotenzial, da viele Web-Anwender die Anonymität im Internet an sich traditionell als schützenswertes Gut betrachten. Deshalb sind sie häufig Bestrebungen gegenüber, Benutzerprofile im Netz zu generieren (Stichwort „gläserner Web-Surfer", [Meis96]), sehr viel negativer eingestellt als der Erhebung personenbezogener Daten im „normalen" Leben. Weitzner nennt dieses Phänomen, das sich an folgendem Beispiel (siehe Abbildung 2) recht gut verdeutlichen lässt, „The Web trust gap" [Weit99].

Aktivität	Benutzereinschätzung	
	Offline (z. B. Buchladen)	Online (z. B. Amazon.com)
Protokollieren des individuellen Einkaufsverhaltens	Persönliche Note	Zudringlichkeit
Informieren des Kunden, wenn neues Produkt lieferbar	Verkäufer denkt mit	„Spamming“
Aussprechen von Empfehlungen aufgrund der Präferenzen anderer Nutzer (Recommender System)	Guter Verkäuferstil	Angst vor Big-Brother im System

Abbildung 2: Beispiel für das Phänomen der sog. „Web trust gap“ (nach [Weit99])

Man erkennt, dass Bestrebungen zur individuellen Betreuung von Kunden im Offline-Bereich durchweg positiv betrachtet werden (der Einzelne fühlt sich vom Verkaufspersonal zuvorkommend behandelt), während die gleichen Aktivitäten, wenn sie ein Computersystem durchführt, negative Reaktionen hervorrufen. Dem ist wohl vor allem so, weil es sehr viel schwieriger ist, ein Vertrauensverhältnis zu einer Maschine aufzubauen, als es bei einem menschlichen Verkäufer der Fall ist. Zudem sind die Anwender u. U. verunsichert, da ein Rechner alle Daten, die sie ihm zur Verfügung stellen, unbegrenzt lange speichern kann und deshalb die Auswertung und Nutzung dieser Informationen zu Zwecken, die nicht vereinbart waren (Werbung etc.), sehr viel leichter möglich ist.

Das P3P ist eine Initiative des W3C zusammen mit einigen großen Unternehmen, wie Microsoft, Netscape oder IBM, mit der versucht werden soll, dieses immanente Misstrauen gegenüber Web-Anwendungen, die persönliche Daten benötigen, abzubauen. Um dieses Ziel zu erreichen, richtet sich das Projekt an folgenden Leitprinzipien aus [Cran98; Marc00]:

1. Benachrichtigung und Kommunikation

   Ein Anbieter, der Daten über einen Nutzer sammeln möchte, soll diesem gegenüber eindeutig - sowohl maschinenlesbar als auch in Klartext – bekannt geben, welche Daten er zu welchem Zweck erhebt, wie er mit ihnen weiter verfährt u. a. Aufseiten des Benutzers sind Werkzeuge zu realisieren, die es ihm ermöglichen, unkompliziert die Anfrage eines Dienstes zu beantworten.

2. Wahlmöglichkeit und Kontrolle

   Der Anwender soll stets bestimmen können, welchem Dienst er für welche Aufgaben welche Informationen zur Verfügung stellt. Auch im Nachhinein muss die Freigabe von Daten einsehbar und widerrufbar sein. Dazu stellt die Client-Software Funktionen bereit, die darüber hinaus sicherstellen, dass ein Zugriff auf persönliche Informationen erst nach einer wissentlichen Zustimmung (informed consent) des Kunden möglich ist.

3. Fairness und Integrität

   Ein Diensteanbieter sollte nur diejenigen Daten vom Anwender abrufen, die er zur Durchführung der jeweiligen Aufgaben auch unbedingt benötigt. Außerdem hat er sich streng an die in der Benachrichtigung des Nutzers getroffenen Aussagen bezüglich Datenverwendung etc. zu halten.

4. Sicherheit

   P3P stellt definiert zwar selbst keine Sicherheitsmechanismen, wie Verschlüsselung o. Ä., empfiehlt aber dringend deren Nutzung bei der Durchführung von P3P-Aktionen und stellt Schnittstellen zu Kryptographie-Werkzeugen zur Verfügung.

Zur Schaffung eines Frameworks, das diesen Leitprinzipien genügt und auf dem Werkzeuge zur Unterstützung der Diensteanbieter auf der einen sowie der Anwender auf der anderen Seite aufbauen können, bedient sich P3P verschiedener WWW-Basistechnologien, die ebenfalls im Umfeld des W3C entwickelt wurden.

2.2 Basistechnologien

2.2.1 XML – Extensible Markup Language

Die E**x**tensible **M**arkup **L**anguage (XML) leitet sich ebenso wie die bekannte Web-Seiten-Beschreibungssprache HTML (**H**yper**t**ext **M**arkup **L**anguage) von einer allgemeineren Dokumenten-Beschreibungssprache, der SGML (**S**tandard **G**eneralized **M**arkup **L**anguage), ab. Während allerdings HTML eine Anwendung von SGML darstellt, d. h., es wurde mit SGML vorab eine mehr oder weniger unveränderliche Menge von Tags (Markierungen) definiert, mit denen man Struktur, Layout und Inhalt einer WWW-Seite beschreiben kann, ist XML eine Untermenge von SGML. Dies führt dazu, dass in XML die grundlegenden Funktionen und Prinzipien von SGML erhalten bleiben. Insbesondere sind dies die Möglichkeit, eigene Tags zu definieren, welche den jeweiligen Anforderungen eines Anwendungsbereichs gerecht werden, sowie die strikte Trennung von Struktur, Inhalt und Layout eines Dokuments. Es wurden lediglich der Sprachumfang von SGML um für Internet-Anwendungen irrelevante Konstrukte verkleinert sowie einige Strukturen „vorgedacht“, die in diesem Anwendungsfeld von Nutzen sind. Dabei handelt es sich z. B. um die Qualifikation eines Dokuments als „wohlgeformt“, wenn es bestimmten Anforderungen genügt, welche dazu führen, dass es besser maschinell zu verarbeiten ist [OV00a]. Man könnte XML also als Meta-Auszeichnungssprache verstehen, mit der sich beliebige „eigene“ Auszeichnungs-sprachen definieren lassen. Dies geschieht in der sog. **D**ocument **T**ype **D**efinition (DTD), die

somit eine Grammatik für eine Klasse von Dokumenten bildet [Bray98a]. Hier legt man die Strukturen und Elemente eines Dokuments sowie in rekursiver Form wiederum deren Aufbau fest. Da die Semantik (also die Bedeutung) verschiedener Zeichenketten im Dokument enthalten ist, lässt sich ein XML-Dokument sehr viel leichter maschinell verarbeiten als ein unstrukturierter Text. Dies führte dazu, dass XML inzwischen mehr als eine Sprache des automatischen Informationsaustauschs als der Gestaltung von Dokumenten anzusehen ist.

2.2.2 RDF – Resource Description Framework

Auch das **R**esource **D**escription **F**ramework (RDF) stellt eine Initiative des W3C dar. Im Mittelpunkt steht hier die Beschreibung von Web-Ressourcen mithilfe strukturierter Metadaten, also Daten über Daten. Hierbei ist unter einer Ressource alles zu verstehen, was über einen URI (**U**niform **R**esource **I**dentifier) eindeutig angesprochen werden kann [Mill98]. Der Begriff URI umfasst neben den bekannten URLs (**U**niform **R**esource **L**ocator), also beispielsweise HTML-Seiten, XML-Ausdrücke, vCard-Visitenkarten etc., auch sog. URNs (**U**niform **R**esource **N**ame), die bestimmten Anforderungen genügen müssen (Näheres siehe [Conn98]). Dadurch, dass das RDF alle diese Ressourcen näher beschreibt, also mit mehr Semantik ausstattet, lassen sich viele Aufgaben im Web, die bisher mit relativ „dummen“ Methoden, wie Volltextsuche o. Ä., angegangen wurden, eleganter lösen. So können Metadaten etwa Suchmaschinen, die Katalogisierung von Inhalten oder auch die Bewertung des Inhalts von Web-Dokumenten unterstützen. Man vollzieht den Schritt von „maschinenlesbaren“ Dokumenten hin zu „von der Maschine verstehbaren“ Ressourcen [Lass97].

Um dies zu erreichen, definiert das RDF ein Datenmodell, das auf Eigenschafts-Werte-Paaren basiert. Zur Modellierung werden drei Objekttypen herangezogen [Lass99]:

1. *Ressource:* alles, was über einen URI eindeutig anzusprechen ist (siehe oben).

2. *Eigenschaft:* ein Attribut einer Ressource, für welches eine bestimmte Bedeutung, ein Wertebereich, die Ressourcen für die es gültig ist sowie seine Beziehungen zu anderen Attributen definiert sind.

3. *Aussage:* besteht aus einer Ressource, einer Eigenschaft und einem spezifischen Wert dieser Eigenschaft, die man auch als Subjekt, Prädikat und Objekt der Aussage verstehen kann. Der Wert einer Eigenschaft kann dabei atomar sein (z. B. eine Zeichenkette) oder ebenfalls wieder eine Ressource darstellen.

Eine derartige Aussage lässt sich im RDF auf zwei verschiedene Arten repräsentieren: zum einen als gerichteter, beschrifteter Graph und zum anderen als XML-Statement, das speziellen Regeln entspricht. Beispielsweise ist im Unterschied zu reinem XML die Reihenfolge der

Elemente, die für die Gestaltung eines Dokumentes - den Ursprungszweck von XML - wesentlich ist (z. B. der Betreff vor der Grußformel in einem Brief), völlig nachrangig. Außerdem erlaubt XML Konstruktionen, bei denen die Elemente recht kompliziert verschachtelt sind, während im RDF die Struktur so einfach wie möglich gehalten wird. Beide Punkte dienen dem Designziel des RDF, eine gute Skalierbarkeit zu erzielen, um die riesige Informationsmenge im Internet mit vertretbarem Aufwand mit Metadaten beschreiben und diese dann auch wieder auswerten zu können [Bray98b].

Ein einfaches Beispiel mag die Darstellungsalternativen verdeutlichen. Die Aussage: „Thomas Franke ist der Autor der Web-Seite *www.wi1.uni-erlangen.de/projekte/frankenmall/frankenmall.html*“, ließe sich mit dem RDF grafisch folgendermaßen darstellen:

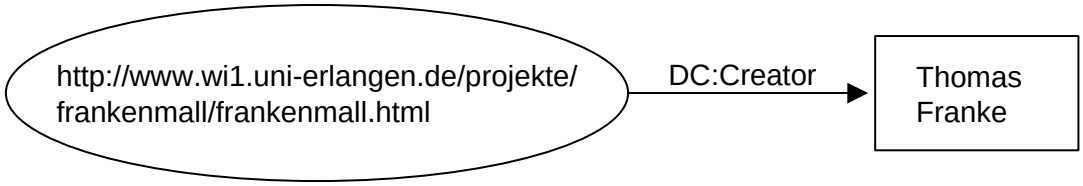

Abbildung 3: Darstellung einer RDF-Aussage in Graphen-Notation

Ein ovaler Knoten repräsentiert hierbei eine Ressource, der Pfeil eine Eigenschaft der Ressource und der eckige Knoten deren Wert. Der Zusatz „DC:“ vor dem Eigenschaftsnamen weist auf den *Namespace* hin, dem das Attribut entnommen wurde, d. h. welchem Vokabular es entstammt. Ein Zweck des RDF ist es, unterschiedlichen Organisationen ein Werkzeug an die Hand zu geben, mit dem sie Vokabulare (d. h. systematisierte Zusammenstellungen von Attributen) erstellen können, die die Metadaten ihrer jeweiligen Domäne möglichst gut beschreiben. Da es möglich ist, dass verschiedene Vokabulare den gleichen Attributnamen verwenden, jedoch mit unterschiedlicher Semantik behaftet sind, ist in der RDF-Notation stets die Herkunft des Attributs anzugeben. „DC:“ steht beispielsweise für **D**ublin-**C**ore-Elements, ein Vokabular für bibliografische Angaben (näheres siehe auch [Weib98]). In XML-Schreibweise sieht der in Abbildung 3 dargestellte Sachverhalt wie folgt aus:

```
<rdf:RDF
   xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
   xmlns:dc="http://purl.org/metadata/dublin_core#">
  <rdf:Description about="http://www.wi1.uni-erlangen.de/projekte
                                        /frankenmall/frankenmall.html">
    <dc:Creator>Thomas Franke</dc:Creator>
  </rdf:Description>
</rdf:RDF>
```

Abbildung 4: Darstellung der Aussage aus Abbildung 3 in XML-Schreibweise

Auch hier sieht man (in der zweiten und dritten Zeile), dass die verwendeten Namespaces deklariert werden (hier der Standard-RDF-Namespace und die Dublin Core Elements).

Neben den angesprochenen Konstrukten stellt das RDF noch Container-Strukturen zur Verfügung, die dazu dienen, einer Eigenschaft mehrere Werte zuzuweisen. Im Einzelnen handelt es sich dabei um die *Alternative* (z. B. Angabe verschiedener Mirror-Sites im WWW), die *Sequenz* (sortierte Liste, z. B. für die alphabetische Aufzählung mehrerer Autoren) sowie die *Bag* (unsortierte Liste).

Nachdem nun sowohl die Zielrichtung von P3P als auch die Basistechnologien, derer es sich bedient, beschrieben sind, widmet sich der folgende Abschnitt detaillierter der internen Struktur des Konzepts.

2.3 Struktur und Bestandteile

2.3.1 Privacy Policy und Proposal

Der erste Baustein von P3P, der hier diskutiert werden soll, ist aufseiten des Diensteanbieters, respektive Datensammlers angesiedelt. In seiner Privacy Policy (Datenschutzpolitik) identifiziert sich der Anbieter und gibt bekannt, wie er mit personenbezogenen Daten umgeht, d. h., welche Daten er überhaupt sammelt etc. Diese Erklärung stellt gleichzeitig ein Angebot an den Benutzer dar, unter welchen Bedingungen er die Dienste der jeweiligen Web-Site nutzen kann. Sie liegt in maschinenlesbarer Form vor, und zwar XML-kodiert und den Regeln des RDF genügend, enthält jedoch einen Verweis auf ein Klartext-Dokument gleichen Inhalts. Der Zweck dieser doppelten Darstellung besteht darin, zum einen einem (Software-)Benutzeragenten die Möglichkeit zu geben, das Proposal automatisch auszuwerten und womöglich sogar zu beantworten. Zum anderen soll auch der Mensch direkt Einblick in die Datenschutzpolitik des Anbieters bekommen.

Diese wird in einem Web-Dokument durch das XML-Tag `<POLICY>` markiert und beantwortet zunächst folgende Fragen:

1) Die `<ENTITY>` gibt darüber Auskunft, welche natürliche oder juristische Person die personenbezogenen Daten sammelt. Dazu gehören Name, Anschrift und sonstige Kontaktinformationen. (**Wer?**)

2) Das `<ACCESS>`-Tag klärt, welche seiner gesammelten Daten der Kunde jederzeit einsehen kann. Die möglichen Werte reichen dabei von `<all/>`, d. h., der Benutzer hat Zugriff auf alle personenbezogenen Daten, über `<ident_contact/>` (Zugriff nur auf Kontaktinformationen wie Adresse und E-Mail) bis zu `<none/>` (kein Zugriff). Anmerkung: Das

Bundes**d**aten**s**chutz**g**esetz (BDSG) schreibt in Deutschland grundsätzlich vor, dass alle Daten einsehbar sein müssen [BDSG]. Werden überhaupt keine personenbezogenen Daten gesammelt, macht dies die Kennzeichnung `<nonident/>` deutlich.

3) Mit dem Problem, wie Streitfälle im Zusammenhang mit einer Verletzung der Privacy Policy zu behandeln sind, beschäftigt sich der Abschnitt `<DISPUTES>`. Vorgesehen sind etwa die Möglichkeiten, sich an den Kundenservice des Betreibers oder eine unabhängige Organisation zu wenden oder aber sich z. B. auf die einschlägige Gesetzesgrundlage zu berufen. Innerhalb dieses Tags werden auch die `<REMEDIES>` definiert, d. h. die Maßnahmen, die zu ergreifen sind, wenn ein Kunde sich beschwert. Diese erstrecken sich von einer einfachen Korrektur der aufgetretenen Fehler (`<correct/>`) über eine finanzielle Entschädigung des Benutzers (`<money/>`) bis hin zu den Maßnahmen, die wiederum die einschlägige Gesetzesgrundlage vorsieht (`<law/>`).

Den Kern einer Datenschutzpolitik bilden jedoch eines oder mehrere sog. Statements, die darüber Auskunft geben, welche Daten zu welchem Zweck wie lange gespeichert und an wen sie weitergeleitet werden. Dies geschieht mithilfe folgender vordefinierter Tags:

4) Zweck der Datenerhebung: `<PURPOSE>` (**Wozu?**)

Wert	Bedeutung
`<current/>`	Durchführung der aktuellen Tätigkeit
`<admin/>`	Web-Site- und Systemadministration
`<develop/>`	Verbesserung des eigenen Angebots, jedoch nicht individuelle Information
`<customization/>`	Individuelle Informationsversorgung (vom Benutzer ausgehend/ eingestellt)
`<tailoring/>`	Individuelle Informationsversorgung nur für die aktuelle Sitzung
`<pseudo-analysis/>`	Aufbau eines Benutzerprofils auf Pseudonymbasis zur indirekten Auswertung
`<pseudo-decision/>`	Aufbau eines Benutzerprofils auf Pseudonymbasis zur individuellen Informationsversorgung
`<individual-analysis/>`	Aufbau eines Benutzerprofils zur indirekten Auswertung
`<individual-decision/>`	Aufbau eines Benutzerprofils zur individuellen Informationsversorgung
`<contact/>`	Kontaktaufnahme (z. B. zu Marketingzwecken)
`<historical/>`	Datensammlung für sozialgeschichtliche Auswertungen
`<telemarketing/>`	Kontaktaufnahme zu Marketingzwecken über das Telefon

Abbildung 5: Mögliche Datenerhebungszwecke in P3P

Jedem Zweck wird per Attribut zugeordnet, ob er für die Dienstleistung der Web-Site unbedingt erforderlich ist. Ist dies nicht der Fall, muss der Benutzer entweder für die jeweilige

Nutzung sein Einverständnis geben (opt-in) oder aber bestimmte Nutzungsarten explizit ausschließen (opt-out).

5) Empfänger der gesammelten Daten: `<RECIPIENT>`

Wert	Bedeutung
`<ours>`	Nur Eigenverwendung und Weitergabe an Erfüllungsgehilfen
`<delivery>`	Weitergabe der Kontaktinformationen zu Lieferzwecken (z. B. Post)
`<same>`	Weitergabe von Informationen an Dritte mit vergleichbaren Datenschutzpraktiken
`<other-recipient>`	Weitergabe an Dritte, die dem Anbieter rechenschaftspflichtig sind
`<unrelated>`	Weitergabe an unverbundene Dritte
`<public>`	Öffentlich zugängliche Speicherung (z. B. Diskussionsforen)

Abbildung 6: Datenempfänger nach P3P

Es lassen sich auch für bestimmte Daten mehrere Empfänger spezifizieren.

6) Dauer der Datenhaltung: `<RETENTION>`

Wert	Bedeutung
`<no-retention/>`	Keine Speicherung, Verarbeitung nur während einer Online-Transaktion
`<stated-purpose/>`	Speicherung bis angegebener Zweck erfüllt ist (frühestmögliche Löschung)
`<legal-requirement/>`	Speicherung zur Erfüllung des angegebenen Zwecks, jedoch verlangt ein Gesetz eine darüber hinaus gehende Archivierung
`<business-practices/>`	Je nach Geschäftsgebaren des Anbieters
`<indefinitely>`	Beliebig lange Speicherung

Abbildung 7: Stufen der Datenhaltung nach P3P

Die Angaben 4), 5) und 6) beziehen sich jeweils auf eine Informationskategorie (siehe Abbildung 8) aus dem Data Repository des Kunden.

2.3.2 Data Repository

Ein weiterer Bestandteil von P3P ist das Data Repository. Es stellt eine in verschiedene Kategorien gegliederte Datensammlung dar, in der ein Anwender sein persönliches Profil ablegen kann (siehe Abbildung 8). Sowohl der Informationssammler (in seiner Privacy Policy) als auch der Kunde (bzw. sein Benutzeragent, siehe Abschnitt 2.3.3) greifen auf diese Kategorisierung zurück; der eine, um gezielt Daten anfordern zu können, der andere, um zu entscheiden, welche Informationen unter welchen Bedingungen freizugeben sind. Im Einzelnen lassen sich folgende Rubriken unterscheiden:

Wert	Bedeutung
`<physical/>`	Physische Kontaktinformation (z. B. Adresse, Telefon)
`<online/>`	Kontaktinformation über das Internet (z. B. E-Mail-Adresse)
`<uniqueid/>`	Eindeutige Kennung
`<purchase/>`	Ver- / Einkaufsinformationen (z. B. Produkte, Zahlungsart)
`<financial/>`	Informationen über das Finanzgebaren (z. B. Kontostände, Zahlungsverhalten)
`<computer/>`	Informationen über den Rechner des Kunden (z. B. IP-Adresse, Betriebssystem)
`<navigation/>`	Navigationsdaten, Verweilzeiten, Clickstream (passiv generiert)
`<interactive/>`	Nutzungsdaten durch explizite Aktivitäten des Kunden (z. B. Suchanfragen)
`<demographic/>`	Demographische und/oder sozio-ökonomische Daten (z. B. Geschlecht, Alter, Einkommen)
`<content/>`	Explizite Äußerungen des Anwenders (z. B. Inhalt von E-Mails)
`<state/>`	Status der aktuellen Anwendungssitzung
`<political/>`	Daten über Zugehörigkeit zu Parteien, Religionsgemeinschaften u. Ä.
`<health/>`	Medizinische Informationen
`<preference/>`	Allgemeine Benutzerpräferenzen (Hobbies, Interessen etc.)
`<location/>`	Gegenwärtiger Aufenthaltsort (z. B. GPS-Daten)
`<other>...</other>`	Neu definierte Rubriken mit Beschreibung

Abbildung 8: Kategorien des P3P-Benutzerprofils

Jede Teilinformation, die der Kunde innerhalb des P3P-Systems bekannt macht, wird einer oder mehrerer dieser Rubriken zugeordnet. Dies geschieht entweder im Moment der Eingabe seitens des Benutzers oder durch Festlegung von Datenschemata, wobei P3P ein Grundschema, welches die wichtigsten Daten bereits enthält, vordefiniert. So existieren z. B. Datenstrukturen für die Objekte *Benutzer* und *Unternehmen*. Der Name einer Person gehört darin etwa den Rubriken *Physische Kontaktinformation* sowie *Demographische und sozio-ökonomische Information* an. Anhand dieser Zuordnung lassen sich recht exakt Regeln formulieren, die das Verhalten eines Softwareagenten steuern, der die Weitergabe von Informationen kontrolliert.

2.3.3 User Agent und APPEL

Für einen solchen Benutzeragenten bieten sich laut W3C unterschiedliche Realisierungsmöglichkeiten an: er könnte 1) in einen Web-Browser eingebaut, 2) als Java-Applet umgesetzt oder 3) in sonstige Client-seitige Software integriert werden. Seine Aufgabe ist es, den Web-Auftritt eines Diensteanbieters nach dessen Privacy Policy zu durchsuchen und je nach

Kundenpräferenzen die entsprechenden Datenfelder aus dem Data Repository weiterzuleiten. Zur Formulierung dieser Präferenzen und Steuerung des Agenten entwickelte das P3P-Gremium die XML-basierte Sprache APPEL (**A** **P**3P **P**reference **E**xchange **L**anguage, [Lang00a]). Abbildung 9 stellt schematisch dar, wie dabei vorgegangen wird: Ein Proposal trifft beim Benutzeragenten ein, dieser überprüft, ob es eine Vorschrift gibt, die auf das Angebot anwendbar ist, und führt ggf. die hinterlegte Anweisung aus.

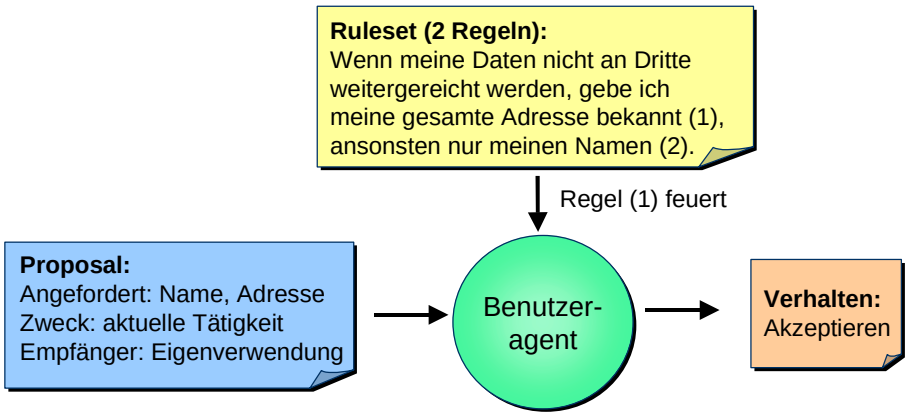

Abbildung 9: Beispiel zur Auswertung einer Regel durch den P3P-Benutzeragenten

APPEL stellt Konstrukte zur Verfügung, mit denen der Anwender sog. Rulesets definieren kann, die wiederum aus mehreren einzelnen Regeln bestehen. Eine solche Einzelvorschrift umfasst einen Handlungsteil, der bestimmt, wie sich der Agent verhält, falls die Regel feuert, sowie mehrere sog. Expressions. Sie beziehen sich auf bestimmte Rubriken der Datenschutzpolitik und legen fest, welche Charakteristika diese aufweisen muss, damit die vorliegende Regel überhaupt ausgeführt werden kann. Expressions lassen sich einerseits untereinander mit Boole‘schen Operatoren (UND/ODER) verknüpfen, können andererseits aber auch intern Bezug auf mehrere Kategorien der Policy nehmen, die ebenfalls mit logischen Operatoren verknüpft werden. So kann man etwa eine Regel formulieren, die ein Proposal akzeptiert, wenn entweder nur Online-Kontaktinformationen für Marketingzwecke oder Einkaufsinformationen ausschließlich zur Abwicklung der aktuellen Tätigkeit innerhalb der eigenen Organisation erhoben werden. Zu beachten ist dabei, dass der Agent die verschiedenen Regeln innerhalb eines Rulesets sequenziell auswertet und die Evaluation abbricht, sobald er eine Regel findet, die feuern kann. Deshalb spielt die Reihenfolge der Vorschriften eine große Rolle und wirkt sich stark auf die Semantik des Rulesets aus. Um den Kunden dabei nicht allein zu lassen, setzen hier Werkzeuge an, die aus einer natürlichsprachlichen Anforderung, die er formuliert, möglichst automatisch semantisch korrekte APPEL-Regeln erzeugen. Jeder Satz sollte dabei eine Vorschrift beinhalten, die ausgeführt wird, falls keine der anderen zutrifft. Dieses „Standardverhalten“ eines Rulesets kennzeichnet man mit dem Tag `<otherwise>`.

Derzeit kennt der Sprachumfang von APPEL nur vier Standard-Verhaltensweisen des Benutzeragenten: Akzeptieren bzw. Zurückweisen einer Anfrage (hierbei handelt das

Programm selbstständig) sowie Information bzw. Warnung des Benutzers (hier wendet sich der Rechner an den Anwender und überlässt diesem die endgültige Entscheidung). Das Konzept sieht jedoch die Möglichkeit vor, bei Bedarf weitere (evtl. auch komplexere Verhaltensweisen, vgl. Abschnitt 2.4) definieren zu können.

2.4 Ablauf einer P3P-Transaktion

Nachdem der vorherige Abschnitt die einzelnen Bestandteile des P3P-Konzeptes vorgestellt hat, soll hier nun deren Zusammenspiel bei der Abwicklung einer Transaktion veranschaulicht werden (siehe Abbildung 10).

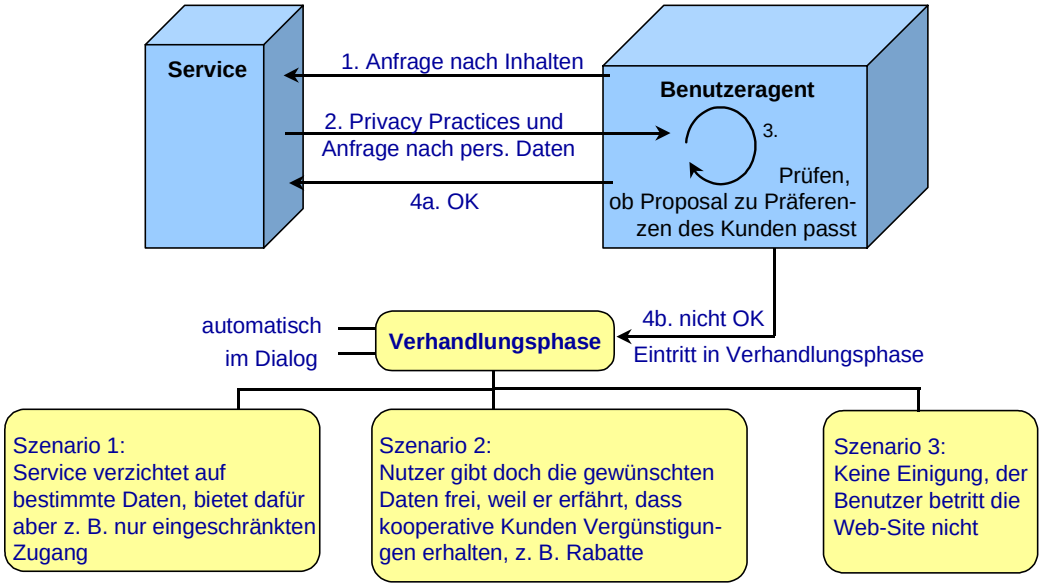

Abbildung 10: Ablaufvarianten einer P3P-Transaktion

Zu Beginn greift der Kunde auf eine Web-Site zu, die das P3P-Konzept unterstützt (1). Ein Dienst, der auf dem Server des Anbieters läuft, übermittelt nun dessen Datenschutzpolitik und fordert gegebenenfalls persönliche Informationen des Benutzers an, wie in Abschnitt 2.3.1 beschrieben (2). Nun prüft der Benutzeragent, ob der Vorschlag der Web-Site den Präferenzen des Anwenders dahingehend, wie mit seinen Daten umzugehen ist, entspricht. Dabei nutzt er die in Kapitel 2.3.3 vorgestellten Strukturen und Methoden. Kommt er (als Folge einer APPEL-Regel) zu dem Ergebnis, dass das Proposal ohne Weiteres annehmbar ist, so übermittelt er die angeforderten Informationen aus dem Data Repository (vgl. Abschnitt 2.3.2) an den Server. Häufig wird es aber so sein, dass der Vorschlag des Anbieters nicht unverändert übernommen werden soll. In diesem Fall tritt das System zukünftig in eine Verhandlungsphase ein, die entweder im Dialog mit dem Menschen (beginnend mit der Information bzw. Warnung des Kunden, siehe Abschnitt 2.3.3) oder automatisch vom Benutzeragenten abgewickelt werden kann. Hier kommen dann die oben erwähnten, frei

definierbaren Verhaltensweisen im Aktionsteil einer APPEL-Regel ins Spiel. Sie legen fest, unter welchen Bedingungen welche Daten weiterzugeben sind.

Prinzipiell lassen sich drei mögliche Ergebnisse der Verhandlungsphase unterscheiden:

1. Der Betreiber der Web-Site sammelt weniger Daten, als er eigentlich geplant hatte. Eventuell kann er aber in der Folge nicht die volle Funktionalität seines Dienstes bereitstellen, weil etwa für eine Beratungskomponente benötigte Informationen fehlen. Diese eingeschränkte Nutzbarkeit muss aber nicht darauf beruhen, dass die Leistungserbringung faktisch unmöglich wird. Vielmehr kann der Anbieter sie auch als Instrument bzw. Anreiz für den Kunden, sich kooperativer zu zeigen, einsetzen.

2. Der Kunde bzw. der Benutzeragent entschließt sich, dem Anbieter die angeforderten Daten doch zur Verfügung zu stellen, obwohl er damit den ursprünglichen Präferenzen zuwider handelt. Für ein solches Verhalten kann es verschiedene Gründe geben: beispielsweise bietet ein Betreiber kooperativen Kunden besondere Vergünstigungen wie Sonderangebote oder Rabatte oder die Web-Site ist nur nach Angabe sämtlicher Informationen uneingeschränkt nutzbar (siehe Punkt 1).

3. Wenn keine der beiden Seiten zu Zugeständnissen bereit ist, kommt es zu keiner Einigung, und der Kunde kann die Dienste des Anbieters nicht in Anspruch nehmen.

Leider sind in den bisherigen Versionen des P3P-Konzeptes Methoden zur Abwicklung einer mehrstufigen Verhandlung, und inbesondere deren automatische Behandlung durch einen Software-Agenten, zwar angedacht, aber noch nicht konkretisiert.

2.5 Kritische Würdigung des P3P-Ansatzes

Um die Eignung von P3P zur Verbesserung des Datenschutzes im WWW hat sich in letzter Zeit eine lebhafte Diskussion entwickelt. So führen Gegner der Initiative beispielsweise an, dass P3P die Entwicklung weiterer Lösungen für den Online-Datenschutz eher gehemmt als gefördert hat, indem ursprünglich der Anspruch erhoben wurde, alle Aspekte dieses Problemfeldes abzudecken, und deshalb die Öffentlichkeit die Dringlichkeit der Aufgabe nicht in ausreichendem Maße wahrgenommen habe. Tatsächlich lägen aber nach drei Jahren Projektlaufzeit nur wenige konkrete Ergebnisse vor [Catl99]. Auch seien die an dem Vorhaben beteiligten großen Unternehmen nicht die geeigneten Partner, wenn es darum gehe, den Datenschutz voran zu bringen, da ihr Interesse mehr darin liege, Daten über ihre Kunden zu sammeln, als deren Privatsphäre zu schützen. Dagegen ist zu sagen, dass P3P gerade deshalb relativ langsam vorangeschritten ist, weil man einen strukturierten Entwicklungsprozess durchlaufen hat, an dem viele Interessengruppen – auch vonseiten der Datenschützer – beteiligt waren [Clar98; Mull00].

Auch wird der Vorwurf erhoben, P3P sei nicht praktikabel, da der Kunde ohne einschlägige Gesetzesgrundlage keine Maßnahmen gegen einen Anbieter ergreifen könne, der sich nicht an die von ihm veröffentlichte Datenschutzpolitik hält. Allerdings kann die P3P-Initiative in Ländern, die bereits ein Internet-Datenschutzgesetz haben, ganz andere Aufgaben erfüllen als in solchen ohne eine derartige Regelung. In Letzteren gilt es, zunächst Aufmerksamkeit für das Problemfeld des Datenschutzes zu wecken und das öffentliche Bewusstsein zu steigern. Dagegen kann P3P in Deutschland, wo das **T**ele**d**iensted**a**tens**c**hutz**g**esetz (TDDSG) bereits viel strengere Regelungen vorsieht, v. a. die Transparenz der Datensammlung erhöhen [Grim00]. Daneben lassen sich marktwirtschaftliche Abläufe nachbilden, indem Angebot und Nachfrage den Austausch von persönlichen Informationen regeln [OV00b]: Der Benutzer entscheidet, für welche Gegenleistung er bereit ist, welche Daten über sich preiszugeben.

Allerdings gibt es in der Tat einige Aspekte im P3P-Konzept, die sich nicht vollständig mit den Regelungen des TDDSG vereinbaren lassen. So läuft es etwa dem Grundsatz der Datenvermeidung zuwider, dass es häufig eine Voraussetzung ist, persönliche Daten zu übermitteln, um eine Web-Site zu betreten, auch wenn kein zwingender, aus der Sache resultierender Grund dafür vorliegt. Dies leistet einem möglichen Missbrauch solcher Informationen Vorschub, d. h., der Anbieter sammelt Daten, die er zur Leistungserbringung nicht unbedingt benötigt. Auch die Tatsache, dass P3P nicht in jedem Fall eine ausdrückliche Zustimmung des Anwenders zur Erhebung seiner Daten vorsieht, sondern im Gegenteil häufig ein Opt-out, also eine Weigerung seitens des Kunden nötig ist, wäre in Deutschland nicht rechtmäßig. Schließlich ist noch anzuführen, dass P3P zwar bekannt macht, welche der gesammelten Informationen vom Kunden eingesehen werden können, jedoch keinen Mechanismus bereitstellt, der dies ermöglicht. Dies ist jedoch nach dem TDDSG für alle gesammelten Daten zwingend nötig.

Häufig unterstellt man der P3P-Inititiative auch ein „kritische Masse“-Problem [OV00c]. Es gäbe zu wenige Kunden, die daran interessiert wären, ihre Vorlieben bez. des Datenschutzes so detailliert auszuformulieren, wie P3P es vorsieht. Auf der anderen Seite wird P3P als ein guter erster Schritt bezeichnet, der mit seinem universellen technischen Standard [OV00b] gerade dazu geschaffen sein könnte, diese „kritische Masse“ zu erreichen. Auch das einheitliche Vokabular im Hinblick auf personenbezogene Daten und den Umgang mit ihnen wirkt in diese Richtung und macht darüber hinaus Datenschutzpolitiken leichter verständlich [Mull00]. Darüber hinaus lassen es andere Internet-bezogene Datenschutz-Werkzeuge, die ausschließlich auf Anonymisierung abzielen, gar nicht zu, individuell zugeschnittene Dienstleistungen über das Web anzubieten, wohingegen P3P dies mit seinem differenzierten Datenschema ausdrücklich unterstützt (siehe Abbildung 8).

Leider ist im ersten Entwurf der P3P-Spezifikation ein wichtiges Element, das ursprünglich vorgesehen war, nicht mehr enthalten. Dabei handelt es sich um den mehrstufigen Verhandlungsmechanismus, der für die automatische Abwicklung noch zu komplex erschien [OV00c]. Eine personelle Verhandlung, jedes Mal wenn ein Benutzer eine neue Web-Site betritt, erscheint zu aufwändig und damit ebenfalls nicht praktikabel. Dennoch ist die Struktur sowohl der Privacy Practices als auch des Data Repository sehr gut geeignet, um einen automatischen Verhandlungsprozess zu realisieren [Thib00], was derzeit bereits individuell erstellte Werkzeuge möglich machen, in Zukunft mit Version 2.0 der P3P-Spezifikation aber auch universell geregelt werden soll.

Einige weitere Argumente gegen P3P sind eher als Detail-, denn als Grundsatzkritik einzuordnen. So werden in der Strukturierung des Data Repository Transaktions- und Marketingdaten nicht strikt getrennt [Coyl00] und manche Begriffe sind nicht eindeutig definiert: So könnte es sein, dass ein Anbieter nach *Name* und *Alter* eines Kunden fragt, nach dessen Zustimmung jedoch das gespeicherte *Geburtsdatum* der Person übertragen wird. Dadurch würde eine eindeutige Identifikation sehr viel leichter möglich als nur mit der Altersangabe [Coyl99]. Ein weiteres Manko ist, dass ein Kunde auf jedem Rechner, an dem er arbeitet, seinen Benutzeragenten konfigurieren und pflegen muss. Für diesen Nachteil zeigt jedoch Kapitel 4 eine mögliche Lösung in Form eines Chipkarten-basierten Agenten auf.

Zusammenfassend lässt sich sagen, dass die erste Version der P3P-Spezifikation noch einige Schwachstellen aufweist, die aber, wie zu hoffen ist, in weiteren Entwicklungsstufen bereinigt werden können. Der Grundansatz, maschinenlesbar personalisierte und in Kategorien eingeteilte Informationen auszutauschen, scheint hingegen für individualisierte Dienstleistungen im WWW äußerst viel versprechend. Auch die geplante Funktionalität einer mehrstufigen, automatischen Verhandlungsphase bietet mannigfaltige Möglichkeiten, etwa in Online-Beratungssystemen.

3 P3P und das Franken-Mall-Projekt

Im Folgenden soll geprüft werden, inwiefern sich der P3P-Ansatz auf das Franken-Mall-Projekt übertragen lässt, welche Datenrubriken aus dem Data Repository hierbei von Nutzen sein könnten und ob auch ein Verhandlungsmechanismus zu verwirklichen ist. Dies geschieht anhand ausgewählter Funktionalitäten der beiden Teilbereichen des Projekts (siehe Abschnitt 1.1)

3.1 Eignung und Einsatzmöglichkeiten im Freizeitberatungs-Modul

Die Freizeitberatung arbeitet bisher mit einem Interessenprofil, das in einer relationalen Datenbank auf dem Web-Server abgelegt ist. Die Informationssammlung umfasst Interessen-

werte in verschiedenen Kategorien, wie Sehenswürdigkeiten, Musik, Sport oder Kultur, die wiederum in Unterrubriken aufgeteilt sind (z. B. Museen, Baudenkmäler etc. für Sehenswürdigkeiten oder verschiedene Musikrichtungen im Fall der zweiten Kategorie). Sie ließe sich ohne größere Schwierigkeiten in das Data Repository eines P3P-Anwenders übertragen, wo sie unter der Rubrik `<preference/>` einzuordnen wäre. Zusammen mit einer eindeutigen Identifizierung des Kunden (`<uniqueid/>`) stellt dies einen ersten wichtigen Schritt in Bezug auf die Anwendbarkeit von P3P im Rahmen des Beratungsmoduls dar, auf dem die anderen Funktionen aufbauen können. Als Zweck für die Datenerhebung wäre neben der Durchführung der aktuellen Tätigkeit `<current/>` auch der Aufbau eines Benutzerprofils zur individuellen Informationsversorgung `<individual-decision/>` anzugeben.

3.1.1 Erstellung eines individuellen Freizeitplans

Dieses Modul stellt für einen Kunden ein Programm zusammen, das er während seines Aufenthalts in einer Region absolvieren kann. Die Auswahl der empfohlenen Objekte erfolgt einmal anhand der oben erwähnten Freizeitinteressen, indem verstärkt solche Aktivitäten vorgeschlagen werden, die einen hohen Interessenwert im Profil besitzen. Darüber hinaus lassen sich aber auch demographische und sozio-ökonomische Informationen (`<demo-graphic/>`) zur Verfeinerung der Empfehlung heranziehen: Beispielsweise könnte man vom Einkommen der Person ableiten, in welcher Preiskategorie die Hotels liegen sollen, die man zur Buchung auswählt. Außerdem lässt sich anhand des Alters der Zielperson evtl. darauf schließen, welche Restaurants sie bevorzugt oder für welche Art von Theaterstücken sie sich besonders begeistert. Das Alter kann außerdem Anhaltspunkte dafür geben, wie sehr auf (wenig) körperliche Anstrengung im Programmablauf zu achten ist. Einen weiteren logischen Schritt stellt an dieser Stelle die Einbeziehung medizinischer Informationen (`<health/>`) dar, sodass etwa einem gehbehinderten Reisenden keine Attraktionen angezeigt werden, die er im Rollstuhl gar nicht erreichen kann (z. B. die Nürnberger Lochgefängnisse). Hier setzt die Aufgabe des Benutzeragenten an, der in einer möglichen Verhandlungsphase u. U., aufgrund seiner Regelbasis, zunächst nur die reinen Profildaten freigibt und später, nachdem das Beratungssystem erklärt hat, dass sich durch die Angabe weiterer Daten die Qualität des Freizeitplans verbessern kann, auch den Zugriff auf die weiteren genannten Rubriken gestattet (evtl. nach Rücksprache mit dem Anwender).

Daneben ergänzt der Algorithmus ein Freizeitprogramm auch mit Empfehlungen anderer Kunden, die einen ähnlichen Interessenverlauf besitzen wie der zu Beratende (Collaborative Filtering). Er greift dabei auf Bewertungen von bereits absolvierten Programmen dieser Kunden zurück und wählt diejenigen Aktivitäten mit hohen Durchschnittsnoten aus. Das System verwendet in diesem Fall also Nutzungsdaten, die durch explizite Aktivitäten (die

Online-Bewertung) zustande gekommen sind (<interactive/>) zur indirekten Auswertung (<individual-analysis/>). Auch hier ergibt sich ein Verhandlungsspielraum: Nur wer bereit ist, zumindest einen Teil der von ihm absolvierten Programme zu benoten, erhält im Gegenzug Empfehlungen anderer Teilnehmer.

3.1.2 Versenden eines personalisierten Veranstaltungs-Newsletters

Dieses Teilsystem stellt anhand des o. g. Benutzerprofils Veranstaltungen zusammen, die den jeweiligen Kunden interessieren könnten, und versendet sie periodisch. Zusätzlich zum Profil bedient es sich dabei noch weiterer Schlagworte, die der Anwender angeben kann, wenn er seinen Newsletter abonniert (es handelt sich somit um <interactive/>-Daten). Veranstaltungen, auf die sich eines der Schlagworte bezieht, nimmt der Algorithmus in jedem Fall in die zu versendende Nachricht auf. Danach erfolgt die Auswahl von „Events“, die aus Rubriken stammen, welche der Kunde sehr hoch bewertet hat. Ist die vorgegebene Kapazität des Newsletters damit noch nicht ausgeschöpft, so füllen weitere Ereignisse aus nachfolgenden Kategorien diese auf.

Darüber hinaus könnte man auch Verweilzeiten auf Beschreibungsseiten von Veranstaltungen protokollieren (<navigation/>) oder die tatsächlich getätigten Ticketkäufe (<purchase/>) über ein evtl. noch zu realisierendes Transaktionsmodul auswerten, um auf Interessenschwerpunkte des Kunden zu schließen.

Damit es den zusammengestellten Brief direkt versenden kann, muss dem System die E-Mail-Adresse des Abonnenten bekannt sein (<online/>). Hilfreich ist es auch zu wissen, welche Art von Mail-Programm dieser benutzt (<computer/>), da entweder einfache Textnachrichten oder grafisch gestaltete und damit komfortabler lesbare HTML-Dokumente verschickt werden, je nachdem, ob die Software in der Lage ist, diese zu verarbeiten.

3.1.3 Vermittlung von Freizeitpartnern und Virtual Community

Die Freizeitpartnervermittlung bietet ihren Nutzern zwei alternative Einstiegsmöglichkeiten: Einmal kann der Anwender aktiv nach einem Partner für eine bestimmte Aktivität suchen. Dazu gibt er das Datum an, an dem er etwas unternehmen möchte, sowie weitere Merkmale, die den Wunschpartner beschreiben, etwa dessen Alter und Geschlecht. Das Gegenstück dazu bildet die passive Eintragung in einen Pool mit möglichen Partnern, aus denen bei der aktiven Suche ausgewählt wird. In beiden Fällen gilt, dass die Zuordnung (das Matching-Verfahren) umso genauer arbeiten kann, je mehr Informationen die jeweiligen Anwender über sich preisgeben.

Diese Angaben können aus allen Sparten des P3P-Data-Repository stammen, da es darum geht, Personen einander zuzuordnen, die in vielen Lebensbereichen möglichst große Übereinstimmungen aufweisen bzw. möglichst gut zusammenpassen. Die Chance, einen Partner zu finden, steigt ebenfalls mit dem Umfang der bekannt gemachten Daten, da der Matching-Algorithmus davon ausgehen muss, dass bei fehlenden Werten für bestimmte Merkmale keine Übereinstimmung vorliegt, sodass kein hoher Ähnlichkeitswert erreicht werden kann. Es bietet sich demnach ein ideales Einsatzgebiet für einen Verhandlungsprozess nach dem zukünftigen P3P-Schema („Wenn Sie mir als Benutzer mehr Informationen über sich geben, kann ich Ihnen im Gegenzug zusichern, dass Ihre Chancen auf eine erfolgreiche Vermittlung steigen!“).

Eine weitere (geplante) Funktion, die - ebenso wie die Partnervermittlung - stärker die Interaktion zwischen den Anwendern betont, als die zwischen Kunde und Anbieter, ist eine Virtual Community für den Freizeitbereich. Gerade dieser Themenbereich weist zahlreiche Gelegenheiten auf, zu denen sich verschiedene Nutzer untereinander austauschen können. Beispielsweise ist an eine „personelle“ Partnervermittlung zu denken, indem ein Suchender seine Freizeitpläne und Partnervorstellungen auf einem elektronischen „schwarzen Brett“ veröffentlicht und sich Interessenten daraufhin persönlich bei ihm melden. Auch eine Art „Veranstaltungskritik“ ist möglich, in deren Rahmen Benutzer online Kinofilme, Theatervorstellungen o. Ä. rezensieren, um andere bei der Entscheidungsfindung zu unterstützen. Diese Art personenbezogener Daten fällt unter die P3P-Rubrik `<content/>`, der Nutzungszweck ist `<develop/>` und der Empfängerkreis `<public>`.

3.1.4 Routing-Modul

Bei der Routing-Komponente handelt es sich um ein Teilsystem der Freizeitberatung, das mithilfe eines genetischen Algorithmus zum einen – ähnlich der Freizeitplanerstellung in Abschnitt 3.1.1 – individuelle Programme für die Anwender zusammenstellt. Hierbei wird allerdings die geografische Lage der einzelnen Aktivitäten stärker berücksichtigt, sodass ein möglichst guter „Stadtrundgang“ entsteht, der dem Reisenden überflüssige Wege erspart. Zum anderen eignet sich dieses Modul auch dazu, vorgegebene Aktivitäten, die mittels anderer Verfahren (z. B. die in Abschnitt 3.1.1 geschilderten Methoden oder personelle Auswahl durch den Kunden selbst) selektiert wurden, in eine günstige Reihenfolge zu bringen. Plant der Anwender seinen Aufenthalt von zu Hause aus, kann das System zusätzlich die Anreise ausarbeiten, wozu es aber Informationen über seine Adresse benötigt (`<physical/>`). Da der Zugang zu dem beschriebenen Beratungssystem auch über Kiosk-Terminals vor Ort möglich sein soll, muss auch die Option berücksichtigt werden, direkt auf den aktuellen Standort des Kunden zuzugreifen (`<location/>`), um einerseits den Ausgangs-

punkt für die Routenplanung festzulegen und andererseits den Weg vom Kiosk-Terminal zur ersten Aktivität beschreiben zu können. Geht man noch einen Schritt weiter, könnten die Reisenden über das **G**lobal **P**ositioning **S**ystem (GPS), das mittlerweile immer mehr Hersteller in Armbanduhren, Mobiltelefone, PDAs, Digitalkameras und ähnliche Geräte integrieren [Lang00b], geortet werden (ebenfalls `<location/>`-Information). Damit ist es möglich, automatisch Ansagen zu bestimmten Sehenswürdigkeiten, an denen der Anwender gerade vorbeikommt, z. B. als MP3-Datei abzuspielen oder Wegbeschreibungen in Echtzeit an die tatsächlichen Laufwege des Reisenden anzupassen.

3.1.5 Abwicklung von Transaktionen

Eine weitere Funktion, die ein Freizeitberatungssystem anbieten könnte, ist die Online-Durchführung von Transaktionen. Hier ist etwa an den Kauf von Fahrkarten sowie Eintrittskarten für empfohlene Veranstaltungen (Theater, Museum usw.) oder an die Reservierung und Buchung von Hotelzimmern zu denken. Um diese Vorgänge abwickeln zu können, benötigt das Modul unter anderem Daten über getätigte Käufe, den aktuellen Warenkorb des Kunden sowie die gewünschte Zahlungsart (`<purchase/>`. Bei größeren Beträgen, wie z. B. bei der Buchung für eine ganze Reisegruppe, sind unter Umständen auch Auskünfte über die finanzielle Situation und das Zahlungsverhalten in der Vergangenheit wünschenswert (`<financial/>`). Diese Aufgabe, Online-Einkaufsprozesse abzubilden und zu unterstützen, stellt gleichzeitig die Schnittstelle zum Shopping-Modul der Franken-Mall dar.

3.2 Eignung und Einsatzmöglichkeiten im Shopping-Modul

Kundenorientierung spielt gerade beim Electronic Shopping eine große Rolle. Primäres Ziel einer umfassenden Kundenbetreuung ist es, den Kunden langfristig zu binden. Eine Kundenbindungsstrategie bringt eindeutige, ökonomische Vorteile, denn Neukunden zu akquirieren ist teurer als Kunden zu halten (siehe [Diet97, S. 270] und [KoBl99, S. 28]). Kotler und Bliemel [KoBl99, S. 28] nennen verschiedene Kundenbindungsstrategien. Die vom Kunden bevorzugte Art der Bindung ist diejenige, die auf Zufriedenheit und Vertrauen beruht. Es ist also u. a. die Aufgabe einer Mall, Vertrauen zum Kunden aufzubauen. Zufriedene Kunden bleiben länger „treu“, bevorzugen auch neue Produkte, denken und sprechen gut über die Mall und beachten Angebote der Konkurrenz weniger stark. Insgesamt ist ein solcher Kunde kostengünstiger zu betreuen, da Transaktionen mit ihm zur Routine werden. Eine weitere Zielsetzung der Shopping Mall ist es, den Nutzen ihrer Kunden zu steigern sowie deren Erwartungen zu erfüllen (zu *Steigerung der Nutzensumme des Kunden* siehe [Blie00, S. 14ff.]). Dies bringt ihr wiederum einen Vorteil, der sich in Form von Wiederholungs- und Zusatzkäufen oder Weiterempfehlungsabsichten des Kunden zeigen kann.

Da, anders als beim Real-Shopping in einem Kaufhaus, bei einer Mall kein direkter Kundenkontakt stattfindet, ist es umso wichtiger, zum richtigen Zeitpunkt mit den richtigen Argumenten ein maßgeschneidertes Informations- und Leistungsangebot zu unterbreiten. Dazu gehört das Anbieten eines geeigneten Produktes, eines Preises, eines Liefertermins etc. Eine Voraussetzung zu einem umfassenden und individuellen Angebot ist die möglichst genaue Kenntnis des Kundenprofils, also spezifische Interessen, Präferenzen, Einstellungen sowie der Kaufhistorie des Mall-Kunden.

P3P kann zur Erfassung und Bearbeitung kundenspezifischer Daten eine Unterstützung bieten. Dies wird durch einen permanenten Informationsfluss zwischen der Mall und ihren Kunden sichergestellt, sodass Daten in adäquater Art und Menge zur Verfügung stehen. Bei der Erhebung der Daten ist zwischen der expliziten Benutzermodellierung (über Fragen an den Nutzer) und der impliziten Benutzermodellierung (durch Beobachtung des Einkaufsverhaltens) zu unterscheiden. Schumann [Schu00, S. 127ff.] hat wichtige Daten bei der Abwicklung von Transaktionen in einer Shopping Mall zusammengestellt. Die Übersicht in Abbildung 11 ist ein Auszug auf der Basis von Schumanns Recherchen.

Kunden-Daten	Informationsquellen	Verwendung
Personenbezogene Daten: - Unkritische Daten (Name, Anschrift, E-Mail, Telefonnummer, Lieferadresse) - Sensible Daten (Alter, Ausbildung, Beruf, Haushaltseinkommen, Familienstand, besondere Lebensumstände, z. B. Hobbys, Krankheiten)	Explizite Angaben des Kunden: - Anmeldung zum System - Erste Bestellung - Gewinnspiel - Kundenbefragung - ...	- Persönliche Anrede - Lieferung bestellter Ware - Gezielte Ansprache im Rahmen von Marketingmaßnahmen - Vorhersage latenter Bedürfnisse - Ableitung von Produktpräferenzen - Beratung
Reaktionsdaten: - Vergangenheitseinkäufe - Beschwerden - Anregungen - ...	Explizite Angaben des Kunden: - Bewertung von Produktempfehlungen - Beschwerdemanagement Beobachtung des Kunden: - Tatsächlich getätigte Einkäufe	- Empfehlung von Produkten - Anpassung des Sortiments - Verbesserung des Dienstleistungsangebots
Potenzialdaten: - Kontakthäufigkeit - Kaufverhalten (z. B. Navigations-, Informations-, Entscheidungsverhalten) - Bestellfrequenz - Umsatz pro Bestellung - Gesamtumsatz - Wie lange ist er bereits Kunde? - ...	Beobachtung des Kunden: - Interaction Tracking (Messung von Verweilzeiten, Reihenfolge der aufgerufenen Seiten) - Auswertung des Warenkorbes - ...	- Cross-Selling-Möglichkeiten - Abschätzung von Wiederbeschaffungsintervallen - Gezielte Marketingmaßnahmen

Abbildung 11: Relevante Daten beim Electronic Shopping

Kritisch sind hierbei die personenbezogenen sensiblen Daten zu sehen. Um diese der Mall zur Verfügung zu stellen, muss der Anwender ein absolutes Vertrauen in die Sicherheit und

Diskretion der Mall haben. Dazu sollte ein Zusatznutzen für ihn erkennbar sein (Prinzip des Value Exchange, [Schu00, S. 126]). Die Reaktionsdaten geben Aufschluss darüber, wie gut oder schlecht sich der Konsument beraten fühlt und wie zufrieden er mit den gekauften Waren ist. Anhand dieser Daten wird das Bild des Anwenders ständig ergänzt, was wiederum die Basis zur kontinuierlichen Verbesserung der Qualität der Beratung sein kann. Die erfassten Potenzialdaten sind die Grundlage für eine evtl. Kundenbewertung, insbesondere um Nutzer zu selektieren, bei denen ein gewisses Umsatzpotenzial vermutet wird. Damit können diese Daten auch als Ausgangspunkt für die Planung gezielter Marketingmaßnahmen gesehen werden.

Abbildung 9 (S. 12) zeigt die Kategorien des P3P-Benutzerprofils. Bezogen auf die relevanten Daten beim Electronic Shopping könnten über die P3P-Werte `<physical/>` und `<online/>` alle personenbezogenen unkritischen Daten abgelegt werden. Die sensiblen Daten lassen sich über `<demographic/>`, `<health/>` und `<preference/>` erfassen.

Alle personenbezogenen Daten dienen dem Erstaufbau eines Benutzerprofils, ganz gleich ob zur individuellen Informationsversorgung (über `<pseudo-decision/>` oder `<individual-decision/>`) oder zur indirekten Auswertung (über `<pseudo-analysis/>` oder `<individual-analysis/>`) (siehe Abbildung 6, S. 10). Bei einer gezielten Ansprache im Rahmen von Marketingmaßnahmen kommt als Zweck `<contact/>` infrage.

Zur Erfassung der Reaktionsdaten bedient sich P3P u. a. des Wertes `<content/>`, worüber explizite Äußerungen des Anwenders, z. B. Beschwerden und Anregungen, erfasst werden. Auf dieser Basis kann es zur Anpassung des Sortiments oder Verbesserung des Dienstleistungsangebots kommen, was unter `<develop/>` festgehalten wird.

Die Potenzialdaten lassen sich über `<navigation/>` (z. B. Navigationsdaten, Verweilzeiten etc.), `<purchase/>` (Zahlungsart, Umsatz pro Bestellung usw.) und `<financial/>` (z. B. Zahlungsverhalten) erfassen. Diese Daten können ein weiterer Anlass für gezielte Marketingmaßnahmen (`<contact/>`, siehe oben) sein.

Alle erhobenen Daten (personenbezogene, Reaktions- und Potenzialdaten) dienen dem Aufbau eines Kundenprofils. Dieses wird im Data Repository abgelegt. Je nach Datenart kommt es zu keiner Speicherung (`<no-retention/>`) bis hin zur beliebig langen Speicherung der Kundendaten (`<indefinitely/>`) (vgl. Abbildung 8, S 11). In jedem Fall wird der Kunde über die Art und Dauer der Datenhaltung informiert, ebenso über den Empfänger seiner Daten (vgl. Abbildung 7, S. 11). Gerade für eine Mall ist eine gute Informationspolitik wichtig, um das Vertrauen des Kunden zu gewinnen. Erst dies stellt eine Basis für gezielte Aktionen der Kundenansprache und -beratung dar. Je öfter Transaktionen zwischen der Mall und dem Kunden getätigt werden, umso besser lässt sich ein relativ scharf umrissenes Bild von den Verbrauchsgewohnheiten und Vorlieben des Konsumenten darstellen. Daraus ergibt sich ein

Nutzen für die Mall dahingehend, dass sich Erkenntnisse hinsichtlich der Präferenzen des Konsumenten, aber auch wichtige Hinweise auf Cross-Selling-Potenziale für eine kontinuierliche, qualitative Verbesserung der Mall nutzen lassen.

Auf der Basis der erhobenen Daten könnte man, wie es auch in der Marktforschung üblich ist, Stereotypen aufbauen. Hierzu bedient man sich der Lebensstilanalyse. Dabei wird davon ausgegangen, dass das Interesse eines Kunden an einem bestimmten Produkt von seinem Lebensstil bestimmt wird. Durch die Analyse wurde festgestellt, dass die konsumierten Produkte in der Tat Ausdruck des Lebensstils sind (ausführlicher in [KoBl99, S. 443f.]). Es gibt mehrere Klassifizierungsansätze für den Lebensstil (siehe dazu [KoBl99, S. 320ff.]). Die Lebensstilanalyse bietet eine gute Grundlage für die Stereotypisierung von Mall-Nutzern. P3P kann dazu alle wichtigen Daten liefern. Den Anbietern von Produkten in einer Shopping Mall bietet sich hierdurch eine Möglichkeit, ihre Produktpalette / ihr Angebot besser auf die Zielgruppe auszurichten, aber auch eine gezieltere Werbung durchzuführen.

4 Multifunktionale Chipkarte als P3P-konformer User Agent

In Abschnitt 2.5 wurde als ein Manko des P3P-Konzepts bereits erwähnt, dass ein mobiler Anwender, der von verschiedenen Rechnern aus P3P-konforme Web-Sites nutzt, auch mehrere Benutzeragenten bzw. Regelbasen pflegen muss. Gerade für das Anwendungsgebiet der Freizeitberatung, stellt dies einen erheblichen Nachteil dar. Denn hier ist es als Normalfall anzusehen, dass der Kunde sich zunächst vorab am heimischen PC orientiert und dann vor Ort am Reiseziel etwa an einem Kiosk-Terminal, wie sie die Telekom bis Ende 2001 plant [OV00d], Detailinformationen abruft. Diese Schwachstelle ließe sich umgehen, wenn der Benutzer sein Profil stets bei sich tragen würde, was z. B. die Speicherung auf einer Chipkarte ermöglicht.

4.1 Rahmenbedingungen

Das in Abschnitt 1.1 erwähnte, mittelfränkische Konzept zum Media@Komm-Wettbewerb sieht eine multifunktionale Chipkarte als zentrale Klammer über alle Teilprojekte vor. Diese soll die Kommunikation zwischen allen drei Zielgruppen (Bürger, private Unternehmen und Kommunen) unterstützen. Um zugleich einen hohen Verbreitungsgrad der Karte und eine hohe Akzeptanz in der Bevölkerung zu erreichen, sieht das Konzept vor, die potenziellen Anwender nicht durch die Ausgabe einer neuen, zusätzlichen Karte zu belasten. Vielmehr ist geplant, weit verbreitete Karten mit den relevanten Zusatzfunktionalitäten auszustatten. Insbesondere wollen einige ortsansässige Banken und Sparkassen ihre ec-Karten mit den

Media@Komm-Anwendungen aufrüsten, wodurch im Rahmen der Projektlaufzeit schätzungsweise ca. 80 % der in der Region umlaufenden Bankkarten abgedeckt werden können. Die Tatsache, dass Kreditinstitute maßgeblich an der Verbreitung der Karte beteiligt sind, spiegelt sich auch in der Zusammensetzung des Anwendungsportfolios auf dem Chip wider, wie der Abbildung 12 zu entnehmen ist.

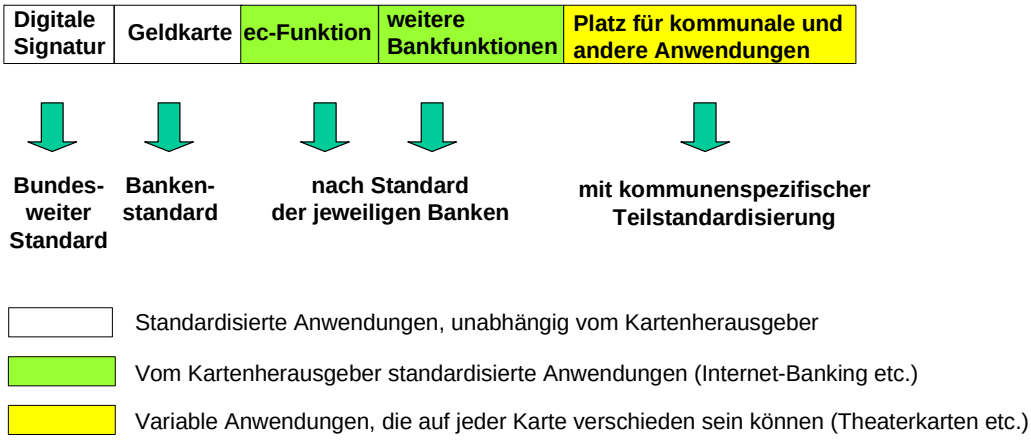

Abbildung 12: Speicheraufbau der multifunktionalen Chipkarte

Zu den Basiselementen *Unterstützung der Digitalen Signatur* (asymmetrische Verschlüsselung etc.) und *bargeldlose Bezahlung per Geldkarte* (d. h. Nutzung als elektronische Geldbörse) treten zunächst weitere bankbezogene Aufgaben. Wie oben bereits erwähnt, rüsten die Ausgabeinstitute im Rahmen des Media@Komm-Projekts ihre ec-Karten multifunktional auf, wovon die ec-Funktion natürlich unberührt bleibt.

Darüber hinaus kommen aber noch weitere Bankfunktionen, wie Abfrage von Aktiendepots, Abwicklung von Kreditanträgen etc. hinzu. Der verbleibende Speicherplatz steht für kommunale (z. B. elektronisches Einwohnermeldeamt, Abwicklung von Baugenehmigungen) und sonstige Anwendungen (hierunter fällt auch die Franken-Mall) zur Verfügung.

4.2 P3P-Funktionalität

Um einen P3P-konformen Benutzeragenten mithilfe der oben beschriebenen Chipkarte zu realisieren, könnte man vorgehen wie in Abbildung 13 skizziert.

Zunächst ist der Kartenspeicher um eine weitere Rubrik, welche die für P3P relevanten Daten bzw. Algorithmen enthält, zu erweitern. Wegen der begrenzten Kapazität der Karte findet sicherlich nicht der komplette Software-Agent mit allen benötigten Daten direkt auf der Karte Platz. Um festzulegen, welche Teile wo gespeichert werden, ist eine Dreiteilung sinnvoll: Einmal sind hier die in Abschnitt 2.3.3 erwähnten Rechenvorschriften zur Evaluation eines Rulesets zu nennen. Sie sind vom P3P-Gremium festgelegt und bei jedem Benutzer identisch,

sodass sie nicht auf der Chipkarte, sondern im jeweiligen Kiosk-Terminal, PC oder sonstigen Zugangssystem abgelegt werden können.

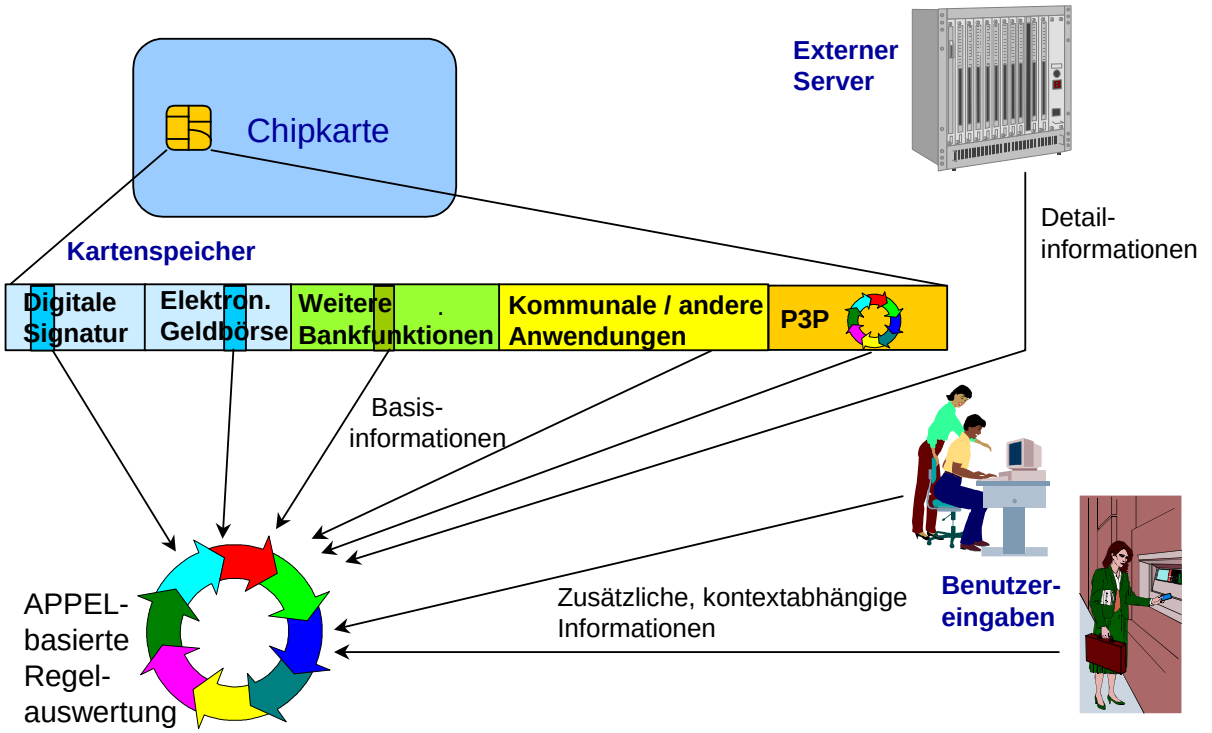

Abbildung 13: Multifunktionale Chipkarte als P3P-konformer Benutzeragent

Die beiden übrigen Rubriken sind:

- die Regelbasis, die der Anwender definiert, und
- seine persönlichen Daten im Data Repository.

Sie sind ein wenig differenzierter zu betrachten. Einige Informationen (wie z. B. der Name des Benutzers) werden sehr häufig oder von fast allen Anwendungen benötigt. Solche Daten könnte man direkt auf der Karte unterbringen, um den Zugriff schnell und kostengünstig zu halten. Anders verhält es sich mit Angaben, die nur für wenige Funktionen zur Verfügung stehen müssen. Diese könnte man auf einen externen Server auslagern, von wo sie bei Bedarf heruntergeladen werden. Um die Sicherheit von Daten zu gewährleisten, die sich nicht mehr im direkten Einflussbereich des Kunden befinden, und um dessen Vertrauen in das System zu stärken, ist es nötig, bestimmte Maßnahmen zu ergreifen. So sollte der Betreiber des Servers ein unabhängiger Dritter sein, dem die Anwender vertrauen. Außerdem ist es erforderlich, die Daten verschlüsselt abzuspeichern, sodass ein Zugriff wiederum nur mithilfe der Chipkarte möglich ist, die bereits über die dafür nötigen Mechanismen verfügt. Durch die erforderliche Online-Verbindung und die durchzuführende Dechiffrierung der persönlichen Informationen ist ein solcher Zugriff gegenüber der direkten Speicherung auf der Karte sowohl teurer als auch langsamer, sodass man genau abwägen muss, welche Werte auf welchem Medium vorzuhalten sind.

Schließlich gibt es noch Informationen, die zum Zeitpunkt der Leistungserbringung dem System noch gar nicht bekannt sind. Diese gibt der Anwender im Dialog ein. Daraufhin werden sie, je nachdem was die Privacy Policy des Anbieters festlegt, nach der Durchführung der Transaktion wieder gelöscht, auf der Karte gespeichert oder an den externen Server weitergeleitet.

Ähnlich wie mit dem Data Repository verhält es sich mit der Regelbasis. Häufig benötigte Regeln (aufgrund der Auswertungsmechanik des P3P-Regelinterpreters, der die Vorschriften sequenziell prüft, bis eine feuern kann, wären dies wohl die ersten *n* Regeln eines Rulesets) bzw. solche, die meist zu einem Ergebnis führen (z. B. die `<otherwise>`-Regel), legt man direkt auf der Karte ab, während auf andere ebenfalls extern zugegriffen wird. Dabei mag die „optimale“ Verteilung, sowohl der Daten als auch der Auswertungsvorschriften, im Laufe der Zeit durchaus variieren. Protokolliert das System Zugriffshäufigkeiten und -zeitpunkte mit, lassen sich für die „Verdrängung“ von Elementen aus dem Kartenspeicher auf den „Hintergrund“-Server ähnliche Algorithmen anwenden wie sie von der virtuellen Speichertechnik in Datenbankmanagement- oder Betriebssystemen bekannt sind [Mert00, S. 14].

4.3 Anwendungsszenario

Im Folgenden soll an einem konkreten Beispiel aufgezeigt werden, wie die vorgestellten Konzepte bei der Leistungserbringung in der Franken-Mall zusammenwirken:

Ein Anwender, der bereits P3P nutzt, betritt zum ersten Mal vom heimischen PC aus die Franken-Mall, um sich ein individuelles Aufenthaltsprogramm für ein Wochenende in Nürnberg zusammenstellen zu lassen. Aufgrund früherer P3P-Sitzungen sind so grundlegende Daten wie Name, Alter und evtl. E-Mail des Kunden bereits direkt auf der Karte vorhanden und auch über die Regelbasis für eine individuelle Leistungserbringung freigegeben. Über seine Freizeitpräferenzen ist aber noch nichts bekannt, da er erstmals ein touristisches Beratungssystem nutzt. Deshalb bittet ihn das System, die relevanten Informationen im Dialog einzugeben und um die Erlaubnis, diese bei Bedarf dauerhaft speichern zu dürfen. Wie in Abschnitt 3.1.1 bereits erwähnt, zieht das Beratungsmodul aber auch Gesundheitsinformationen heran, um die körperliche Leistungsfähigkeit der jeweiligen Zielperson in die Beratung einfließen zu lassen und so Überbelastungen zu vermeiden. Obwohl diese Informationen bereits auf einem externen Server verschlüsselt gespeichert sind, meldet der Benutzeragent an dieser Stelle die Verletzung einer Regel, da der Anwender seine Gesundheitsinformationen nur für Zugriffe ärztlicher Systeme freigegeben hat. Nachdem das System ihm erklärt hat, wozu es solche Daten benötigt, mag er zustimmen, einige der unkritischeren Informationen freizugeben. Es erfolgt ein Zugriff auf den Server, bei dem die Verschlüsselungsalgorithmen der Chipkarte zum Einsatz kommen.

Nach der Zusammenstellung des Wochenendprogramms möchte der Reisende evtl. für die Theatervorstellung, die ihm empfohlen wurde, Eintrittskarten kaufen. Hier befindet sich die Schnittstelle zum Shopping-Modul der Mall, das nach Abwicklung der Transaktion in unserem Beispiel zur Zusendung der Tickets auf die physische Adresse des Kunden zugreift, falls dieser es erlaubt hat. Anschließend kann der Kunde durch Eingabe seiner PIN direkt über die ec-Funktionalität seiner Chipkarte bezahlen.

Nach seiner Ankunft beschließt der Benutzer, sich an einem Kiosk-Terminal für einen Teil der ihm empfohlenen Aktivitäten einen „Rundreiseweg“ ausarbeiten zu lassen. Den dazu benötigten aktuellen Aufenthaltsort kann die Routenplanung in diesem Fall auch ohne GPS aus dem Standort des Terminals ermitteln und die Gebühr für den farbigen Ausdruck der Route lässt sich direkt von der elektronischen Geldbörse (siehe Abbildung 12) abbuchen.

5 Ausblick

Kapitel 3 dieses Berichts hat gezeigt, dass sich die in P3P spezifizierten Strukturen sehr gut in beiden Teilen der Franken-Mall einsetzen lassen. Fast alle bisher konzipierten oder bereits als Prototyp realisierten Teilmodule könnten auf dem P3P-Benutzermodell aufbauen, da die dort festgelegten Informationskategorien den größten Teil der in der Mall benötigten Daten abdecken. Auf diese Weise ließe sich ein standardisiertes Datenmodell kreieren, was die Übertragung des Franken-Mall-Konzepts auf andere Regionen (die ja bereits angedacht ist) erleichtern würde. Auch aus den zukünftigen P3P-Funktionen, wie z. B. dem automatisierten Verhandlungsmechanismus, können v. a. die komplexeren Beratungsmodule (wie in Abschnitt 3.1 beschrieben) Nutzen ziehen.

Nun gilt es zu prüfen, ob auch die anderen (kommunalen und privaten) Teilprojekte im Nürnberger Media@Komm-Konzept, und insbesondere die Herausgeber der Chipkarte, mit der P3P-Spezifikation arbeiten können bzw. wollen. Denn einerseits kommen erst dadurch die Vorteile eines standardisierten Kundenprofils richtig zur Geltung, andererseits könnte nur dann die Karte in Zukunft als P3P-Benutzeragent ausgestaltet werden.

Darüber hinaus entstehen in beiden Teilgebieten der Mall weiterhin neue Konzepte und Prototypen. Im Shopping-Bereich wird derzeit an der Unterstützung unterschiedlicher „Lebenslagen“ (wie Hochzeit, Umzug, Autokauf u. Ä.) durch den Rechner gearbeitet. Das System soll den Anwender bei der Abwicklung der oft recht komplexen Vorgänge anleiten, damit nichts vergessen wird, und Teilaufgaben, die automatisiert werden können, auch selbst übernehmen. Zunächst wird exemplarisch das Ereignis Autokauf untersucht, da hier sowohl der private (Autohändler, Versicherungen etc.) als auch kommunale Bereich (Zulassungsstelle, Anwohnerparkausweis usw.) betroffen sind, was gut zum Gesamtkomplex Media@Komm passt.

Ein Reisekonfigurator, der aus größeren Reisebausteinen weitgehend automatisiert Pauschalreisen „zusammenbauen“ soll, ergänzt demnächst die Freizeitberatung. Hier kommt es zuerst darauf an, sinnvolle Bausteine zu identifizieren und strukturiert zu beschreiben. Anhand dieser Beschreibung kann dann eine Auswahl von Modulen automatisch über einen Abgleich mit dem jeweiligen Benutzerprofil erfolgen. Abschließend müssen die selektierten Bausteine noch unter Berücksichtigung von (Zeit-)Restriktionen zu einem Reisepaket geschnürt werden.

Literaturverzeichnis

[Blie00] *Bliemel, F. et al. (Hrsg.):* Electronic Commerce; Herausforderungen – Anwendungen – Perspektiven. 3. Auflage, Gabler, Wiesbaden 2000.

[Bray98a] *Bray, Tim et al.:* Extensible Markup Language (XML) 1.0 - W3C Recommendation. http://www.w3.org/TR/1998/REC-xml-19980210.html, 1998-02-10, Abruf am: 2000-12-12.

[Bray98b] *Bray, Tim:* RDF and Metadata. http://www.xml.com/xml/pub/98/06/rdf.html, 1998-06-09, Abruf am: 2000-12-12.

[Catl99] *Catlett, J.:* Technical standards and privacy, http://www.junkbusters.com/ht/en/standards.html, 1999-09-13, Abruf am: 2000-12-12.

[Clar98] *Clarke, R.:* Platform for Privacy Preferences – A Critique. In: Privacy Law and Policy Reporter 5 (1998) 3, S. 46-48.

[Conn98] *Connolly, Dan:* Naming and Addressing: URIs, URLs, ... http://www.w3.org/Addressing/, Abruf am: 2000-12-12.

[Coyl00] *Coyle, K.:* A Response to „P3P and Privacy: An Update for the Privacy Community“ by the Center for Democracy and Technology. http://www.kcoyle.net/response.html, Abruf am: 2000-12-12.

[Coyl99] *Coyle, K.:* P3P: Pretty Poor Privacy? – A Social Analysis of the Platform for Privacy Preferences. http://www.kcoyle.net/p3p.html, Abruf am: 2000-12-12.

[Cran98] *Cranor, Lorrie F.:* Internet privacy: a public concern. In: netWorker: The Craft of Network Computing, 2 (1998) 3, S. 13-18.

[Diet97] *Dietze, U.:* Reklamationen als Chance nutzen. Moderne Industrie, Landsberg/Lech 1997.

[Grim00] *Grimm, R. et al.:* P3P and the privacy legislation in Germany: can P3P help to protect privacy worldwide?. http://sit.gmd.de/~grimm/texte/P3P-Germany-e.pdf, Abruf am: 2000-12-12.

[KoBl99] *Kotler, P.; Bliemel, F.:* Marketing-Management. 9. Auflage, Schäffer Poeschel, Stuttgart 1999.

[Lang00a] *Langheinrich, Marc et al.:* A P3P Exchange Language (APPEL) – W3C Working Draft. http://www.w3.org/TR/2000/WD-P3P-preferences-20000420, 2000-04-20, Abruf am: 2000-12-12.

[Lang00b] *Lange, Edgar:* Lotse am Handgelenk. In: Wirtschaftswoche o.Jg. (2000) 34, S. 92.

[Lass97] *Lassila, Ora:* Introduction to RDF Metadata – W3C Note. http://www.w3.org/TR/NOTE-rdf-simple-intro-971113.html, 1997-11-13, Abruf am: 2000-12-12.

[Lass99] *Lassila, Ora et al.:* Resource Description Framework (RDF) Model and Syntax Specification – W3C Recommendation. http://www.w3.org/TR/1999/REC-rdf-syntax-19990222, 1999-02-22, Abruf am: 2000-12-12.

[Marc00] *Marchiori, Massimo et al.:* The Platform for Privacy Preferences 1.0 Specification. http://www.w3.org/TR/2000/WD-P3P-20000915, 2000-09-15, Abruf am: 2000-12-12.

[Meis96] *Meissner, R.:* Faules Backwerk - Auf dem Weg zum gläsernen Web-Surfer. In: c't o.Jg. (1996) 6, S. 25.

[Mert00] *Mertens, Peter et al.:* Grundzüge der Wirtschaftsinformatik. 6. Auflage, Springer, Berlin 2000.

[Mill98] *Miller, Eric:* An Introduction to the Resource Description Framework. In: D-Lib Magazine, 4 (1998) 5. http://www.dlib.org/dlib/may98/miller/05miller.html, Abruf am: 2000-12-12.

[Mull00] *Mulligan, D. et al.:* P3P and Privacy: An Update for the Privacy Community. http://www.cdt.org/privacy/pet/p3pprivacy.shtml, 2000-03-28, Abruf am: 2000-12-12.

[NIK99] *NIK e. V.:* Konzeption zum Projekt „RegioSignCard" – Wettbewerbsbeitrag des NIK e. V. (Nürnberger Initiative für die Kommunikationswirtschaft e. V.) für den Städteverbund Nürnberg-Fürth-Erlangen-Bayreuth im Rahmen des bundesweiten Städtewettbewerbs MEDIA@Komm. Nürnberg 1999.

[OV00a] *O .V.:* XML FAQ. http://www.textuality.com/xml/faq.html, Abruf am: 2000-12-12.

[OV00b] *O. V.:* Pressemitteilung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak00/p3p_pm.htm, 2000-08-29, Abruf am: 2000-12-12.

[OV00c] *O. V.:* Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. http://www.epic.org/Reports/prettypoorprivacy.html, Abruf am: 2000-12-12.

[OV00d] *O. V.:* Telekom plant öffentliche Internet-Stationen. In: Frankfurter Allgemeine Zeitung vom 2000-12-01, S. 19.

[Schu00] *Schumann, P.:* Die Electronic Mall im internetbasierten Handel; Betriebswirtschaftliches und informationstechnisches Konzept. Gabler, Wiesbaden 2000.

[Thib00] *Thibadeau, R.:* A Critique of P3P: Privacy on the Web. http://dollar.ecom.cmu.edu/p3pcritique/CritP3P.PDF, 2000-08-24, Abruf am: 2000-12-12.

[Weib98] *Weibel, S. et al.*: Dublin Core Metadata for Resource Discovery. http://www.ietf.org/rfc/rfc2413.txt, Abruf am: 2000-12-12.

[Weit99] *Weitzner, Daniel J.:* Building Trust on the Web: Platform for Privacy Preferences (P3P). Vortrag auf der 8. International World Wide Web Conference, Toronto/Kanada 1999. http://www.w3.org/Talks/1999/0511-www8p3p/, Abruf am: 2000-12-12.

Gesetzestexte

[BDSG] Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954). http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm, 1997-12-17, Abruf am: 2000-12-12.

[IuKDG] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) vom 22. Juli 1997 (BGBl. I S. 1870). http://www.iid.de/rahmen/iukdgbt.html, 1997-06-13, Abruf am: 2000-12-12.