# Multi Dimensional Personalisation Architecture Proposal for a Prototype

S.W.Schilke[1, 2], U.Bleimann[2], S.M.Furnell[1] and A.D.Phippen[1]

[1] Centre for Information Security and Network Research, University of Plymouth,
Plymouth, United Kingdom
[2] Institute of Applied Informatics Darmstadt (aida),
University of Applied Sciences Darmstadt, Germany
e-mail: steffen@schilke.net

## Abstract

Multi Dimensional Personalisation (MDP) is based on the location, the interest and the location of the user. Recommendations of online content as well as offline events shall be offered to the user. At the right time, at the right place the right information or service will be offered. Instead of having to request this information this new service concept would proactively provide the information and services. MDP depends on a loosely coupled communication between the mobile device client and the MDP / server. In this paper the communication paths between the mobile MDP client and the MDP server are described. In addition an architecture proposal for the implementation of a MDP prototype is presented. This prototype implementation has to cover the user requirements of protecting the privacy and at the same time allowing the openness to deal with information / service providers. In addition it can be used to evaluate the feasibility of the proposed MDP architecture.

## Keywords

LBS, Location Based Services, Personalisation, GPS, Architecture, Multi Dimensional Personalisation, REST

## 1. Introduction

This paper describes the proposed architecture for the client and server side for the implementation of the Multi Dimensional Personalisation (MDP) services. MDP can be considered the next generation of a personalisation approach which goes beyond where most personalisation projects have gone before. Besides the personalisation efforts the location of the user will be taken into account. In addition a temporal dimension will be considered. These shall be considered to be the main dimensions used or applied for this new personalisation approaches hence the name Multi-Dimensional-Personalisation.

The scope of the proposal covers the communication paths, the mobile device and a loosely coupled server architecture which shall fulfil the requirements and is later capable to scale into a real world scenario.

In addition the implementation has to cope with the technical problems like the problem of protecting the privacy of the users via the proposed Chinese Wall concept (Schilke et al, 2005). This will be implemented by using a shadow data base with anonymised user data.

### 1.1. Multi Dimensional Personalisation

The concept of Multi Dimensional Personalisation (MDP) was first described in 2003 (Schilke, 2003). This concept goes beyond the “traditional” personalisation concepts used on web sites or portals nowadays (Abowd & Mynatt, 2000). The concept combines different (multiple) dimensions like time, location (past and future movement patterns) and the interests of the user to provide the user with an automatic personalisation experience which spans from the online world to the offline world (Schilke *et al.* 2004; Abowd & Mynatt, 2000; José and Davies, 1999; Mobasher *et al.* 2001).

As users are concerned about the privacy (like message content, identity, location and actions (e.g. connection to services) - (Askwith *et al.* 2000).) and their privacy is protected by laws (e.g., based on the German Teleservices Data Protection Act (1997) reference by Kobsa, 2002) such an application has to take this into account.

In order to achieve this a Chinese Wall concept is proposed (Schilke *et al.* 2005) which separates the Single Point of Trust (Schilke *et al.* 2006a), i.e., the MDP provider, from the service providers. This allows the service provider to request the publishing of their services to end users anonymously. By doing so the MDP provider becomes the Single Point Of Trust (SPOT). Via the MDP / SPOT it is possible to approach users without a breach in the protection of their privacy. The user knows which service provider is approaching him but the service provider will only get access to an anonymous profile of the user (Schilke *et al.* 2007). This knowledge can be used to rate service providers or report spam or unwanted recommendations.

The following sections introduce the architecture of mobile device operating systems, the communication for the proposed MDP client and server, the Chinese Wall concept used to implement a SPOT for the MDP users and a proposed architecture model for the communication between MDP client and server. This shall be the base for a discussion of the proposed architecture and the implementation of the MDP prototype for evaluation purposes.

## 2. Mobile Device Architecture

According to market research data from IDC (Business Week, 2008 ) the main players in the mobile phone device (i.e., mobile phones, smart phones) market are Nokia (i.e., Symbian 56%), Microsoft (Windows Mobile 13%), Research In Motion (i.e., Blackberry 12%), Linux (e.g., LiMo or OpenMoko 9.4%), Apple iPhone (6.9%), Plam OS (2%), Google (0% as no devices are available – based on Linux and Java) among other market minorities like local or specialist systems in the market.

The most systems use a layered architecture (e.g., Google, 2008a; LiMo; OpenMoko; Symbian) which separates the different layers kernel, runtime, libraries, application framework and the application itself.

Layers build up onto each other and provide services to the layer above by using the functionality of the layers below. Different functionalities are optional and as the MDP is depending on the location information the GPS functionality should be provided by the system / architecture of the mobile device. In addition a necessary function is the possibility to exchange data with the MDP server by using an IP based connection.

Besides these infrastructure topics the access to the GUI, a local data store (e.g., data base) and the schedule of the device must be available to the MDP client application in order the use the information of future appointment to be able to plan ahead. This also demands that the events in the calendar can be stored with machine readable location information. In order to support this the "standard" calendar format, e.g., VCAL, could be extended to hold this information (Vcalendar, 1996; Schilke, 2006b)

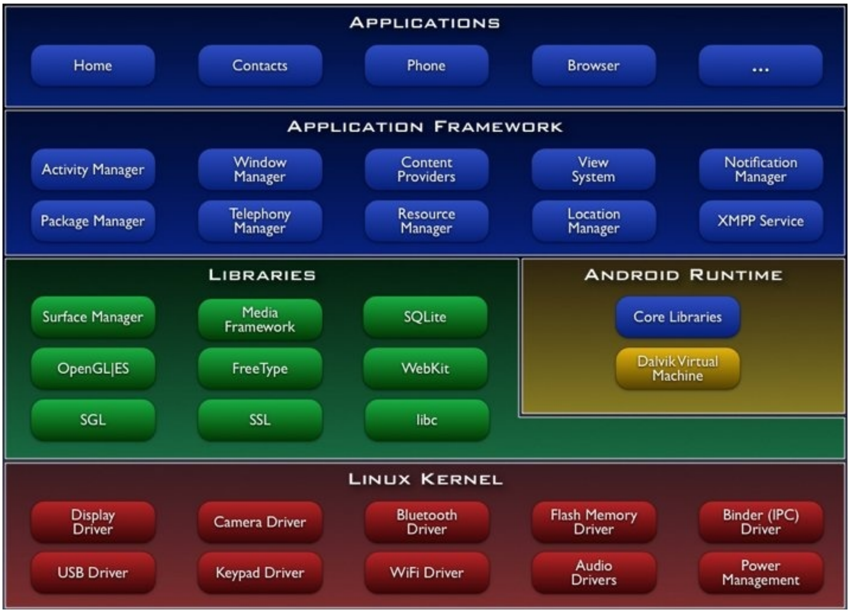

**Figure 1 Google Android Architecture (Google, 2008a)**

In order to provide the necessary functions for the implementation of a MDP client application such a system has to provide at least the following functions:

Access to a connection to the MDP / SPOT services via an IP-based connection (e.g., using GPRS, UMTS, WiFi / WLan, Bluetooth ...) using different protocols (e.g., HTTP ...).

Services to communicate with the user (e.g., messages, events, alerts, confirmations, profile updates, attachments ...).

A media to store information from / about the user (e.g., the interest profile, information from the MDP movement patterns during a time when no connection information could be sent ...).

The calendar of the user must be accessible to the application if the future appointments of the user shall be taken into account for recommendations (e.g., if there are events at the place of a scheduled business trip which match the user's interests).

Access to location information (e.g., GPS, AGPS, Triangulation, Cell ID ...) if this is not available from the mobile device the location of the mobile device (i.e., the user) has to be reported by the GSM / UMTS Service provider of the user (e.g., identified by the IMEI of the mobile device to the MDP / SPOT).

As the location component is very important one of the two ways described above are absolutely necessary in order to provide MDP services to a user. If it is not possible to provide location information to the MDP server the concept of MDP does not work in it's full as the location dimension is missing.

The mobile devices which are based on the mobile / smart phone operating systems mentioned above are prepared to support the use of a GPS device (e.g., Google, 2008a; LiMo; OpenMoko; Symbian). The use of such a device for the MDP prototype is mainly depending on the availability of the hardware device itself. The Google Android device looks promising but lacks the availability of the hardware. But there is a working emulator available which can also simulate movement patterns by a mock Location provider (Google, 2008b). The promising factor is that there are 30+ members in the consortium of the Open Handset Alliance (OHA, 2008) and the openness of the mobile device operating system.

Others have a less strong support in the market, the systems are fragmented (e.g., the LiMo and OpenMoko Linux derivates) or their hardware is in a very early stage with not so strong Location Based Services (LBS) support or weaker implementations of the emulators (including LBS support). The commercial systems like Windows Mobile, RIM or Symbian carry a high initial cost for a development and prototype environment. Even the commercial systems come in different flavours which makes it more difficult to select such a system for prototyping (e.g., Symbian).

## 3. MDP Communication

This section describes the communication between the mobile device of the user and the MDP Server.

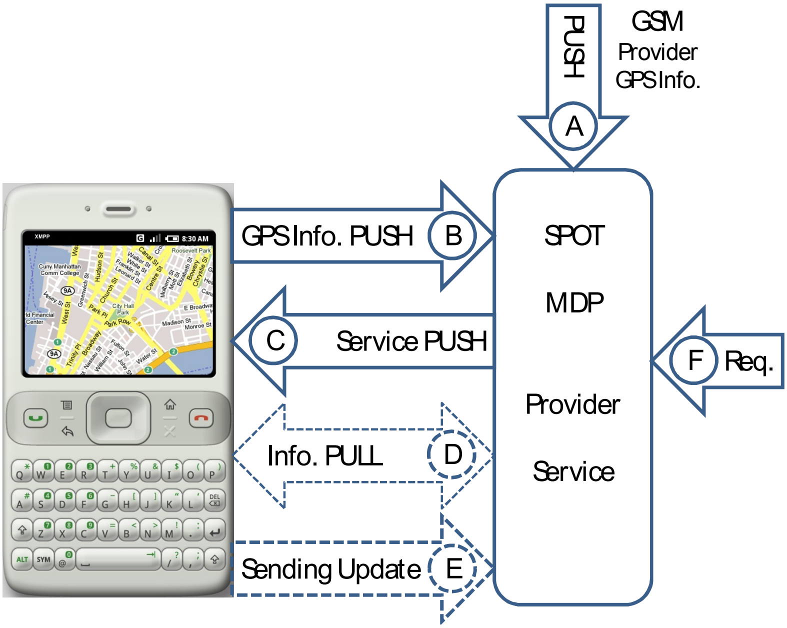

**Figure 2 Client to MDP / SPOT communication**

During this paper the letters in the circle refer always to the same step or process. It will be assumed that the mobile device of the user has at least an IP-based data connection to the MDP server.

In case of that the device is not equipped with a GPS component (or similar location information providing device) the GSM provider has to provide the location information for the MDP subscriber. In order to identify the user / mobile device a unique id has to be passed to the MDP service provider (e.g., the IMEI number of the device).

If the device is equipped with a GPS (or similar) the device has to send its location on a regular and configurable base. This will be used by the MDP service provider to track the user's movement pattern. If the device is not equipped with an GPS device at least a regular update on the IP address of the device has to be posted (e.g., every time the IP has changed) in order to enable the MDP service provider to reach the device. In the latter case the movement patterns / location information has to be provided by the mobile phone provider (see A). More on this will be explained later.

In order to notify the user of information or to update information on the client the server has to be able to push data to the mobile device. This supports the claim that users want to be provided with the information they want or need, without expecting from them to ask for it explicitly (Mulvenna *et al.* 2000; Hagen *et al.* 1999; Chavez *et al.* 1998). More on this will be explained later.

In case of the user wants to request information outside of his usual repertoire / profile the communication between mobile device and server has to support an information pull as well. In this scenario the user requests information and receives the information from the server if some matching information is available.

If the user decides to change information of the profile or switch the active profile the client has to support this by pushing the updated information to the MDP server. In case of the user can change his profile online on a MDP server this update would have t be pushed to the MDP client as well.

The information or service provider will be able to submit his information via the Chinese Wall to the users. This will be pushed to the users like described in C.

These are the basic communication paths necessary to run the MDP in a client server environment. As the mobile device are not so powerful it is necessary to deploy a protocol which does not need a lot of overhead and can transport different payloads. The messages which have to be exchanged are rather small. In case of that the mobile device is connected via a larger bandwidth the transmission of larger messages could be appropriate (e.g., events with images or videos). All this depends on the used mobile device, the available bandwidth and the settings of the user. Similar to the IMAP or RSS / ATOM protocols the user could choose in its profile to receive only the header / short information and will be able to download more (e.g., attachments) if he desires. The next figure describes the communication routes in scenarios based on the communication paths described above.

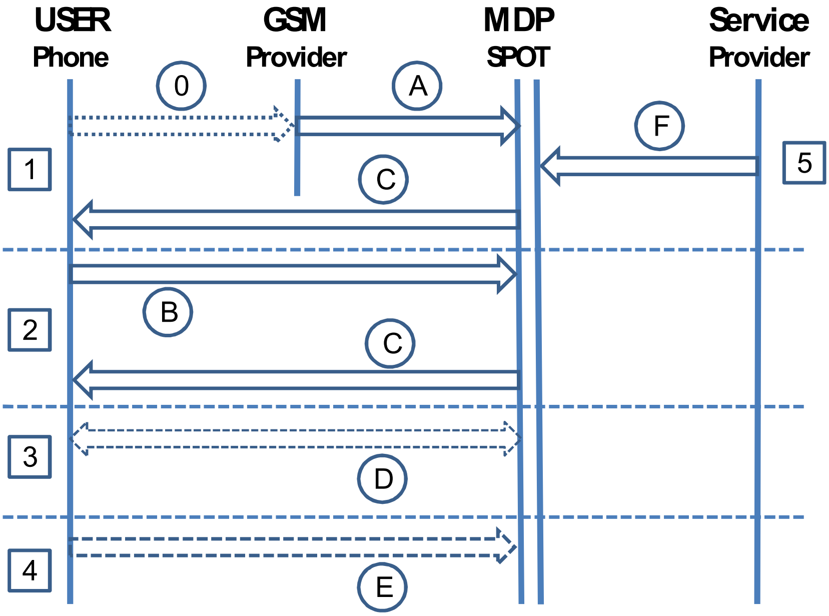

**Figure 3 Communication diagram MDP**

1) If the device cannot provide its own position (0) to the MDP service provider, the mobile phone provider has to pass this information to the

MDP service provider (A). This could be done by using, e.g., the cell id or triangulation between cells the mobile device is connected to. As soon as the MDP service gets this information it can start updating the users information pool on the mobile device (C).

2) In case of that the device is able to provide location information directly to the MDP service provider (B) a support by the mobile phone provider is not necessary. The MDP service will know about the whereabouts of the user / mobile device and can send information directly to the user / mobile device (C).
3) This scenario describes an active request of the user for information and the response of the server (D).
4) In this communication the client is directly sending information from the mobile device to the user, e.g., to update the profile or switch the active profile (E).
5) Information offered by a service provider (F) is passed via the SPOT to the MDP service provider which will be passing it on to the user (C) if the service provider is not on the "black list" of the user.

## 4. MDP Chinese Wall Architecture

The server architecture of the MDP server has to be able to fulfil different functions and must be able to accept and provide information close to real time. The server architecture has to be able to scale depending on the demand and the number of the users and information providers.

The server will receive position updates from every mobile device using the service either synchronous or asynchronous (if neither the device nor the GSM provider can provide this information). In addition the server or a separated application server component will receive requests from service providers for selecting anonymous user profiles or for sending information / service offers to users selected by their anonymous user profile (Schilke *et al.* 2005).

The MDP database will be guarded by the MDP service provider as he is the SPOT for the users. Losing the trust of the users by allowing, e.g., spam, to get through to the user will let the MDP / SPOT let lose users (Schilke *et al.* 2007). In order to enable the information / service providers to request that their services or information will be promoted to users of the service it is necessary that they can select their target audience by a request to the MDP / SPOT (F) (see next figure).

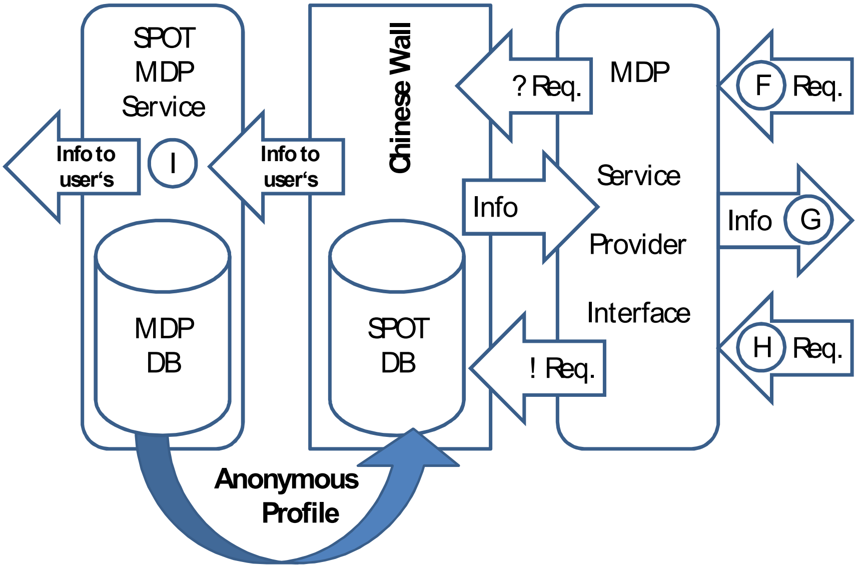

**Figure 4 Use of the Chinese Wall in the Server Communication**

The selection of the target audience based on the selection criteria will be done by the MDP / SPOT on a copy of the original database (Senicar *et al.* 2003). In this SPOT database the user data is anonymised so that only the movement patterns and the interest are available in this database. This represents the "Chinese Wall" which protects the real user data from external requests (Brewer & Nash, 1989; Lategan & Olivier, 2002; Sandhu, 1992; Cranor, 1999). The information / service provider will never get direct access to the SPOT data. The only information which will be returned is a figure which expresses how many hits in the defined target audience are available (G).

The next step (H) would be the dissemination of the message to the target audience. The SPOT / MDP would take the message with the earlier supplied hit list and would pass it on to the MDP service provider which would select the "real" users from the database and will distribute the data to the users (I). A check which would be performed before sending the information to the user is if the information / service provider is on the black list of the user. The number of delivered messages would be the number reported back in order to be able to bill the service (Schilke *et al.* 2006a).

To be trustworthy the SPOT must guard the users' data as well the data of the service providers. The users will know which service provider has sent them an offer or information, but the service provider will not know to whom its information was sent. If the receiving MDP user of the information accepts an offer from a service provider he shall not have to reveal his identity to participate (unless the service provider uses personalized vouchers, but even then he can only identify that this user fits a certain profile he used to send out his offer; he cannot identify this specific individual user). The SPOT will prevent that information will be passed on to users if there is only a small numbers of matching profiles to prevent a service provider from narrowing down his searches in order to identify certain users.

An additional aspect could be that users create their own information and provide this to the fellow MDP users on a kind of Web 2.0 like basis. In such a case the person adding the location depending information or recommendation will be differentiate from "normal" service provider information as they are user generated. This information will be stored by the MDP / SPOT provider and the same ranking or "self cleaning" mechanism will be applied through the other users.

## 5. MDP Client / Server Communication

In order to allow the mobile device (client) to communicate efficiently with the MDP server, a lightweight and efficient protocol is necessary. We have to distinguish between synchronous and asynchronous communication between the client and the server processes. In the case of the MDP scenario, information will be provided as a push service. Even in the occasion of the information request / pull from the user is pushed to the server and the resulting information will be pushed back to the user. The communication between the server and the mobile device is stateless each request is treated as an independent transaction that is unrelated to any previous request.

One important point in a mobile scenario has to be kept in mind: as a mobile connection via an IP connection is necessary to exchange data between the client and the server it could happen that the transmission of the data might be interrupted by a breakdown of the IP connection. In such a case the connection has to be re-established and the server has to check if the transmission is still appropriate, depending on the date and time when the information / event was scheduled to happen and the actual time and location of the user / mobile device.

A Web Services Architecture (Booth *et al.* 2004) is nowadays a common architecture for providing services in a loosely coupled computing environment. Another way to communicate between applications via HTTP is the Representational State Transfer (REST) (Fielding, 2000; Fielding & Taylor, 2002). By comparing both architectures they have their positive and negative sides (Pautasso, 2008). To summarize, the clear advantage of REST is that is a lightweight protocol that allows the transfer of simple and even more complex data via an easy transport media, i.e., calling URIs via HTTP. This kind of architecture is also called Resource Oriented Architecture (ROA; Richardson & Ruby, 2007). The ROA is based on resources, their names (URIs), their representation and the links between them (Richardson & Ruby, 2007).

As HTTP is a rather lightweight and stateless protocol this method would be suited to fit the requirements for an implementation of a MDP / SPOT prototype based on a ROA. The stateless HTTP-based REST protocol can cope with a temporarily disconnection of the IP data connection to the MDP server. This is one of properties of a ROA. The other properties are addressability, connectedness and a uniform interface (Richardson & Ruby, 2007).

In addition it is possible to easily scale such an application by commonly available equipment like load balancers and servers to meet the increased demand.

Instead of dealing with client side Web Services libraries the application on the MDP client, i.e., the mobile device must provide a tiny web server which could accept the REST communication from the server to the client. The MDP client application would react on these rest calls depending on the payload included (e.g., new events, notifications, updates ...). The easier part in this architecture is to implement the server side, as it is rather state of the art to implement a REST-based server application using a HTTP server or JEE application server.

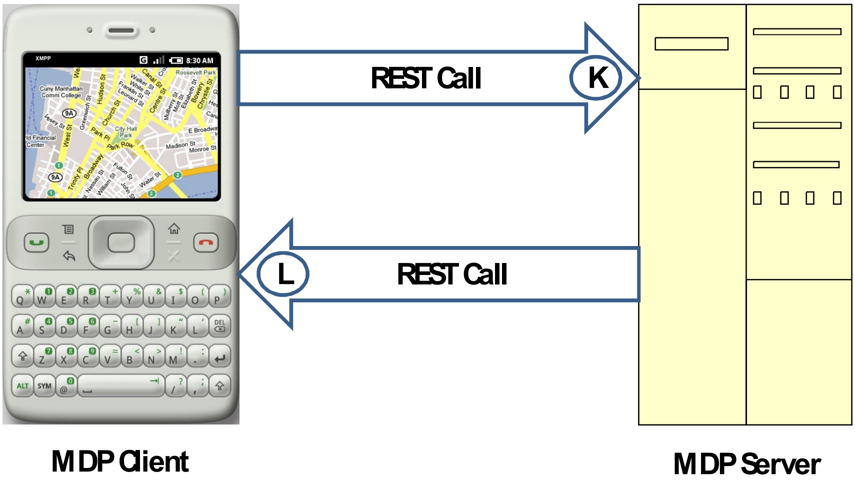

**Figure 5 MDP REST Communication**

The REST calls from the MDP client (K) would cover the communication described as B, D and E. The REST calls from the MDP server to the MDP client (L) would cover the communication paths C (and I respectively the “answer” to D).

By encapsulation all communication between client and server with the REST calls both communication paradigms of synchronous and asynchronous communication can be implemented and depend only on the implementation of application.

## 6. Further Outlook & Discussion

The proposed architecture for the implementation of the MDP / SPOT prototype will be based on standard technologies like REST, Java, Google Android (Emulator and mobile device), Google Maps and other freely available technologies. The technology and architecture of the proposed prototype seems to be capable to scale to a real world application scenario by using technologies like server clusters and load balancers to cope with a larger number of users.

The implementation of the prototype based on this proposed architecture will deliver valuable insights if the ROA architecture can deliver what is promising. As soon as the Android device becomes available in October the tests can be done in the real world scenario by moving from the emulator to a mobile device and talking with the prototype MDP server.

The Chinese Wall component depends on database technologies which will allow a "near time" push of the changes of the MDP data in anonymised form to the SPOT data base. By implementing a prototype Chinese Wall the handling of the selection process based on anonymised profiles can be evaluated as well as the creation of user based recommendation from MDP users for MDP users. In addition security concerns can be evaluated and further discussed.

The results of the evaluation of the prototype will be evaluated in order to adjust the architecture of the MDP / SPOT if necessary and to correct any design flaws identified.

## 7. References

Abowd, G.D. and Mynatt, E.D. (2000) "Charting Past, Present, and Future Research in Ubiquitous Computing", *ACM Transactions on Computer-Human Interaction* 7(1): 29-58

Askwith, B., Merabti, M. and Shi, Q., (2000) "MNPA: a mobile network privacy architecture", *Computer Communications* 23, 1777-1788, Elsevier

Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., Ferris, C. and Orchard, D. (2004), "*Web Services Architecture*" at http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/, last accessed 2.08.2008

Brewer, D.F. and Nash, M.J (1989) "The chinese wall security policy" *Proceedings of the IEEE Symposium on Security and Privacy* (Oakland, Calif., May 1-3). IEEE Computer Society Press, Los Alamitos, Calif., 206-214.

Business Week, Website "*Mobile-Phone Showdown*" at http://images.businessweek.com/ss/08/06/0625_mobile_showdown/index.htm, last accessed 01/08/2008

Chavez, E., Ide, R. and Kirste, T. (1998) "SAMoA: An experimental platform for Situation-Aware Mobile Assistance" *Proceedings of Workshop on Interactive Applications of Mobile Computing*

Cranor, L.F. (1999) "Internet privacy" *Communications of the ACM*, 42(2):29-31, Feb. 1999

Fielding, R.T. and Taylor, R. N., (2002), "Principled Design of the Modern Web Architecture" (PDF), *ACM Transactions on Internet Technology* (TOIT) (New York: Association for Computing Machinery) 2(2): 115–150, doi:10.1145/514183.514185, ISSN 1533-5399, PDF from http://www.ics.uci.edu/~taylor/documents/2002-REST-TOIT.pdf, last accessed 01/08/2008

Fielding, R.T. (2000), "*Architectural Styles and the Design of Network-based Software Architectures*", University of California, Irvine, PDF from http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm, last accessed 02/08/2008

Google (2008a) Website "*What is Android?*" at http://code.google.com/android/what-is-android.html, last accessed 01/08/2008

Google, (2008b) Website "*Location-based Service APIs*" at http://code.google.com/android/toolbox/apis/lbs.html, last accessed 02/08/2008

Hagen, P.R., Manning, H. and Souza, R., (1999) "*The Forrester Report. July 1999. Smart Personalization*", Forrester, Cambridge, MA, USA: Forrester Research, Inc., p. 8

Kobsa, A (2002) "Personalized hypermedia and international privacy" *Communications of the ACM*, Volume 45, Issue 5 (May 2002), SPECIAL ISSUE: The adaptive web, Pages: 64-67 in there is the German Teleservices Data Protection Act (from 1997) referenced at http://www.datenschutz-berlin.de/recht/de/rv/tk_med/iukdg_en.htm#a2

José, R. and Davies, N., (1999) "Scalable and Flexible Location-Based Services for Ubiquitous Information Access" *Proceedings of First International Symposium on Handheld and Ubiquitous Computing*, HUC'99

Lategan,F.A. and Olivier,M.S., (2002) "A Chinese Wall approach to privacy policies for the web" *26th Annual International Computer Software and Applications Conference (COMPSAC 2002)*, Oxford, UK, 940-944, IEEE

LiMo, Website "*What is the Platform*" at http://www.limofoundation.org/en/what-is-the-platform.html, last accessed 01/08/2008

Mulvenna, M.D., Anand, S.S. and Buchner, A.G. (2000) "Personalization on the Net using Web Mining" *Communications of the ACM*, August 2000/Vol. 43, No. 8, pp. 123-125

Mobasher, B., Berendt, B. and Spiliopoulou, M. (2001) "KDD for Personalization" *5th European Conference on Principles and Practice of Knowledge Discovery in Databases* September 6,2001

OHA, Website of the Open Handset Alliance Members Section, at http://www.openhandsetalliance.com/oha_members.html last accessed 1.08.2008

OpenMoko, Website "*OpenMoko Developer Guide*" at http://wiki.openmoko.org/wiki/Openmoko_developer_guide, last accessed 01/08/2008

Pautasso, C., Zimmermann, O. and Leymann, F. (2008), "RESTful Web Services vs. Big Web Services: Making the Right Architectural Decision" (HTML), *17th International World Wide Web Conference (WWW2008)* (Beijing, China) – PDF accessed at http://www.jopera.org/docs/publications/2008/restws at the 02/08/2008

Richardson, L. and Ruby, S. (2007), *RESTful Web Services*, O'Reilly Media, Inc.

Sandhu, R.S. (1992) "Lattice-Based Enforcement of Chinese Walls" *Computers & Security*, Volume 11, Number 8, December 1992, pages 753-763

Schilke S.W. (2003) "Personalisierung - das vergessene Thema?", *bdvb aktuell 83*, Mitglieder-Magazin des Bundesverbandes Deutscher ISSN 1611-678X, p18, 2003

Schilke S.W., Bleimann U., Furnell, S.M. and Phippen, A.D. (2004), "Multi-Dimensional-Personalisation for the online and offline world", *Proceedings of the Fourth International Network Conference (INC 2004)*, Plymouth, UK, 6-9 July 2004, pp545-552

Schilke, S.W., Bleimann, U., Furnell, S.M. and Phippen, A.D. (2005), "A Chinese Wall Approach for Anonymous Recommendation in a Multi-Dimensional-Personalisation Scenario", *Proceedings of Sciences Electroniques, Technologies de l'Information et des*

*Telecommunications (SETIT) 2005*, 27-31 March 2005, p155 (abstract), ISBN: 9973-51-546-3; Full Paper on CD

Schilke, S.W., Furnell, S.M., Bleimann, U. and Phippen, A.D. (2006a), "Enhancing Privacy Through Anonymous Recommendation for Multi-Dimensional-Personalisation", *Proceedings of the 5th Security Conference*, April 19-20, Las Vegas, USA, ISBN: 0-9772107-2-3

Schilke, S.W., Bleimann, U., Stengel, I. and Phippen, A.D. (2006b) "Fitting Extended Blended Learning and Multi-Dimensional-Personalization into Learning Management Systems" *Proceedings of the Sixth International Network Conference (INC2006)*, Plymouth, UK, 11-14 July, pp393-400

Schilke S.W., Bleimann U., Furnell S.M. and Phippen A.D. (2007), "Multi-dimensional-personalisation - in "whom" we trust? Perception of trust & privacy", *Proceedings of the Third Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2007)*, Plymouth, UK, ISBN: 978-1-8410-2173-7, pp11-22

Senicar, V., Jerman-Blažič, B. and Klobučar, T., (2003) "Privacy-Enhancing Technologies—approaches and development" *Computer Standards & Interfaces* 25, p. 147–158, Elsevier

Symbian, Website "*Symbian Developer Network – System Documentation*" (SVG Images) at http://developer.symbian.com/main/documentation/technologies/system_models/index.jsp , last accessed 1.08.2008

VCalendar (1996) "*The Electronic Calendaring and Scheduling Exchange Format*", Version 1.0, versit Consortium Specification, Internet Mail Consortium, September 18, 1996 http://www.imc.org/pdi/