Chapter 19
Open Personal Identity as a Service

Miroslav Behan and Ondrej Krejcar

Abstract. The mobile technologies establish communication environment where mash able solutions are more than convenient. Open personal identity is independent service which is gathering available identity resources and provides unified person identities. The service enables to resolve current mobile device problematic around multiplicities, backup or change management of person identification where multiple devices replication is an option.

19.1 Introduction

Do you remember the situation when you have changed your phone number and you had to tell this change to all of your friends, relatives even workmates? That time is over with the Open Person Identity as a Service. Imagine worldwide Internet service which provides on-line personal information such as mobile numbers, current living address or current friend's cross different social media. There are many advantages of usage of such a kind of service. We would like to introduce some of them in more details.

The modern knowledge society produces much more information than we are able to consume and therefore the utilization or clarity of information is more than convenient. Only those kinds of services which are not complicated or confusing would be accepted by many and the strength of intuitive factors for applications or services behavior will increase in time. That's why social media have such power of influence because they are gathering information from many sources in easy and comprehensive personal way. The problem is when you have more social media then the amount of time spent by scanning or posting into the different sources would not be efficient. The case is about to find an open solution which consolidates all media in one place and basically provide personal social connector as a convenient user-friendly solution with an easy and comprehensive user interface.

Miroslav Behan · Ondrej Krejcar
University of Hradec Kralove, FIM, Department of Information Technologies
Rokitanskeho 62, Hradec Kralove, 500 03, Czech Republic
e-mail: miroslav.behan@uhk.cz, ondrej.krejcar@asjournal.eu

A. Zgrzywa et al. (Eds.): Multimedia and Internet Systems: Theory and Practice, AISC 183, pp. 199–207.
springerlink.com

19.2 Problem Definitions

The amount of social media networks, multiplicity of personal identity[2] and the inconvenient way of handling the important personal information lead us to think that there some better ways how to make our lives a little bit easier. That's why we start to think about the problem in terms of usability in current available on-line social technologies [8, 9].

We started to ask how to solve our daily life common problems and we summarized them in following questions. What if we have more than one mobile device but each one of them has a different content? Or if we have just one mobile device but we lost it? Could we exchange mobile device platforms without any inconveniences? Do we have to notify everyone when we change our mobile number or even when we do not use it anymore as an identity? When we answered positively to some of those questions, we considered us in correct problem definition [10, 11].

That was just a brief overview of a complex task to solve. In this article we are focusing on personal identity service which is used for virtual personal identification and enables communication between people over modern technologies; nevertheless we consider that kind of service as open and as an independent concept where commercial influences are minimized. At first we describe communication process between two or more sides where communication could be established if there is an existing compatible informational data flow exchange between mobile device clients. To start process at first we need to know the identity of persons with whom we would like to communicate. The identification of personal identity consists of our tacit knowledge where the identity is located in available informational resources and how is the identity knowledge externalized by visualization in comprehensive form. After correct identification of required person the communication process can start.

As current personal identification mainly used in mobile devices we assume a phone contact list where identities are expressed by names, personal pictures or associated phone numbers. That kind of establishment was made by mobile providers over the world. Another personal identity used in mobile device communication that we recognize are the instant messaging systems where identities are commonly defined by user name coded by sequence of characters. We consider these types of identification as obsolete and we propose a new concept in chapter New Design.

Also we define the environment as an on-line with unlimited access to the Internet according to the fact that the increasing mobile device on-line connectivity is arising. We announce the off-line mode of Internet connectivity as temporary state which is identified by status of not connected client and which would be changed by user interaction or predefined settings device behavior to on-line mode and proceeds in delayed tasks. We considered on-line Internet access to mobile device in terms of synchronization of contact list with the Open Person Identity Service (OPIS) over message based client-server where changes are only made by authorized identity owner. In those terms of change management we defined following concept of Front-End and Back-End where:

Front-End – all clients which are accessing over Internet to service by message based communication and perform user's actions corresponding to correct content within associated devices and also can perform data merge operation with current device content.
Back-End – the server provides service based on client-server type of connection and background resource processing which interacts with social media as automated direct resource connector.

Next chapter highlighted the solution concept (see figure 19.1) which can solve our defined problematic by changing establishment and by exploiting today's technologically innovated environment surrounding us with increasing mobile Internet connectivity.

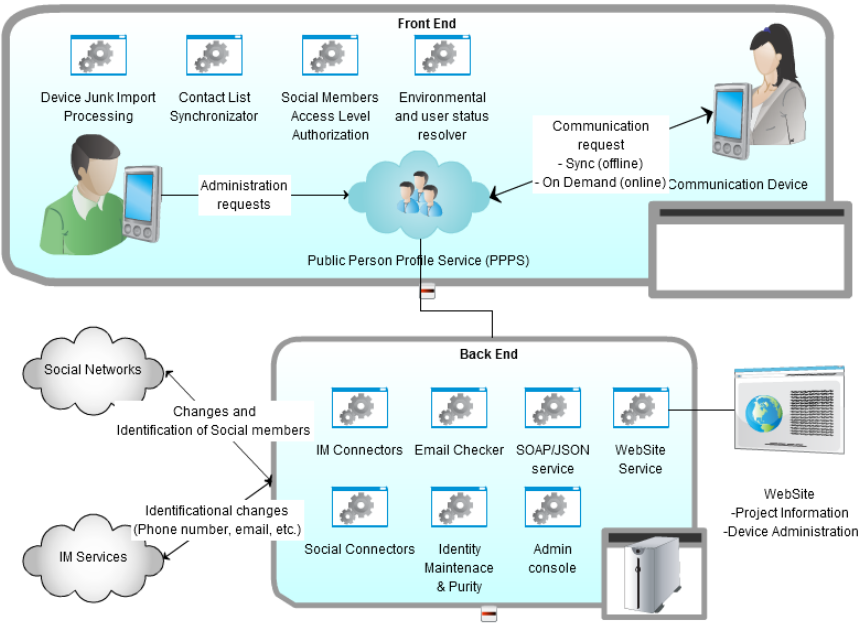

Fig. 19.1 Scenario of Open Personal Identity as Service

19.3 Related Works

Today's personal identities are stored mostly in mobile device as a contact list saved on a local storage. Synchronization with other devices or with desktop applications is normally made over USB or Bluetooth which is connected directly to personal computer. For instance we just highlight some of software solutions: Apple iTunes, Nokia PC suite, Microsoft Phone Data Manager. These mentioned software solutions have some disadvantages. The installation requires dedicated computer where are all data and management placed. Supported mobile devices

are basically only with corresponding platform or manufacturer in terms of single content management or in case of mobile device lost or exchange.

Those disadvantages of current local data management software of mobile devices led us to propose remote data management solution so a part in this article is covering a solution for personal identities service based on a contact list embedded in mobile devices, which could be manageable from device itself or from web interface from Internet [4, 5].

The reason why we considered such solution is a usability of mobile devices due to its limitations in editing the contact where small screen and lower level maturity of a user's input interface is provided in comparison with common desktop. The other reason is a possibility of data replication to other different types of mobile devices. In short it is to create an independent platform for mobile phone users who have more than one device. It is also useful for an easy recovery of a contact list data in case the device is lost or broken.

The new solution considers security issues and authorization of publishable personal information. The main reasons why such a service may be not acceptable from user's point of view are data privacy issues where users will not like to share data of their contacts. That issue we solve in terms of use and encryption system policy where no one could decrypt personal data without a password.

We announce well-known OpenID service as different type of web service [6, 7] which basically provides uniform access to multiple web sites or application which implements OpenID access as a 3rd side authentication process. The principals are different in basic scenarios where for example in case of OpenID the user visits a web application and is able to log in without registration or native login process but instead of that the user will be only authorized by OpenID with the same credentials when service is implemented and provided. The principals about OPIS are described as following use case scenario. The user have only one place for real identity attributes and these information are in case of change automatically redistributed to connected systems or they are provided as a service like on-line requests by gathered data from social connectors where last update event of specific identity detail is provided.

19.4 Solution Design

As was mentioned in chapter above the developed solution is based on front-end and back-end architecture where as a front-end we assume only devices which are opened to software maintenance and which are configurable such as smart phones, tablets, and computers or even for instance the cars with embedded customizable control unit [3, 11]. The front-end in our perspective is basically any customized client with Internet connection ability, device with contact list accessibility and with background processing possibility. As an extension of front-end in term of user device application also user interface whereas the output we consider graphical (GUI) or voice interface (VUI) and as the input a touch, keyboard or voice recognition user interface [12, 13]. Next part, the back-end could be any server

technology which is able to store data of identities and their associations with clients, which have Internet connectivity and providing services on specified ports and also which are able to maintain informational flow between external resource providers such as social networks or instant messaging services and internal web-site accessibility for remote device administration [14, 15]. That was in short the concept of described solution where we are focusing on types of user actions on client side and then on server side on back-end processing.

For more precise description of front-end we would define common end-user's actions and divide them into two parts as an interoperability types of actions which come first and as an administrative action types which come after. The task that would not necessary starts at first time after client installation is the import of personal identities processing where available resource is embedded in a device contact list, in usage of instant messaging systems or in social networks. All that kind of application would be recognized at first time or upon user's additional task completion. Therefore user's actions are about to import existing contact list, add social media connector or add instant messaging provider. As a complementary user's actions to each of designed entities would be to create, read, update and delete (CRUD) actions from administration point of view. During the process of an identity import is mandatory a user's support where actions as human recognition are required, because data mash or the other identity conflicts are machine irresolvable. Next actions covered administrative part of application where client behavior settings ability options are shaped by Internet connectivity which could became as off-line or on-line device mode. The off-line mode recognizes active connections to Internet and automatically synchronizes changes with back-end instance. If the device does not support background listener of network status change than the responsibility of connectivity is up to user over corresponding passive sync actions. While the active on-line mode requires requests to be served just in time and therefore personal identities would be provided any time up to date when they are required by user or by another application. Also in this case devices without support of background processing are using contact list as an provider of identities and accessibility for other application have to use embedded contact list as informational resource which is replicated upon user actions. Also there is possibility to use designed communication client where identities are automatically remotely resynchronized. Another administrative action is definition of access level permissions for each specific identity where user could globally setup public, protect or hide permission for concrete identity or in more sophisticated customization could specify permissions based on member groups.

The back-end part actions are mainly focused on background processing of connected clients or connected external identities providers. For better comprehensive overview we highlighted the entity diagram in next figure 19.2 where are required kinds of information gathered into the database. Data are consolidated within user's point of view and saved only with partial information based on social networks providers.

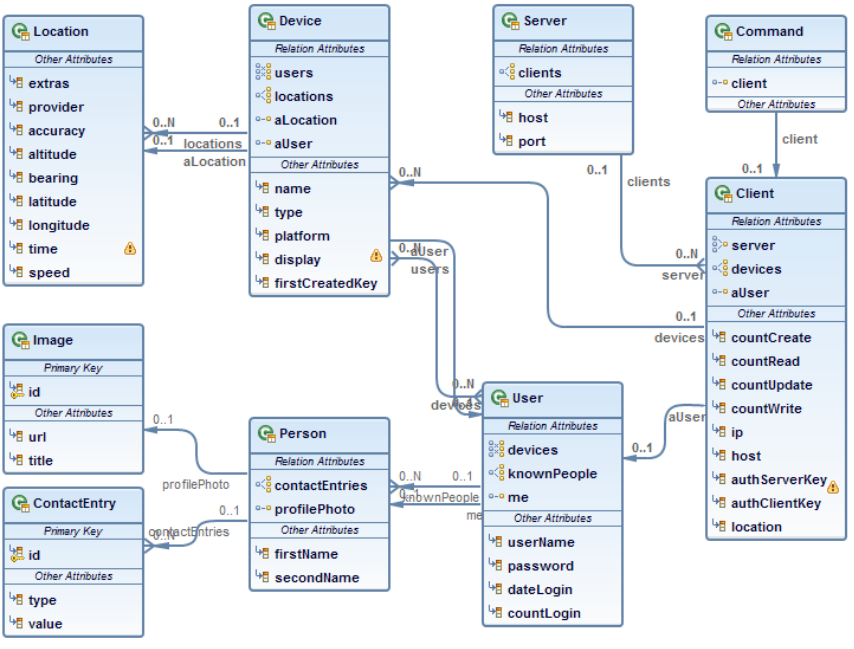

Fig. 19.2 JPA Entity diagram

The social networks and instant messengers are converging subset of external identity providers. Not all are enabling open informational exchange for independent clients. One of open exchange protocol is called Extensible Messaging and Presence Protocol (XMPP). Standardized on port 5222 and messages are exchanged over Extensive Mark-up Language (XML). We considered standard above as convenient and it will be used for interaction in further development on interface [16] with most of instant messenger providers. For social networks providers are common criteria with third side authorization process of external application which was mainly developed and enhanced by Facebook due to external social content providers who have to have only limited access to social media private data [17]. The same principles are used in G+ for accessing personal identity details.

19.5 Implementation

During the project realization we were challenging the suitability of used technologies. As the most portable solution we decided to use Java object language and supportive development framework Eclipse due to Java virtual machine (JVM) technology where clients could be implemented in any kind of device which supports embedded Java even for instance in car's radios which are able to be connected instantly to Internet [18, 19]. The prototype of testing server which

provides open personal identities as a service is developed as socket Java server and running as a background process within Linux distribution (Cent OS) on virtual private server (VPS) [20]. The testing client prototype is based on Android platform because of a rapid application development (RAD) where Java is also included as a platform development language. The communication between server and client is based on message driven protocol. The messages are transferred by Java objects serialization. As server storage we used ObjectDB database engine caused by its performance results [1]. We consider that engine as the fastest in terms of usage Java Persistence API(JPA), where the Java object are annotated as database entities and therefore the transformation of any type of data between persistent Java objects in memory and physical data objects in database back and forth is automated. Currently implemented part of a concept is user interface as Android native application with touch ability. We of course plane web interface for remote management with possible device management extension therefore in the following figure 19.3 is screen of Android client application version 1 which is enabling a merge of different source of personal identities and replicates knowledge to the server.

In a certain time of period background processes are refreshing data from external resources which are announced with public accessibility. Validity for instance of email is checked with background process email checker only on untrusted inputted data.

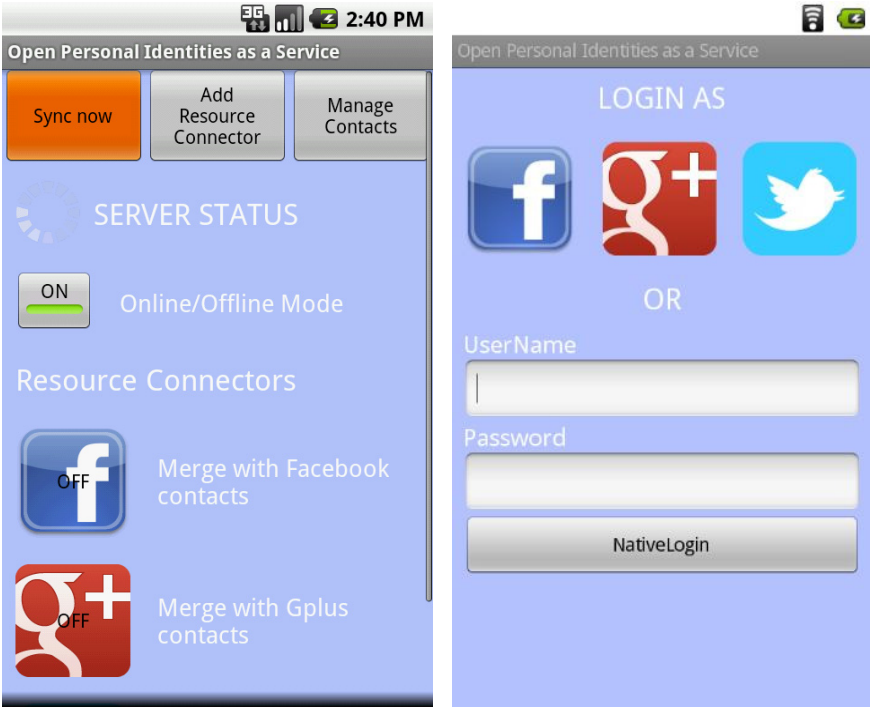

Fig. 19.3 Screens of Android client application

19.6 Conclusions

The Open Personal Identity Service solution is one part of larger scale project which covers Remote Mobile Device Management area. We consider positive influence of application usage on daily bases tasks where personal productivity increased by penetration over connected social networks. The change of any kind personal information supposed to be automatically redistributed over the connected systems. The application increase usability of maintaining social and personal identities characteristics. The open access service increase global knowledge of personal identities and positively influence human adaptability in cyber space. The real benefits of service would be recognized in further discovery with real user's behavior. The result at first step is working prototype which provides remote service of personal contact list management for mobile device users. With an increasing amount of application users the certain of personal impacts will be more obvious.

Acknowledgment. The work and the contribution were partially supported by the project (1) ESF funded project "INDOP – Innovation and Support of the Doctoral Study Program", identification number CZ.1.07/2.2.00/28.0327; (2) "SMEW – Smart Environments at Workplaces", the Grant Agency of the Czech Republic, GACR P403/10/1310; (3) specific research project "Smart Solutions in Ambient Intelligent Environments", University of Hradec Kralove under the project SP/2012/6.

References

1. JPA Performance Benchmark (JPAB), ObjectDB software Ltd. (2012), http://www.jpab.org
2. Ward, D.: Personal Identity, Agency and the Multiplicity Thesis. Minds and Machines 21(4), 497–515 (2011)
3. Mikulecky, P.: Remarks on Ubiquitous Intelligent Supportive Spaces. In: 15th American Conference on Applied Mathematics/International Conference on Computational and Information Science, pp. 523–528. Univ. Houston, Houston (2009)
4. Korpas, D., Halek, J.: Pulse wave variability within two short-term measurements. Biomedical papers of the Medical Faculty of the University Palacky, Olomouc, Czechoslovakia 150(2), 339–344 (2006) ISSN: 12138118
5. Kasik, V., Penhaker, M., Novák, V., Bridzik, R., Krawiec, J.: User Interactive Biomedical Data Web Services Application. In: Yonazi, J.J., Sedoyeka, E., Ariwa, E., El-Qawasmeh, E. (eds.) ICeND 2011. CCIS, vol. 171, pp. 223–237. Springer, Heidelberg (2011), doi:10.1007/978-3-642-22729-5_19
6. Vybiral, D., Augustynek, M., Penhaker, M.: Devices for Position Detection. Journal of Vibroengineering 13(3), 531–535 (2011)
7. Penhaker, M., Cerny, M., Martinak, L., Spisak, J., Valkova, A.: HomeCare - Smart embedded biotelemetry system. In: World Congress on Medical Physics and Biomedical Engineering, Seoul, South Korea, August 27-September 01, vol. 14, pt. 1-6, pp. 711–714 (2006)

8. Brida, P., Machaj, J., Benikovsky, J., Duha, J.: An Experimental Evaluation of AGA Algorithm for RSS Positioning in GSM Networks. Elektronika ir Elektrotechnika 8(104), 113–118 (2010) ISSN: 1392-1215
9. Chilamkurti, N., Zeadally, S., Jamalipour, S., Das, S.K.: Enabling Wireless Technologies for Green Pervasive Computing. EURASIP Journal on Wireless Communications and Networking 2009, Article ID 230912, 2 pages (2009)
10. Chilamkurti, N., Zeadally, S., Mentiplay, F.: Green Networking for Major Components of Information Communication Technology Systems. EURASIP Journal on Wireless Communications and Networking 2009, Article ID 656785, 7 pages (2009)
11. Liou, C.-Y., Cheng, W.-C.: Manifold Construction by Local Neighborhood Preservation. In: Ishikawa, M., Doya, K., Miyamoto, H., Yamakawa, T. (eds.) ICONIP 2007, Part II. LNCS, vol. 4985, pp. 683–692. Springer, Heidelberg (2008)
12. Juszczyszyn, K., Nguyen, N.T., Kolaczek, G., Grzech, A., Pieczynska, A., Katarzyniak, R.: Agent-based approach for distributed intrusion detection system design. In: Alexandrov, V.N., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2006. LNCS, vol. 3993, pp. 224–231. Springer, Heidelberg (2006)
13. Machacek, Z., Srovnal, V.: Automated system for data measuring and analyses from embedded systems. In: 7th WSEAS International Conference on Automatic Control, Modeling and Simulation, Prague, Czech Republic, March 13-15, pp. 43–48 (2005)
14. Bodnarova, A., Fidler, T., Gavalec, M.: Flow control in data communication networks using max-plus approach. In: 28th International Conference on Mathematical Methods in Economics, pp. 61–66 (2010)
15. Bures, V.: Conceptual Perspective of Knowledge Management. E & M Ekonomie a Management 12(2), 84–96 (2009)
16. Brad, R.: Satellite Image Enhancement by Controlled Statistical Differentiation. In: Innovations and Advances Techniques in systems, Computing Sciences and Software Engineering, International Conference on Systems, Electr. Network, December 03-12, pp. 32–36 (2007)
17. Tucnik, P.: Optimization of Automated Trading System's Interaction with Market Environment. In: Forbrig, P., Günther, H. (eds.) BIR 2010. LNBIP, vol. 64, pp. 55–61. Springer, Heidelberg (2010)
18. Thompson, T.: The Android mobile phone platform - Google's play to change the face of mobile phones. Dr. Dobbs Journal 33(9), 40-+ (2008)
19. Shih, G., Lakhani, P., Nagy, P.: Is Android or iPhone the Platform for Innovation in Imaging Informatics. Journal of Digital Imaging 23(1), 2–7 (2010), doi:10.1007/s10278-009-9242-4
20. Hii, P., Chung, W.Y.: A Comprehensive Ubiquitous Healthcare Solution on an Android (TM) Mobile Device. Sensors 11(7), 6799–6815 (2011), doi:10.3390/s110706799