Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 672196, 6 pages
doi:10.1155/2012/672196

Research Article

Open Personal Identity as a Service

Miroslav Behan

Department of Information Technologies, Faculty of Informatics and Management, University of Hradec Kralove, Rokitanskeho 62, 50003 Hradec Kralove, Czech Republic

Correspondence should be addressed to Miroslav Behan, mirek.behan@gmail.com

Received 22 June 2012; Revised 4 December 2012; Accepted 5 December 2012

Academic Editor: Stavros Kotsopoulos

The mobile computing established communication environment where personal identification is a key factor which influence usability of mobile application. Open personal identity is a partial service which enables crowd resource identifications processing in online distributive unified form over secured communication channel. The service provides current fresh personal identificators which are essential in communication process.

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, and even workmates? That time is over with the Open Person Identity as a Service. Imagine worldwide Internet service which provides online 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 behaviour will increase in time. That is 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 than the amount of time to spend on scanning or posting personal information into the different sources is not efficient. The case is about to find an open solution which consolidates all media in one place and basically provides personal social connector as a convenient user-friendly solution with an easy and comprehensive user interface.

2. Problem Definition

The amount of social media networks, multiplicity of personal identity [1], and the inconvenient way of handling the important personal information leads us to think that there are some better ways of 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 online social technologies [2, 3].

We started to ask how to solve our daily life common problems and we summarized them in the 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 [4, 5].

That was just a brief overview of a complex task to solve. In this paper 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 the process at first we need to know the identity of the 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 a 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 online with unlimited access to the Internet according to the fact that the increasing mobile device online connectivity is arising. We announce the offline 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 behaviour to online mode and proceeds in delayed tasks. We considered online 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 the Front-End and Back-End.

Front-End. All clients which are accessing over the Internet to service by message-based communication and perform user's actions corresponding to the correct content within associated devices and also can perform data merge operation with current device content (Figure 1).

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 (Figure 2).

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

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 a personal computer. For instance we just highlight some of software solutions: Apple iTunes, Nokia PC suite,

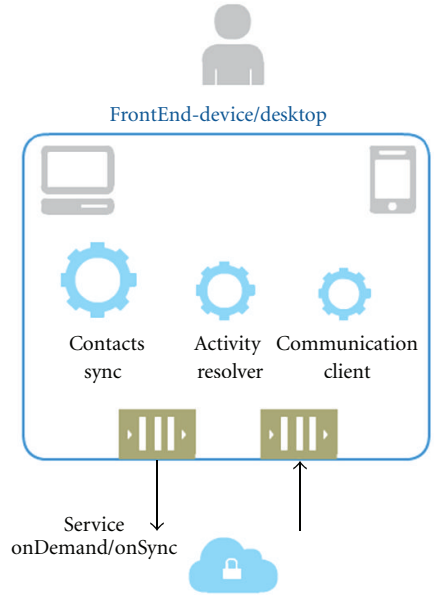

Figure 1: Service design: client.

and Microsoft Phone Data Manager. These mentioned software solutions have some disadvantages. The installation requires dedicated computer where all data are placed and managed. 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 one part in this paper 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 [6, 7].

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 maturity level 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 their contacts. We solve this issue 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 [8, 9] which basically provides uniform access to multiple web sites or application which implements OpenID access as a third 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

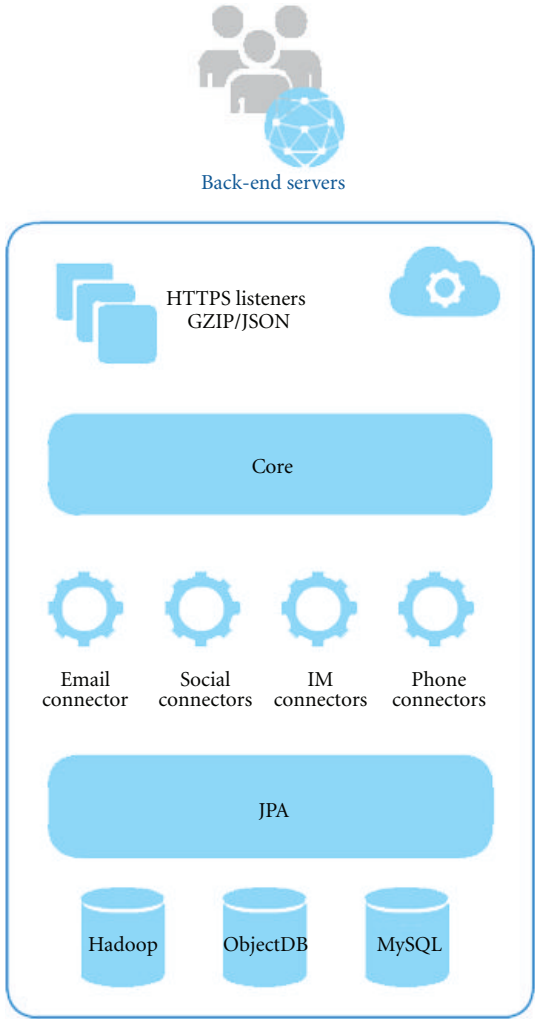

Figure 2: Service design: client.

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 has 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 online requests by gathered data from social connectors where last update event of specific identity detail is provided.

4. Solution Design

As was mentioned in chapter above the developed solution is based on the 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 [5, 10]. 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 the 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 [11, 12]. Next part, the back-end could be any server technology which is able to store data of identities and their associations with clients, which has Internet connectivity and provides services on specified ports and also which is able to maintain informational flow between external resource providers such as social networks or instant messaging services and internal website accessibility for remote device administration [13, 14]. That was in short described the concept solution where we are focusing on types of user actions on the client side and then on the server side on back-end processing (Figure 2).

For more precise description of the 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 start 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 behaviour settings ability options are shaped by the Internet connectivity which could become as offline or online device mode.

The offline 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 then the responsibility of connectivity is up to user over corresponding passive sync actions. While the active online 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 a provider of identities and accessibility for other application have to use embedded contact list as an informational resource which is replicated upon user actions. Also there is a 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 set up 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

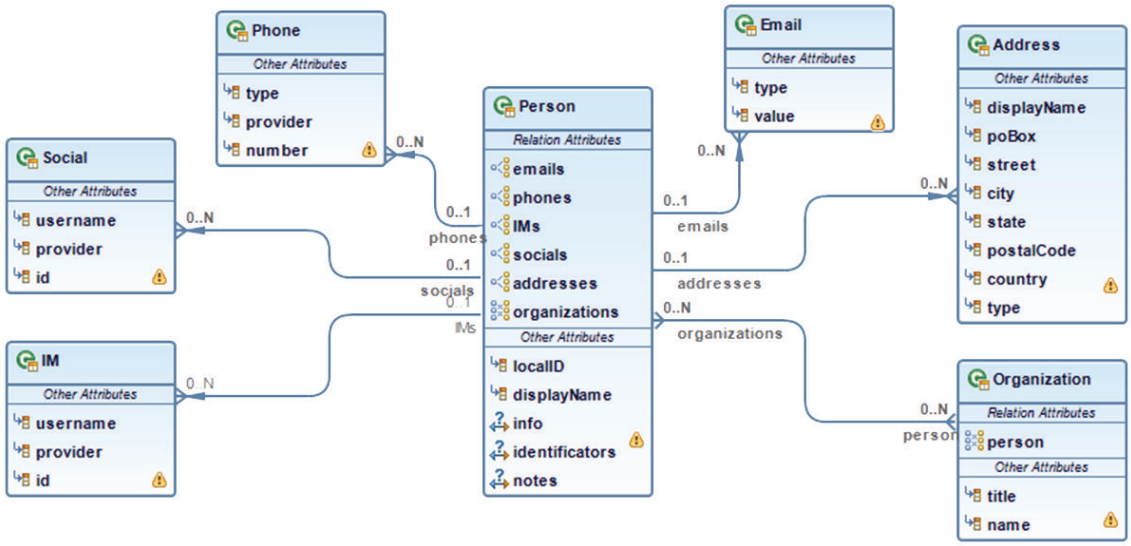

Figure 3: JPA Entity diagram.

identities providers. The Figure 3 above presents the entity diagram where are highlighted required information and their relations which are valued for gathering into the database. Data are consolidated within user's point of view and saved only with partial information based on social networks providers.

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 the open exchange protocol is called the Extensible Messaging and the Presence Protocol (XMPP). Standardized on port 5222 and messages are exchanged over the Extensive Mark-up Language (XML). We considered the standard above as convenient and it will be used for interaction in further development on interface [15] with most of instant messenger providers. In case of social network providers the common authorization process with external applications is based on third sidy party access, which was mainly developed and enhanced by Facebook due to the external social content of providers who have to have only limited access to the social media private data [16]. The same principles are used in G+ for accessing personal identity details.

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 the Internet [17, 18]. 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) [19]. 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 [20]. We consider the engine as the fastest in terms of usage Java Persistence API (JPA), where the Java objects 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 plan web interface for remote management with possible device management extension therefore Figures 4 and 5 present the Android client prototype application which is enabling a merge of different source of personal identities and replicates knowledge to the server. In a certain time of period the 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.

6. Security Issues

The very important aspect of application concept, where maintained personal data are, is the security. Users are sensitive about their personal information and therefore we consider high level of security mechanism for distributing data between server and client. The secure channel is the Secure Socket Layer (SSL) based on the Rivest Shamir Adleman (RSA) asymmetric cipher algorithm. The trust store file with application certificate is included in the client application which is retrieved securely over the password

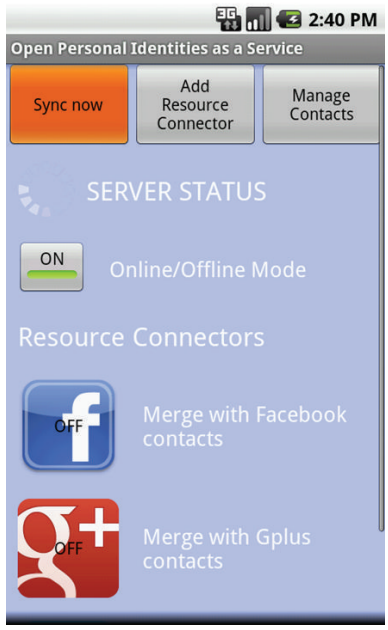

Figure 4: Client android application: services.

Figure 5: Client android application: access point.

and the secure communication would be established between client and server with trusted certificate. Therefore only clients and servers with trusted certificates which are signed by certification authority are able to start communication. In other words the channel is well secured and there is no possibility for man in the middle to decode communication secret without knowledge of 4096B long private key which is used and be covered at safe place on server under the key store password.

Another security threat for Android mobile device platform is hidden on client side in data accessibility over shared memory or over local sqlite3 database which are stored under application uid on local Linux file system. The attackers would be able to view data from memory or from database file. Such scenario is conditional to rooted devices whose users are willing to unlock mobile device for exploit more device features, but on the other hand they losing security capability of nonrooted device.

7. 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 of personal information supposed to be automatically redistributed over the connected systems within secured channel for data exchange. We acknowledged that the users are very sensitive about their personal information and therefore we consider as a must high-security level of data processing and necessary system security capabilities. 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 behaviour. 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.

Acknowledgments

The work and the contribution were partially supported by the project "SMEW—Smart Environments at Workplaces", the Grant Agency of the Czech Republic, GACR P403/10/1310 and "Smart Solutions in Ambient Intelligent Environments", University of Hradec Kralove under the project SP/2012/6.

References

[1] D. Ward, "Personal identity, agency and the multiplicity thesis," *Minds and Machines*, vol. 21, no. 4, pp. 497–515, 2011.

[2] P. Brida, J. Machaj, J. Benikovsky, and J. Duha, "An experimental evaluation of AGA algorithm for RSS positioning in GSM networks," *Elektronika ir Elektrotechnika*, vol. 8, no. 104, pp. 113–118, 2010.

[3] N. Chilamkurti, S. Zeadally, A. Jamalipour, and S. K. Das, "Enabling wireless technologies for green pervasive computing," *Eurasip Journal on Wireless Communications and Networking*, vol. 2009, Article ID 230912, 2 pages, 2009.

[4] N. Chilamkurti, S. Zeadally, and F. Mentiplay, "Green networking for major components of information communication technology systems," *Eurasip Journal on Wireless*

Communications and Networking, vol. 2009, Article ID 656785, 7 pages, 2009.

[5] C. Y. Liou and W. C. Cheng, "Manifold construction by local neighborhood preservation," in *Proceedings of the 14th International Conference on Neural Information Processing (ICONIP '07)*, vol. 4985, pp. 683–692, Kitakyushu, Japan, 2007.

[6] D. Korpas and J. Halek, "Pulse wave variability within two short-term measurements," *Biomedical Papers of the Medical Faculty of the University Palacky, Olomouc, Czechoslovakia*, vol. 150, no. 2, pp. 339–344, 2006.

[7] V. Kasik, M. Penhaker, V. Novak, R. Bridzik, and J. Krawiec, "User interactive biomedical data web services application, e-technologies and networks for development," *Communications in Computer and Information Science*, vol. 171, no. 16, pp. 223–237, 2011.

[8] D. Vybiral, M. Augustynek, and M. Penhaker, "Devices for position detection," *Journal of Vibroengineering*, vol. 13, no. 3, pp. 531–535, 2011.

[9] M. Penhaker, M. Cerny, L. Martinak, J. Spisak, and A. Valkova, "Home care—smart embedded biotelemetry system," in *World Congress on Medical Physics and Biomedical Engineering*, vol. 14, pp. 711–714, Seoul, South Korea, 2006.

[10] P. Mikulecky, "Remarks on Ubiquitous Intelligent Supportive Spaces," in *Proceedings of the 15th American Conference on Applied Mathematics/International Conference on Computational and Information Science*, pp. 523–528, University of Houston, Houston, Tex, USA, 2009.

[11] K. Juszczyszyn, N. T. Nguyen, G. Kolaczek, A. Grzech, A. Pieczynska, and R. Katarzyniak, "Agent-based approach for distributed intrusion detection system design," *Lecture Notes in Computer Science*, vol. 3993, pp. 224–231, 2006.

[12] Z. Machacek and V. Srovnal, "Automated system for data measuring and analyses from embedded systems," in *Proceedings of the 7th WSEAS International Conference on Automatic Control, Modeling and Simulation*, pp. 43–48, Prague, Czech Republic, March 2005.

[13] A. Bodnarova, T. Fidler, and M. Gavalec, "Flow control in data communication networks using max-plus approach," in *Proceedings of the 28th International Conference on Mathematical Methods in Economics*, pp. 61–66, 2010.

[14] V. Bures, "Conceptual perspective of knowledge management," *E & M Ekonomie a Management*, vol. 12, no. 2, pp. 84–96, 2009.

[15] R. Brad, "Satellite image enhancement by controlled statistical differentiation," in *Proceedings of the Innovations and Advances Techniques in systems, Computing Sciences and Software Engineering*, pp. 32–36, December 2007.

[16] P. Tucnik, "Optimization of automated trading system's interaction with market environment," in *Proceedings of the 9th International Conference on Business Informatics Research*, vol. 64 of *Lecture Notes in Business Information Processing*, pp. 55–61, Universität Rostock, Rostock, Germany, 2010.

[17] T. Thompson, "The android mobile phone platform," *Dr. Dobb's Journal*, vol. 33, no. 9, pp. 40–47, 2008.

[18] G. Shih, P. Lakhani, and P. Nagy, "Is android or iphone the platform for innovation in imaging informatics," *Journal of Digital Imaging*, vol. 23, no. 1, pp. 2–7, 2010.

[19] P. C. Hii and W. Y. Chung, "A comprehensive ubiquitous healthcare solution on an Android mobile device," *Sensors*, vol. 11, no. 7, pp. 6799–6815, 2011.

[20] JPA Performance Benchmark (JPAB), ObjectDB software Ltd, 2012, http://www.jpab.org/.