Leveraging New Business Models with Identity Management – An e-learning case study

José M. del Álamo
DIT, Universidad Politécnica de Madrid,
Ciudad Universitaria s/n, 28040 Madrid, Spain
jmdela@dit.upm.es,
http://www.dit.upm.es/jmdela

Abstract. New business models have arisen in different contexts such as the Internet and telecom networks which have been grouped under the umbrella of the buzzword 2.0. They propose opening up service platforms in order to increase profit by means of innovative collaboration agreements with third parties supported by identity management technologies. This paper introduces a research work, the PABIOS project, where these ideas have being applied in an e-learning context. It also describes how identity management technologies have been integrated into its architecture through a validation prototype.

1. Introduction

Many e-companies have been working for a long time just with their own close set of customers and resources. It was one of their treasures and they were jealous to share them with other companies because they were afraid to lose some profit in aid of their competitors. Performing in such a way has lead to walled-garden business models. Their main drawback is that a huge engineering effort has to be spent both on development and also on marketing sides, in order to get a new service up and deployed to the market.

On the other hand, new business models have arisen in different contexts such as the Internet and telecom networks, which have been grouped under the umbrella of the buzzword 2.0: Web 2.0 [1], Telco 2.0 [2], Mobile Web 2.0 [3], and so on. Their common approaches are:

1. The idea of a platform; i.e. there is not a hard boundary as in the walled-garden, but rather, a gravitational core around which the business is created.
2. Harnessing collective intelligence; i.e. turn your customers and providers into a global brain, which could be used to enhance your business.

3. Data is one of the assets a company owns; notice that most of times this information is about the company customers.

Regarding the first point, nowadays there is a trend in telecom and Internet domains towards partnership and the need to build technology platforms that enable for third party providers to collaborate. Relevant examples of this trend are British Telecommunications (BT) Project Web21C [4] and Amazon Web Services [5] platforms, which allow external developers and businesses to build their own applications with a set of Web Services interfaces.

The most innovative case though, is the so called user-centric platform. It allows users (not necessarily technically skilled) to create their own contents and applications (mashups) from the combination of different sources. There are several initiatives of user-centric platforms both in telecom networks, such as the Open Platform for User-centric service Creation and Execution (OPUCE) [6], or in the Internet, such as Yahoo Pipes [7].

The previous paragraphs also point towards the second idea of the 2.0 approach: make profit from allowing your partners/users to innovate over your platform. Everyone can be a reseller now so, if you support with your platform the development and offering of innovative services, you will get some profit from the use of your own services, the use of your platform features from third party developers, and the ancillary services you could provide.

Nonetheless, the combination of user-centric environments with social networks allows users to share their services within a community which will promote the most interesting ones at a minimum cost (viral marketing), thus eliminating the aforementioned main disadvantage of walled-garden business models i.e. development and marketing expenses.

The obvious question now is, why should any third party use my platform and not anyone else's? The answer points to the third idea of the 2.0 approach: data is one of the assets a company owns.

Companies had been collecting identity information about their customers which was kept on information silos just for their own use. However, now they can use this information to boost their platforms and take advantage of the benefits the 2.0 approaches provide, thus leveraging new and profitable business models. Moreover, in most cases they had even established a trust relationship with their customers, which could be also used as a powerful asset.

On the other hand, in most countries there are laws which require companies to ensure security and privacy when revealing personal information about a customer, such as the Directive 2002/58/EC of the European Union [8]. Thus, we have arrived at a point where we could create open platforms that third parties would use to develop innovative and profitable services as far as customers' privacy and anonymity are protected.

Identity management is the cornerstone to support these win-win scenarios because it provides the means to manage and selectively disclose user-related identity information within an institution or between several of them while preserving and enforcing privacy and security needs.

This paper proposes an approach on the usage of Identity Management technologies in order to leverage the new business models represented within the 2.0 concepts. To validate the feasibility of the proposal an e-learning field has been

chosen. In this context, a prototype demonstrates how an e-learning platform supported by identity management allows third parties to offer their services and even to develop their own e-learning applications. The work is framed within a CELTIC European Research project: The P4P Application Based Open Source (PABIOS) project [9].

Next section introduces the e-learning context of the project showing the drawbacks of current e-learning systems and the advantages of the proposed approach. Then, the basics of Federated Identity Management technologies are introduced. Finally, the PABIOS project is described, showing the validation scenarios, and detailing the use of identity management technologies to support the aforementioned ideas. Section 5 concludes the paper with a brief summary and orientation of future work.

2. Application Field: e-learning

Due to the interactivity and ubiquity of the Internet, learning is possible without space and time barriers. The competition between learning institutions is rapidly increasing and therefore they are under pressure to find new strategies and business models to produce and deliver cost-efficient educational products. Moreover, learners are also putting on pressure by demanding specialized and up-to-date contents and services that fit their curriculum requirements.

In this scenario a strategic consideration for learning institutions should be whether to develop all the components of the e-learning business model solely with in-house resources or open their systems to collaboration agreements with third parties such as libraries, publishers, e-learning content providers, other educational institutions, etc. The advantages and drawbacks of both models have been described in the previous section.

Nowadays there are already some initial approaches through collaboration between learning institutions but they are bound to the use of identity management to support single sign on scenarios. One example is the pan-European project called EduRoam (Educational Roaming) [10] which allows users visiting another institution to log on to it using the same credentials they would use if they were at their home institution. Another example is Eduserv Athens [11], the de facto standard for secure access management to web-based services for the UK education and health sectors.

Although these scenarios are a first step in the collaboration process, they are quite limited: it is impossible for the students to use their identity information out of the boundaries of their home institution in order to get better and faster services.

On the other hand, a 2.0-oriented e-learning platform would provide its own e-learning contents and base services, but also the means for third parties to provide theirs based on identity information. This platform will leverage new business models for educational institutions allowing them to provide their students with new materials and services cost effectively, securely and with guarantees for students' privacy and anonymity.

In order to create such a platform a complete identity management solution must be applied. Next section describes its bases.

3. Federated Identity Management Foundations

Identity information is at the core of the relationship of a company with its customers, partners and other companies, and is a basis to support its business models. Extending the definition taken from [12], *network identity* refers to the collections of data about a subject that represent attributes, preferences, and traits in all his open accounts in a network.

Identity management is understood as the discipline that deals with the access management of users to distributed network identity resources in its technical, legal and business aspects. At a technical level, the network management is related to network security, service providing, clients management, easy and transparent log in (single sign on –SSO) and log out (single log out –SLO), distributed identity resources linkage (identity federation) and Web Services providing.

There are two main approaches for identity management: centralized and federated. The requirements of the approaches described in this paper set an environment where there are different entities collaborating e.g. the platform, partners, and other educational entities, each one within a different administrative domain and with its own set of subscribers. Thus a centralized model is not possible.

There are various standards and frameworks that support Federated Identity Management, being the most important the Security Assertion Markup Language (SAML) [13], Liberty Alliance [14] and Shibboleth [15]. SAML is an XML standard from OASIS committee for exchanging authentication, authorization and identity information between security domains. Both Shibboleth and Liberty converge on SAML, but Shibboleth have been developed with the aim of provide support for Web SSO scenarios.

The Liberty Alliance approach for federated identity management associates service providers to trusted domains called circles of trust, that are supported by an architecture and a set of protocols, and by operative agreements in which trust relationships are defined between providers (Fig 1). Within a circle of trust, subscribers can federate (link) isolated accounts that they own across different providers using a pseudonym. Some entities could be especially prepared to manage these federations, as well as providing other ancillary services:

- **Identity Provider (IDP).** It is a trusted entity which authenticates users, maintains their federations, and issues identifiers to other entities. An IDP may include an **Authentication Service** (AS) to authenticate service providers that are working on behalf of end users. A typical identity provider is a university which manages its own directory of accounts of its students.
- **Service Provider (SP).** A role performed by a system that provides services to end-users or other system entities. Within an identity management context, an SP can also provide or ask for users' identity information using Web services. In the former case it is called a Web Service Provider (WSP) and in the latter case it is called a Web Service Consumer (WSC). An SP could be both a WSP and a WSC. Examples of service providers are libraries, on-line book shops, independent e-learning content providers, etc.

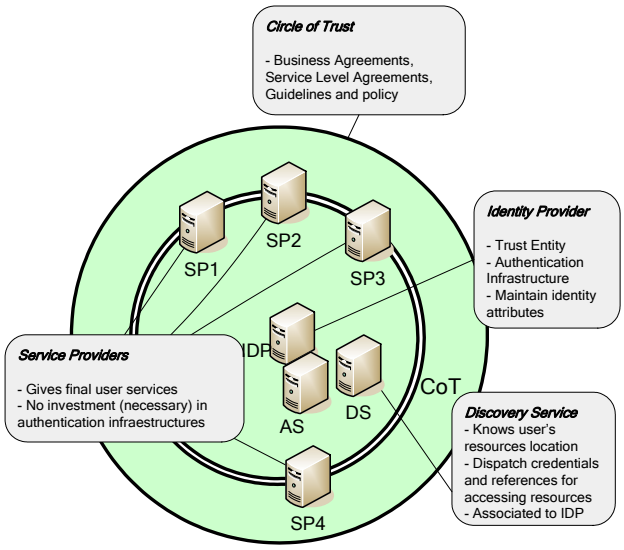

Figure 1 Circle of trust concept

- **Discovery Service (DS).** It knows where the users' identity resources are stored within the circle of trust and how to access them; i.e. it knows all the WSP inside the circle of trust.

4. The PABIOS project

PABIOS project is developing an e-learning oriented environment which allows the creation of social (People for People – P4P) applications by means of the integration of collaborative peer to peer (P2P) services and a large number of other distributed services provided by third parties.

PABIOS provides the P2P infrastructure and a platform with some basic e-learning services as well as the means to incorporate third party ones. The integration of the providers into the platform is supported by federated identity management technologies which provide privacy and security for both the end users and also the providers themselves.

Fig. 2 shows an overview of PABIOS architecture which includes the following entities:

- **PABIOS Learning Management System (LMS)**: It is the basis for the creation, management and delivery of e-learning services. A free, open source implementation of an LMS named Moodle [16] has been used to provide these features.
- **PABIOS framework**: The main task of the framework is being the interface between the P4P applications and the PABIOS LMS, and providing the infrastructure that allows the integration of third party providers.
- **PABIOS P4P application**: This prototype is used to demonstrate the PABIOS features. This client-side application is the main access point for

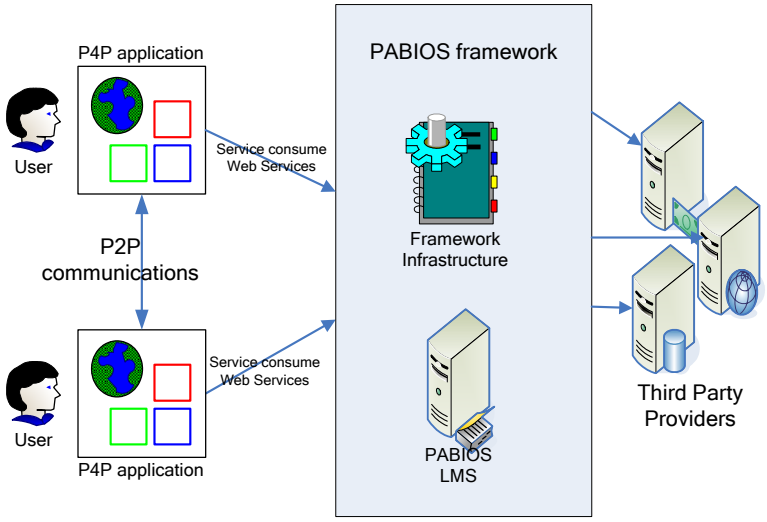

Figure 2 PABIOS Architecture

the users to the PABIOS LMS services, the P2P communication services, and the third party services.

4.1 Validation scenario

The basic scenario consists of a single domain corresponding with an e-learning institution, the PABIOS College, supported by the PABIOS platform. The PABIOS College is offering e-learning materials to thousand of their students through a P4P application.

In the validation scenario students must make a transfer every time they join a new course and send by fax a copy of the payment invoice. This is an annoying process which waste much time. In order to facilitate it, PABIOS College agrees on collaborate with a payment provider which is willing to offer their services to their customers in exchange of a small fee. The PABIOS College will receive a percentage of that fee.

This win-win business model is possible due to the fact that PABIOS system knows all the customers and offers an open identity-based platform for the third party to join. The main requirement of this platform is that no identity information must be reveal to any of the parties participating; thus when students federate the accounts they have both in the payment provider and in the College, a pseudonym is agreed to refer to them during each transaction.

Web Services has been chosen as the middleware to support the communication between all the entities participating. We use Liberty entities to support the identity management requirements of the scenario. Figure 3 shows PABIOS architecture with the Liberty entities that participate in the scenario.

In the implementation the P4P application performs as an SP because it provides services to students introducing them to the PABIOS College and to the e-learning services it offers. On the other hand, whenever students want to join a new course the P4P application needs to use their identity information to make the payment. Thus it

first authenticates against the AS in order to retrieve some information related to where the DS is and how to access it. In this case the P4P application is performing as a WSC.

When the P4P application needs to know some identity information regarding a student, it would firstly query the DS in order to know the location of those identity resources and the credentials to access them, and then it would query the SP that stores such information; i.e. the payment service.

Finally, the payment service performs as a WSP because it modifies identity information as requested by the P4P application, e.g. make a payment on the student account.

4. Conclusions

Identity management is the cornerstone to support the new business models arisen from the Internet that open up service platforms to collaboration with third parties. It allows win-win scenarios where third parties can provide personalized services within a service platform offering and/or using users' identity information.

The PABIOS project aims to create a complete platform to support this business models in an e-learning context. Its initial results have been summarized in this paper, especially those focused on the integration of an identity management infrastructure within the architecture.

In order to validate the suitability of the PABIOS architecture we have developed a simple, but realistic and relevant, prototype. It consists of a simple educational institution which offers its e-learning services through a client-side application and that agrees on collaborate with a payment provider, thus facilitating the process that students must follow to join a new course using their identity information.

Further work considers the validation of other scenarios such as collaboration with online shops, e.g. travel agencies or book shop, which will appreciate the use of identity information of students to improve their business processes.

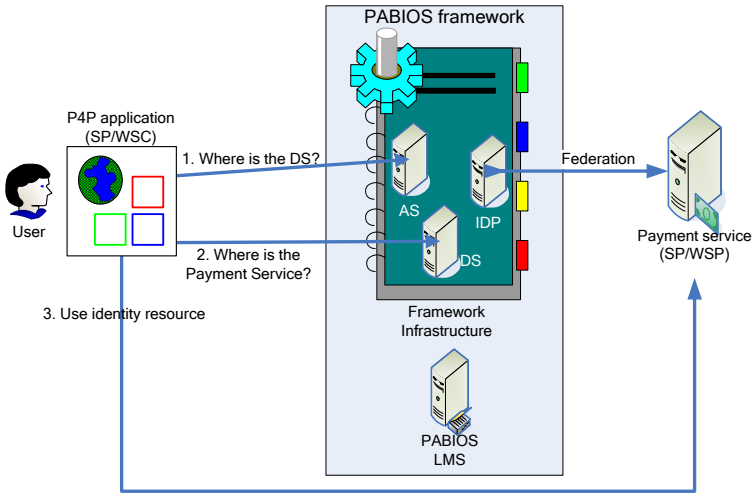

Figure 3 Liberty entities within PABIOS architecture

Acknowledgements

This work is framed within the CELTIC European research and development project PABIOS (*P4P Application Based Open Source*), EUREKA initiative, project ID CP2-020. We thank all our partners in the project for their valuable comments and proposals aiming at improving the ideas described in the paper.

References

1. T. O'Reilly, What is Web 2.0: Design patterns and business models for the next generation of software, O'Reilly Media Inc. (September 30, 2005); http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.
2. STL Partners Ltd., Telco 2.0 Manifesto: How to make money in an IP-based world. (May 16, 2007); http://www.telco2.net/manifesto/.
3. A. Jaokar and T. Fish, Mobile Web 2.0 (Futuretext, London, 2006).
4. Web21C SDK Developer Center (2007); http://sdk.bt.com/.
5. Amazon Web Services (2007); http://www.amazon.com/.
6. OPUCE Website (2007); http://www.opuce.eu/.
7. Yahoo Pipes Website (2007); http://pipes.yahoo.com/pipes.
8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal, L 201, Jul. 2002, pp. 37-47.
9. PABIOS Website (2007); http://projects.celtic-initiative.org/pabios/.
10. Eduroam Website (2007); http://www.eduroam.org/.
11. Eduserv Athens Website (2007); http://www.athensams.net/.
12 P. Windley, Digital Identity (O'Reilly Media, USA, 2005).
13 S. Cantor et al, Assertions and protocols for the OASIS security assertion markup language (SAML), Standard v2.0 (OASIS, 2005).
14 Liberty Alliance Website (2007); http://www.projectliberty.org.
15 Shibboleth Project Website (2007); http://shibboleth.internet2.edu.
16. Moodle Website (2007); http://moodle.org/.