Carriedo, Francisco; Beltrán, Marta

Conference Paper

Providing identity based on the telephone number: a new business model for telecommunication operators

26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24th-27th June, 2015

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Carriedo, Francisco; Beltrán, Marta (2015) : Providing identity based on the telephone number: a new business model for telecommunication operators, 26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24th-27th June, 2015, International Telecommunications Society (ITS), Calgary

This Version is available at:
http://hdl.handle.net/10419/127132

Providing identity based on the telephone number: a new business model for telecommunication operators

Francisco Carriedo and Marta Beltrán
Department of Computing, ETSII
Universidad Rey Juan Carlos, Madrid (Spain)
fcarriedos@gmail.com and marta.beltran@urjc.es

Abstract

Managing user identities to solve authentication and access control for current services and applications remains one of the greatest challenges facing IT today. Using telecommunication operators' infrastructures and experience could surely facilitate identity management in such a scenario, because they hold the best and largest user directory of the world. Telephone numbers allow operators to provide rich and disambiguated identities ready to be used by end-users from anywhere with any device.

This work proposes an Identity Management as a Service (IdMaaS) based on the telephone number and provided by telecommunication operators. Both, the technical architecture and the most suitable business model needed to build and to exploit this new service are presented.

I. INTRODUCTION

Considering the dramatic changes in the telecommunications sector since 2008 (year of the introduction of the first iPhone and of the Apple's App Store), it is clear that telecommunication operators should reinvent the way they work from both, a strategic and a technical point of view ([1]). Some classical revenue streams of these companies, mainly traditional telephony and short messaging services, are in serious danger due to the alternatives offered by the Over-The-Top companies (OTTs). These alternatives, based on agile Internet technologies and models, are increasingly engaging end-users with innovative applications and services provided at very little costs or even free of any charge.

Unless operators want to become just connectivity providers, they should be taking maximum advantage of their key differential value as the mobile network providers: they hold the best user directory of the world and the telephone number is still the most reliable contact method everybody trusts. Telephone numbers are ubiquitous and people generally retain the same number for a long period of time. Very different from identities in the Internet, freely generated and disposed with no tight control over them, telephone numbers are provided and managed by stable and controlled telecommunication companies according to strict regulations under the supervision of national and international organisms that take care of fairness, rights and responsibilities of each party (basically, customers and operators). A digital identity based on the telephone number, above all a trustable identifier, could be extremely useful in the short or midterm for new trends related to the Future Internet such as m-Health, Smart Places or Internet of Things to mention only some significant examples. And providing this identity would allow telecommunication operators to recover their place in the communication services market.

Identity management is normally interpreted as the management of users' identities and credentials for accessing resources and it involves two kinds of functions: authentication and access control. Authentication is the process of verifying the correctness of a claimed identity or origin while access control is the process of granting or denying access to resources as a function of previously determined authorizations based on identities and credentials. Current identity management systems are under review because the rapid growth in the number of services consumed by average end-users leads to an increasing number of different digital identities each user needs to manage. Furthermore, these average users access to all these services using different devices, which may have different security levels.

As a result, many people feel overloaded and ask for identity management systems capable of integrating all possible devices and of providing ubiquitous user authentication and access control. One possible solution is to rely on the Identity management-as-a-service (IdMaaS) model, an identity management service relying on the cloud computing paradigm where the identity management function is provided by a specialized cloud provider. The IdMaaS model has a number of advantages such as reduced cost of ownership, scalability, self-service, location and device independence or rapid deployment. However, there are important concerns preventing the adoption of this model, all of them related to assign a function as critical as identity management to a cloud third party ([2]).

With this work, we aim to propose a new application of mobile cloud computing ([3]-[6]) and make contributions that bring the benefits of this paradigm to telecommunication providers, other companies and end users. More specifically, our contributions can be summarized as (a) We propose a novel kind of IdMaaS model based on an identity related to the telephone number. This model is a new revenue stream for telecommunication operators and a solution for identity management able to combine security and flexibility to meet current users expectations and application/services requirements (b) We define the technical architecture needed to build this new service, specifying five elements: the identity itself, a directory, lifecycle management tools, regulatory mechanisms and governance tools (mainly auditing and reporting tools) (c) We analyze the business model more appropriate for the new service taking into account the particularities of the telecommunications sector and its current environment.

The rest of this paper is organized as follows. Section II presents the considered context and formulates the problem. Section III defines the Identity Management as a Service based on the telephone number and provided by telecommunication operators from a technical point of view. Section IV proposed and analyzes the related business model. Section V summarizes the most important related work. And finally section V presents the main conclusions obtained with this work and some interesting lines for future work.

II. CONTEXT AND PROBLEM FORMULATION

Traditional telephony and short message services revenues are under threat from newer Internet-based alternatives ([1]). Telecommunication operators are trying to define their own next-generation communication services in an attempt to retain their customers, increasingly engaged with these Over-The- Top (OTT) applications and services provided by Internet companies at very little costs or even free of any charge. Many operators are pursuing a profitable route to end users typically based on IMS (IP Multimedia Subsystems) deployments, infrastructure virtualization (through Network Functions Virtualization and Software Defined Networks) or RCS (Rich Communication Services).

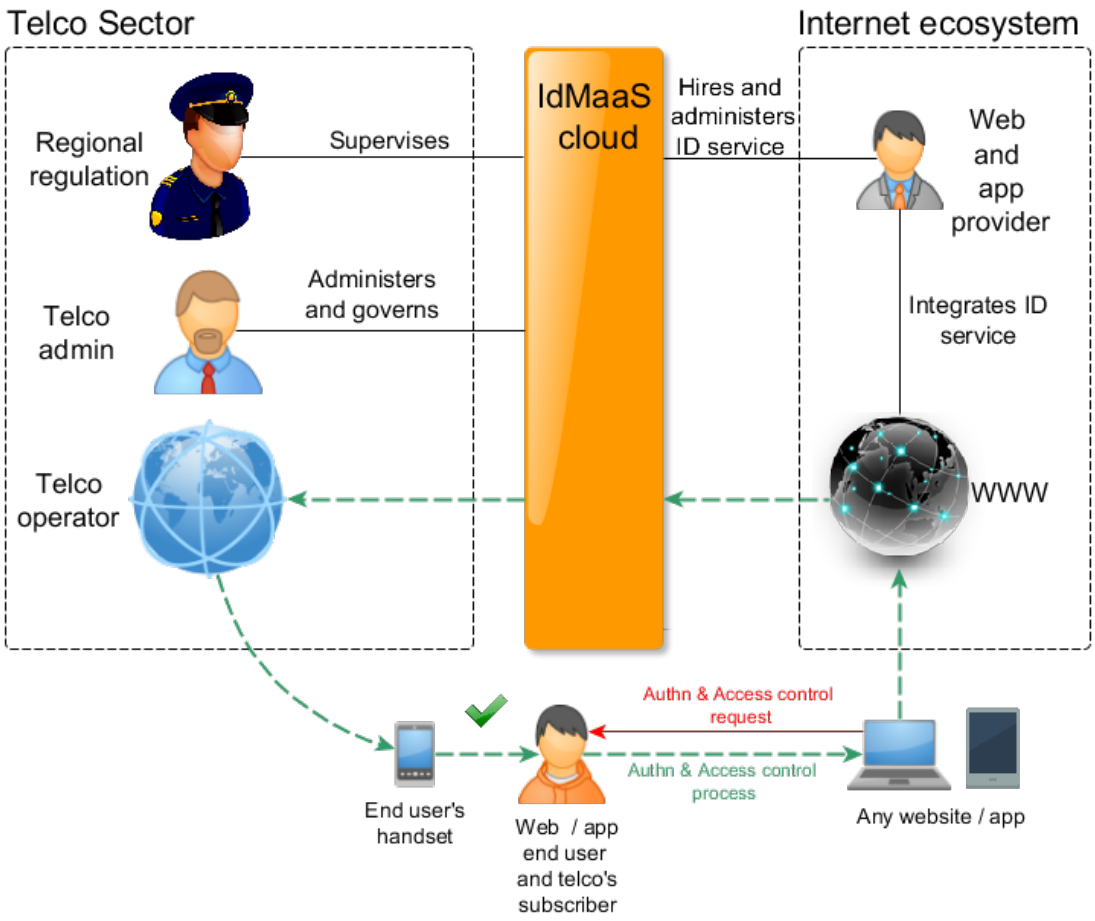

Figure 1. IdMaaS scheme

This work proposes the cloud computing paradigm as a possible solution defining a new cloud-oriented service model for telecommunication operators, the Identity Management as a Service. This kind of service can provide ubiquitous identity (usable from different locations and devices) based on the effective use the telephone number, regardless of the infrastructure available in the lower layer and of the type of services consumed by the end user.

This new service must be defined according to its specific technical and functional requirements but also to the idiosyncrasy, regulations and business ecosystem of the telecommunications sector. Previous works such as [7] or [8] have identified how the success of mobile applications or platforms are every day more dependent on the mobile ecosystem, seen as symbiotic relationships of customers, providers, developers and competitors, and this situation is a good starting point for the introduction of a new cloud-oriented service in the sector (see Figure 1).

The proposed IdMaaS solution can bring the best of the two worlds together (Internet and telecommunications, cloud and mobile) with an important change of strategy, making operators able to compete at the service level. On one hand, this service allows service providers and application developers to concentrate on designing their value outsourcing the identity management instead on performing engineering tasks related to the design and deployment of their individual and proprietary solutions. Current identity management systems are very often too expensive to allow the model to prosper from the economic point

of view, too particular to easily interoperate with other solutions and too traditional to scale and to adapt with the required speed. On the other hand, the proliferation of different identity management solutions is complicating end user everyday tasks, and this kind of service could greatly simplify user's identification (authentication and access control) for almost all services with the aforementioned advantages of an IdMaaS approach.

The proposed model allows telecommunication operators to rent "spare capacity", because they already have the capacity to manage identities based on the telephone number. The main efforts to become providers of the proposed service should be focused on two aspects:

- Developing the cloud-interfaces needed to connect the identity management layer to the third party platform/application layers above.
- Developing and/or selecting and deploying the lifecycle management and governance tools.

The probabilities of success of the operators as providers of this type of service are very high as third party providers and end users can trust them to provision such a critical asset as identity. Telecommunication operators guarantee the size, stability and influence needed to assume this kind of responsibility. Furthermore, they have extensive experience dealing with legal regulations related to privacy and can face the challenge of achieving the desired availability, coverage and delays. And there is another important advantage in the IdaaS proposed model: unlike what happens with most of current digital identities, an identity based on the telephone number provides identity disambiguation. Therefore, an identity to uniquely identify, contact or locate a single person thanks to the contractual relationship between the client (there are commonly available data on the individual, at least name, billing address and bank account) and the operator.

III. IDENTITY MANAGEMENT AS A SERVICE BASED ON THE TELEPHONE NUMBER

A. The identity

Any individual can be authenticated by something she has, something she knows, something she is or by a combination of them. It has to be pointed out that the two first conditions of having and knowing something are fulfilled by any current mobile operator subscriber: if you can be contacted through your phone number this implies that you have the associated SIM (Subscriber Identity Module), and if you are available through the mobile network this implies that you know the PIN (Personal Identification Number) to use this SIM. These two facts enable telecommunication operators to act as reliable identity providers for their subscribers, being the SIM a basic element that strongly links the real identity with the digital identity.

This is an important advantage of the proposed service, the identity provided by telecommunication operators guarantee disambiguation if needed, i.e. to establish a direct relationship between a digital identity and a particular person. Most of social networks, mobile apps and cloud services do not verify user profiles with tangible information such as a government-issued ID or a bank account number. This kind of identities are easy to obtain but they do not allow disambiguation and they may be susceptible to identity spoofing attacks. The identity provided by a telecommunication operator based on the telephone number and on the associated SIM can solve both issues: getting a new telephone number is not as easy as signing up since operators require personal information such as government identification and/or credit information and phone numbers are not easy to fake or to spoof.

Regarding the identity definition, operators already hold in their current identity management systems all the data needed to provide the proposed service in the basic use cases for authentication and control access: accurate and verified personal data plus access to some sort of economical source, be it post-paid or pre-pay. Only if more sophisticated use cases requiring additional information per user got developed, an extension of the current operator's information model would be needed.

B. The directory

The operators already have a strong information basis of their subscribers that can be leveraged through the proposed service. The operators' information systems that usually support this information are the Business Support Systems (BSS). A specific interface to properly integrate these systems with the IdMaaS identities cloud-based repository is needed. This is, mainly, the development effort that would be required of operators to be able to provide the new service.

The proposed IdMaaS approach is a federated identity management system in which identities are distributed over several controllers, controlling each operator a repository storing the identities of her subscribers. Different operators must cooperate in federated schemes (as they usually do in other aspects of their usual operation) to make the identity management services global, probably the best option would be OpenIDConnect ([9]).

C. Lifecycle management tools

The Distributed Management Task Force (DMTF) industry standard organization provides a life-cycle model to use in cloud environments ([10]) that can cover the needs of the IdMaaS model. Following this life-cycle the proposed service should go through the following states:

1. Defining service template.
2. Offering.
3. Contracting.
4. Provisioning.
5. Runtime maintenance.
6. Terminating service and de-provisioning.

D. Regulatory mechanisms

Identity provisioning and de-provisioning processes must comply with regulations affecting the telecommunications sector. There are two possible scenarios when getting an identity based on a telephone number from a telecommunication operator: it is either an available identity or an in-use identity that has to be ported from another provider responding to a user's request. The first case does not represent a problem, as it can be simply internally provisioned by the operator as it is currently done with telephone numbers, but the second case is more complex and depends on the regulatory mechanisms. The same considerations can be made about de-provisioning: it is easy to free an identity but a portability process is needed to move an in-use identity from one provider to another.

In order to analyse the alternatives to define a portability process in the proposed IdMaaS context, three regulation case studies have been selected, paying special attention to their

current portability processes: Spanish regulations ([11]), German regulations ([12]) and USA regulations ([13]). These three regulations have been chosen because they correspond to regions that have already commercially launched RCS (Rich Communication Services), which allows service capabilities for telecommunication operators depending on similar regulatory issues related to identity as IdMaaS does.

In the case of the Spanish regulation, the portability scenario is defined taking into account a subscriber (acting as the client of telecommunication service), the telecommunication operators (one acting as donor of the entity, the other one acting as recipient of the entity and both acting as providers from the point of view of the subscriber) and the reference entity (a national supervisor monitoring each portability process to solve potential conflicts among the involved agents and maintaining the coherency of the identity management).

The portability process is a transaction actually performed by the donor and recipient providers and. When it is completed uneventfully, its result is notified to the reference entity, who registers the new identity situation for everyone interested in knowing its new status.
The reference entity requires the providers to perform the portability transaction in certain conditions:

- It has to be granted by any provider, and participating providers are responsible for all the costs derived from the process, including any harm suffered by the subscriber.
- It cannot be blocked by any provider, regardless payment and contractual status and similar issues.
- It has to be performed electronically.
- It has to be kept as efficient as possible and it must assigned a high level of priority.
- It has to be considered secure, mentioning explicitly some of the most important properties of IT security such as authentication of the participants, integrity and accountability of the exchanged messages and availability.
- Once scheduled, it should be notified to the subscriber and completed in no more than 24 hours during the working days and limiting to that period the allowed downtime in the service due to technical reasons.
- Providers have to accomplish a set of tests defined by the reference entity in order to determine if their infrastructures do satisfy the imposed requirements. This implies that the regulation carefully protects the subscriber, preserving his freedom to choose his preferred provider, trying to keep the process fair and efficient and remarking the role of operators as providers responsible for the product they deliver.

In the other two selected regulations, both German and American, the same baseline can be observed, determining practically the same procedures, limits and responsibilities for the portability and trying to guarantee a dynamic and non problematic process.

After the study of these regulations two conclusions can be drawn, one related to the technical perspective and the other one to the business model. About technical issues, it can be observed how the requirements and conditions dictated by every considered regulator resulted very similar to the SLA regulations used in cloud environments, taking care of similar concerns than in the Internet ecosystem. Ranging from security to the required time periods (for example, porting a telephone number takes no longer than porting a domain name on the Internet), the identity management process in the telecommunication sector seems to follow similar dynamics than in cloud services, being therefore possible to use it directly as it currently is in the proposed IdMaaS context.

Regarding business considerations, it may be interesting to point the homogeneity of the service regulations affecting the different operators. Many time and efforts have been invested to reach a consolidated community of telecommunication operators across the world, all working with similar processes, and that might be an important advantage compared to the fragmentation of current identity management as a service alternatives.

E. Governance tools

Since IdMaaS is a kind of service mainly designed to be provided by telco operators, the associated governance tools should enable the kind of functionalities these enterprises are used to, providing tight control of operations and status of any involved asset. The customers of the service require too convenient tools to allow them to keep track of how their identities are provisioned, used, billed, etc. Both kinds of tools must be provided in a IdMaaS context leveraging proposals such as the SOA framework ([14]) for the operator's governance tools and deploying generic and portable usual cloud governance tools for customers.

IV. A NEW BUSINESS MODEL FOR TELECOMMUNICATION OPERATORS

The Identity Management as a Service provided by telecommunication operators has been presented from a technical point of view in the previous section. In such context different business model representations could be used to illustrate the business model related to this new service. In general, two kinds of representations use to be considered: flow-logic models and system-level models.

The first kind of models represent value flows and activities while the second kind represents a high level abstraction of the business logic. An example of the first kind of models is the e3-Value ([15]), an example of the second is the Business Model Ontology or BMO ([16]). Previous works about new service models in mobile environments have been based in both types of representations.

However, recent works have demonstrated that traditional models are not suitable for service-oriented business models since they are not able to take into account service specific aspects. That is the reason why new representations such as the VISOR framework ([17]) or the Service Model Business Canvas ([18]) have arisen.

In this work the Service Model Business Canvas (SMBC) has been selected to represent and to analyze the proposed business model for IdMaaS (Figure 2). It is an easy, compact and intuitive model based on a representation widely used both in academic and industry contexts, the Business Model Canvas, adapted to service-oriented scenarios. This kind of model allows to identify the interaction points between telco operators, customers and partners (the three perspectives of the model), providing a powerful tool to illustrate (and to analyze, to design and to optimize) how these interactions summarized in nine dimensions or aspects contribute adding value to these operators, customers and partners.

Regarding the proposed service, IdMaaS customers may fall into two categories: end users who provide their own identity to different services and applications (compatible with the proposed approach) using the identity based on the telephone number or third party providers (usually, PaaS and SaaS providers) offering an identity management system based on IdMaaS to their users in order to improve their experience. And one main partner has been identified in the IdMaaS scenario, although it may not be present or there may be more than one: the IT

provider (or providers) helping the telecommunications operator to start providing the IdMaaS service and to keep providing it with the committed quality of service.

Although some operators may have the capacity to provide IdMaaS without relying on an external partner, co-creation is one of the main characteristics of current cloud services and partners use to play an important role in making service business models profitable. In the IdMaaS case the IT partner provides a specific IT solution (some examples could be the infrastructure itself, lifecycle management tools, governance tools or cloud interfaces to the upper layers) allowing the operator to focus on its own value proposition for IdMaaS customers. The IT solution may be provided traditionally (proprietary, in-house) or as a service (cloud-oriented) and it may require an integration process usually provided by the IT partner too.

In Figure 2 the main perspective corresponds to the telecommunication operator and the main dimension is related to the value proposition. As it can be seen the proposed service allows these operators to recover relevance for their customers and to innovate offering a cloud-service. Given the predictable evolution that operators will have to make in the short or medium term, this is very interesting to gain experience with the new business model and to begin to work with a greater degree of openness to Internet and to the cloud paradigm. Furthermore, IdMaaS increases operator's sales and decreases their operational costs, taking advantage of a very often under-utilized infrastructure and tools. Important aspects for the two kinds of consumer are increased interoperability, flexibility, security, availability and scalability. In addition, third party providers can improve customer retention (due to the improved experience related to authentication and access control processes) and reduce their TCO avoiding an in-house identity management solution. Lastly, all possible IT partners can increase their sales by participating in the new service.

The key activities and key resources dimensions summarize the essential tangible and intangible resources and the main tasks that have to be carried out with them by the three involved agents (the operator, customers and partner) to provide and consume the service according to the technical description given in the previous section. It has to be pointed that the key resources for the operator comprise, not only the telephone numbers available for customers but also the cloud interfaces needed to integrate IdMaas with upper cloud layers and the lifecycle management tools. These essential resources may be owned by the operator or may be acquired to the specialized IT partner (most probably).

The relationship dimension illustrates how the operator must make available different tools to start, maintain and terminate the relation with customers. There are mainly four components to link operators and customers at different stages of their relationship and levels: the service catalogue explaining the different offers, the Service Level Agreement between the two participants, the service interface/API and the governance tools. In this dimension it can also be noticed that the relationship between the operator and the partner can be very similar to the relationship between the operator and her customers if the acquired IT solution is offered as a service or it may be the traditional (development or distribution) if the IT solution is offered as an in-house product.

The channel dimension of the model shows how the identity itself is the main way of interaction offered by the operator. Although off-line methods of interaction are provided to offer a customer service. End-users must use a mobile device to consume the service, while for third party providers the main resource for interaction is the IdMaaS interface needed to

		Cost structure	Key resources	Key activities	Value proposition	Relationship	Channels	Revenue streams
Customer perspective	End users	1.Compatible mobile device 2.Usage fees	1.Compatible mobile device 2.Coverage or Internet access	1.Selecting an offering 2.Contracting 3.Initiating, registration, configuring 4.Runtime maintenance (managing account) 5.Terminating service	1.Interoperability 2.Flexibility 3.Increased security 4. Increased availability 5. Scalability	1.Service catalogue (offering) 2.SLA (contracting) 3.Service API (provisioning and runtime maintenance) 4.Governance tools (runtime maintenance)	1.On-line (mobile devices) 2.Off-line (web, email, social network, phone call)	Time and resource savings
	Third party service providers (PaaS or SaaS)	1.TCO (Total Cost of Ownership) of the infrastructure, mainly setup costs 2.Marketing and promotion costs 3.Usage fees	1.Tangibles (IDMaaS SLA and service interface/API, *ad hoc* developments for integration) 2.Intangibles (customer basis and experience with identity management systems) 3.Staff	1.Selecting an offering 2.Contracting 3.Interfacing IDMaaS with provided services 4.Runtime maintenance and SLA monitoring 5.Terminating service	1.Interoperability 2.Flexibility 3.Increased security 4. Increased availability 5. Scalability 6.Increasing sales and customer engagement/ retention 7.Decreasing TCO	1.Service catalogue (offering) 2.SLA (contracting) 3.Service interface/API (provisioning and runtime maintenance) 4.Governance tools (runtime maintenance)	1.On-line (IdMaaS interface) 2.Off-line (web, email, social network, phone call)	1.Time and resource savings 2.More customers
Operator perspective		1.TCO (Total Cost of Ownership) of the infrastructure 2.Marketing and promotion costs	1.Tangibles (telephone numbers, interfaces and lifecycle management tools) 2.Intangibles (customer basis and experience dealing with regulatory mechanisms) 3.Staff	**IdMaaS** 1.Defining service template 2.Offering 3.Contracting 4.Provisioning 5.Runtime maintenance 6.Terminating service	1.Recovering relevance for their customers 2.Increasing sales 3.Decreasing operational costs (renting "spare capacity") 4.Innovating via cloud paradigm and gaining experience for future service offerings	1.Service catalogue (offering) 2.SLA (contracting) 3.Service interface/API (provisioning and runtime maintenance) 4.Governance tools (runtime maintenance)	1.On-line (identity associated to mobile devices) 2.Off-line (customer service)	Usage fees
Partner perspective (IT provider)		TCO (Total Cost of Ownership) of the infrastructure	1.Tangibles (provided IT) 2.Staff	Providing specific IT solution (service or product)	Increasing sales	1.Service catalogue, SLA, service API and governance tools (IT service) 2.Development or distribution (IT product)	1.Internet (IT services) 2.Technical and/or sales force (IT product)	Usage fees (IT services) or traditional sales (IT product)

Figure 2. IdMaaS business model

integrate the consumed identity management system with their own services. The channel for interaction with the IT partner depends again of the kind of service or product involved.

Finally, the cost and revenue dimensions have to be analyzed. The costs for the provision of the proposed service are mainly due to the TCO of the telco infrastructure and to the marketing and promotion costs for the new service. These last costs should be important at first stages because the proposed service implies an evolution that needs to be properly communicated to markets. Costs for end-users are related to the needed mobile device and to the usage fees they have to pay to use the identity management service. Third party providers have to pay these fees too, and they have their own TCO (the setup costs may be important because they have to adapt their service to work with IdMaaS) and marketing and promotion costs (to let their users know the new way in which their identities are going to be managed). Partners have also their TCO providing the proper IT solutions to the operator.

The telecommunication operator obtains its revenues by usage fees and two types of billing model should be considered: subscription to the service for end-users and the common pay-per-use model for the third party providers. In this case the billing unit should be the authentication transaction itself, possibly varying the price depending on the nature of the process requiring authentication and on the required security level (the price would not be the same, for example, to login in a website than to authorize purchase over 500 €). By the utilization of this service, both end-users and third party providers can take advantage of time and resource savings, being authentication and access control processes greatly simplified. Regarding end-users, IdMaaS allows them to avoid complex login processes, to operate with a single identity across any service or application they take part in, to keep the identity on safe hands (telecommunication operators) and to take advantage of different levels of authentication and payment capabilities. Furthermore, direct revenues are generated for third party providers through an increased customer engagement and retention caused by a better (and easier) experience using their service and by a lower barrier to entry. Partners generate their revenues from usage fees (if the IT solution is provided as a service) or traditional sales (if it is a product).

V. RELATED WORK

The nature of identity is changing to the point of considering that identity is the new money ([19]). Mobile phones are perceived as one of the key technologies that will enable the building of an identity infrastructure that can enhance both privacy and security in a context where all that we need for transacting is our identities captured in a unique digital record.

In such a scenario, widely-used identity management mechanisms relying on username and password have become inadequate and different alternatives have raised, being one of the most important the two-factor authentication. This kind of mechanisms requires the presentation of two or more authentication factors to verify an identity: something a user knows, something a user has or something a user is.

Two-factor authentication schemes are currently involving mobile devices in the first two aspects ([20]-[25]) since something a user knows can be a One-Time-Password (OTP) sent to the user's mobile phone using SMS or a similar mechanism and something a user has can be the mobile phone itself (in fact, its SIM card). But, although mobile phones and mobile operators are being involved in different identity management mechanisms, the current solution to the problem does not provide significant benefits for operators and does not allow them to innovate in their business model.

Lastly different OTT companies have understood the value of the telephone number as an identity. There are already several communication applications such as WhatsApp or Viber which use the telephone number as the user identity and important players such as Google or Facebook are getting actively involved in the telecommunications scene. But again, this utilization does not imply direct revenues for operators. Trying to overcome this limitation the GSMA (Groupe Speciale Mobile Association) has defined MobileConnect ([26]) to allow mobile users to authenticate through their mobile phone rather than through personal information. This identity management mechanism is based on OpenIDConnect ([9]) and OAuth2 ([27]) standards. Matching users' identity to their mobile phone makes logging easier, safer and more secure, if a mobile phone is lost or stolen the MobileConnect account will be blocked.

As it can be seen, although current identity management mechanisms use to involve the mobile phone inside two factor authentication schemes, previously defined solutions use to focus almost completely on OTPs or on the SIM card, not in the tremendous potential of the telephone number as an identity itself even more if its management is offered as a cloud-service. Furthermore, current approaches do not allow to propose innovative business models for telecommunication operators.

VI. CONCLUSIONS AND FUTURE WORK

This paper proposes a technical solution to provide Identity Management as a Service (IdMaaS) based on the telephone number as the solution for the telecommunication operators to provide mobile and ubiquitous identities to their clients and to fulfil their expectations and needs. This kind of service could surely make easier, more scalable and more secure identity management in contexts such as Cloud Computing, m-Health, Smart places, Big Data or Internet of Things, using telecommunication operators infrastructure, tools and experience dealing with regulations.

A proper deployment of a service like IdMaaS will ensure the relevance of the mobile operators in both, the Internet and telecommunication markets, allowing their reaction and innovation times to be adequate for the present moment and to take advantage of one of their essential values: the telephone number. This work has defined the business model for IdMaaS using the SBMC representation, providing a holistic perspective of the proposed business logic and illustrating the value proposition of the defined service for the different agents participating in the model and their essential relationships.

We are currently helping two European operators to deploy and to operate their first prototypes of the IdMaaS approach.

REFERENCES

[1] J. Buvat, “Innovating the telco business model drivers and emerging trends,” CapGemini, Tech. Rep., 2011.
[2] N. Mpofu and W.J. Staden, "A survey of trust issues constraining the growth of Identity Management-as-a-Service(IdMaaS)", Proceedings of the Information Security Conference for South Africa (ISSA), pp. 1-6, 2014.
[3] N. Katica and A. Tahirovic, “Opportunities for telecom operators in cloud computing business,” Proceedings of the 35th International MIPRO Convention, 2012, pp. 495–500.

[4] A. Oredope, K. Moessner, C. Peoples, and G. Parr, “Deploying cloud services in mobile networks,” Proceedings of the IEEE Science and Information Conference, 2013, pp. 928–933.
[5] A. Stanik, O. Kao, R. Martins, A. Cruz, and D. Tektonidis, “MOBIZZ: Fostering mobile business through enhanced cloud solutions”, Proceedings of the 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2014, pp. 915–922.
[6] A. Vajda, S. Baucke, D. Catrein, C. Curescu, J. Haln, J. Kempf, Y. Lemieux, B. Melander, A. Mohammed, J. Mngs, M. Naslund, A. Shohel, J. Ylitalo, and S. Thorelli, “Cloud computing and telecommunications: Business opportunities, technologies and experimental setup”, Proceedings of the World Telecommunications Congress, 2012, pp. 1–6.
[7] R. Basole and J. Karla, “On the evolution of mobile platform ecosystem structure and strategy,” Business and Information Systems Engineering, vol. 3, no. 5, pp. 313–322, 2011.
[8] C. Battistellaa, K. Coluccib, A. Tonia, and F. Noninoc, “Methodology of business ecosystems network analysis: A case study in telecom italia future centre,” Technological Forecasting and Social Change, vol. 80, no. 6, pp. 1194–1210, 2013.
[9] OpenIDConnect, http://openid.net/connect/ (last visited in May 2015).
[10] “Use Cases and Interactions for Managing Clouds”. DMTF, Tech. rep., 2009.
[11] Comisión del Mercado de las Telecomunicaciones (CMT), " Resolución de 19 de junio de 2008 sobre la conservación de la numeración telefónica", 2009.
[12] Deutsche Bundesnetzagentur (DBNA), "Probleme beim wechsel", 2014.
[13] Federal Communications Comission (FCC), "Keeping your telephone number when you change service provider", 2013.
[14] “SOA Governance Framework”. OSG, Tech. rep., 2009.
[15] J. Gordijn, “The e3-value toolset,” www.e3value.com.
[16] A. Osterwalder and Y. Pigneur, “An e-Business Model Ontology for Modeling e-Business,” Proceedings of the 15th Bled Electronic Commerce Conference, 2002.
[17] O. El Sawy, F. Pereira and E. Fife, "The VISOR Framework: Business Model Definition for New Marketspaces in the Networked Digital Industry", Personal Communication, 2008.
[18] A. Zolnowski, C. Weiss, and T. Bohmann, "Representing Service Business Models with the Service Business Model Canvas -- The Case of a Mobile Payment Service in the Retail Industry", Proceedings of 47th Hawaii International Conference on System Sciences, 2014 , pp. 718-727.
[19] D. Birch, "Identity Is the New Money", London Publishing Partnership , 2014.
[20] D.S. Stienne, N.L. Clarke and P.L. Reynolds, "Novel Single Sign On Architecture Based on the Subscriber Identity Module for Web Services", Advances in Communications, Computing, Networks and Security, vol. 5, pp. 152-161, Lulu.com, 2008.
[21] Do Van Thanh, I. Jrstad, T. Jonvik and Do Van Thuan, "Strong authentication with mobile phone as security token", Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 777-782, 2009.
[22] M. Alzomai and A. Josang, "The Mobile Phone as a Multi OTP Device Using Trusted Computing", Proceedings of the Fourth IEEE International Conference on Network and System Security, pp. 75-82, 2010.
[23] M.H Eldefrawy, K. Alghathbar and M.K. Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones", Proceedings of Eighth International Conference on Information Technology: New Generations, pp. 327-331, 2011.
[24] D. DeFigueiredo, "Included in Your Digital Subscription The Case for Mobile Two-Factor Authentication", IEEE Security & Privacy, vol. 9(5). pp. 81-85, 2011.
[25] M. Xi, U. Topaloglu, T. Powell, C. Peng and J. Bian, "SIM: A smartphone-based identity management framework and its application to Arkansas trauma image repository, Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine, pp. 53-60, 2013.
[26] MobileConnect, http://www.gsma.com/personaldata/mobile-connect (last visited in May 2015).
[27] OAuth, http://oauth.net/ (last visited in May 2015).