Marko Vulić[1], Marko Ranković[2], Vojkan Vasković[3]
[1]Scholar of the Ministry of Education and Science, Faculty of Organizational Sciences, Belgrade
[2]EuroPlanet d.o.o, Belgrade
[3]Belgrade Business School

Identity Management in Modern Business - an Example of Cloud Systems

UDC: 004.42:004.738.52 ; 004.738.5:005.41
DOI: 10.7595/management.fon.2012.0008

The main subject of this paper is Identity management (IDM) in modern business. IDM is one of the biggest challenges on the Internet today, mainly because of the increasing number of services and possible abuse. Digitization of information has greatly facilitated the collection, storing and sharing large amounts of data, but has also contributed to the development of privacy-related risks in the management. IDM concept, model, relationship and system architecture are analyzed in this paper. The paper presents the model's most important elements, shows some of the most important IDM standards and Cloud patterns in the system.

Keywords: Identity management, IdM model, IdM standards, data security, Cloud patterns

1. Introduction

Identity is defined as a set of personal characteristics that make individual a member of the group. Knowing the identity of the human perspective is viewed through a sense of belonging and a sense of rejection. [1]

IDM involves technology, processes, functions and capabilities to manage information on identity, preserving the identity of the entity as well as complexity and security improvements of business applications. IDM is an area that deals with identifying individuals in the system and controls their access to resources within that system, associating user rights and restrictions with the established identity. [2]

The two main components of IDM are: managing "the" identity and managing "by" identity. Management of the identity is the process of issuing and using digital identities and credentials (e.g. username and password) for authentication. Management by identity combines the identity authenticated users with their authorization, in order to grant access to resources. [3]

2. Development and identity management

The identity and the digital identity can be composed of sets of attributes. Sets of attributes are subsets of partial identities at different ages.

Life cycle stages of partial identity are [4]:
- Establishment of partial identity - identity creation or assignment of any person (individual).
- Development of partial identities - use of partial identities by both owner and the others.
- Completion of partial identity - erasing or partial suspension of identity.

All phases described above are relevant for the formation of partial identity.

In most European countries, soon after the birth of a child, unique identifiers are created for the newborn child. One of such identifiers is a birth certificate containing the name, sex, place of birth, and information about its biological parents. This type of registration cannot be prevented by anyone, not even by the parents, because it is in this way that the child officially becomes a citizen of the State.

The next official document is the medical record. It contains the basic information about the child (name, sex, date of birth), records the unique identification number under which the child is registered as a citizen, and

medical data (height, weight, data on how mother gave birth to the child, etc.). As the child grows up over the years, the medical record contains more data. When the child enters kindergarten, the card with personal data of the child is created, as well as with information on the parents. During the child's stay in care, a partial identity of the child is formed, with which it is eventually identified, and starts to live it.

In order to do business with some companies and businesses, parents can assign the rights of their children or allow them to participate in filming commercials. These materials are rarely deleted, hence digital identity only increases and rarely or never decreases. Some of the partial identity can be said not to ever stop even after the death of the individual, because it can be transferred to another person (e.g. social security number). [4] [5]

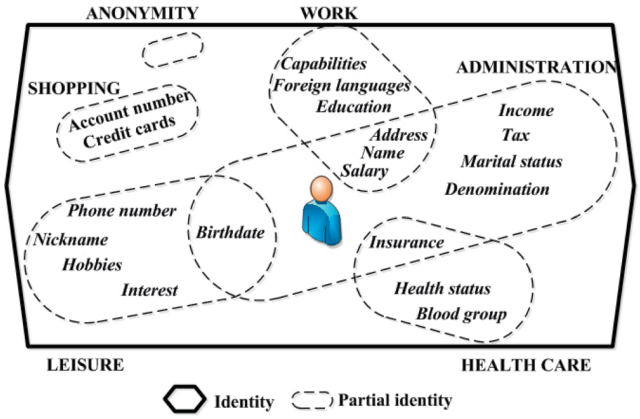


Figure 1 : Partial identities [4]

3. Formal model of the identity management

A formal model of the identity management consists of the following key concepts [6]:

- **Attribute** - An attribute is a feature in connection with an entity (name, date of birth, the generic code, fingerprint, etc.).
- **Identity** - an abstract representation of the entity.
- **Partial identity** - a subset of the attributes associated with entities (name, age, credit card number) that an individual uses to interact with other participants.
- **Identifier** - identifies different persons, places or things. There are two types of identifiers:
  (1) personal identifier - permanent identifiers associated with individual human attributes and the attributes that are difficult to change or that do not change at all (e.g. date of birth, genetic code);
  (2) alias - an identifier associated with the attribute or set of transactions, but without permanent or personal identifiers.
- **Context** – the environment of the entity.

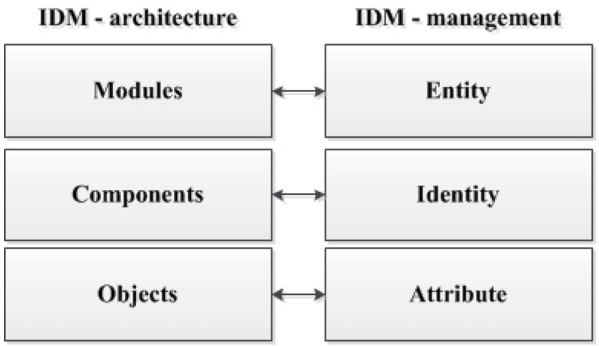


Figure 2: The Relationship between IDM architecture and management [7]

4. Sensitivity of the identity

The perception of the data, i.e., acceptance of any information as sensitive or not sensitive is subjective. The sensitivity of the data is not viewed only from the perspective of privacy, but also through the data security. The European Union has defined a special category of data for which member states are not permitted to process data, except in special circumstances, such as: personal data revealing racial or ethnic origin, political affiliation, religious affiliation, information on health or sex life.

4.1 The sensitivity based on privacy

The attributes that are static over time can be sensitive if they are discovered over and over again in different situations, because this way allows for connecting the related data. The detection of static attribute allows the viewer to connect these situations and gather information that can be used to identify individuals whose attributes are controlled.

There are attributes that the individual cannot determine by himself (e.g. own name), and they can be classified as the initial attributes. They are an inherited attribute values, such as the DNA from the parents or the family name. Partial identity of the child is determined in advance by the parents, because it has not yet been able to just make decisions.

Unsolicited change of attribute values could allow individuals to control their identity, but this is not always possible, as it was shown in the example of static attributes. It means that individual autonomy may be limited to the value of the attribute. Some attributes cannot be detected or changed, if the additional data related to the particular attribute is not discovered. Sometimes it is difficult to put aside the additional information, and it happens that individuals are not able to detect this additional information if they are asked to do so.

An individual can be affected by the value of an attribute or an attribute itself, if it is able to ensure him the position within the group. An individual can remain anonymous as before, or seen in a context in which case his or her privacy may be threatened. For example, the establishment of direct contact by phone or e-mail can be interpreted as a threat to privacy. Even if a direct contact with the individual is not established, negative effects can be achieved through the discrimination.

When it comes to discrimination, only the direct negative effects on individuals are generally taken under consideration, however, these effects can also have an impact on others. If some members of the community get to know some information that is not available to others, they are thus in a better position than others and are able to use this info to discriminate others. [4]

5. Personal data privacy management mechanisms

The best way to protect personal information is to disclose it and make it publically available to a minimum possible amount. Mechanisms that can prevent the misuse of personal data are [4]: managing partial identities, data minimization, executable rules for data processing and operational transparency.

Managing identities and partial protection against a misuse of the same processes are not trivial. Personal information about an individual available on personal computers may be vulnerable if the computers are not used properly, or if the the safety of the system through a number of available patches is not ensured.

Minimization of data does not only include the reduction of the available information, but also reduces the possibility of identifying and connecting to the available data. Communication can be encrypted and redirected to different third-party proxy servers to guarantee anonymity, unless the user does not reveal any additional information.

If personal data leave the environment controlled by the user, the user shall be informed about what will continue to happen with these data. Legislation regulated the ability to cancel the approval of the processing of personal data. The problem can occur if the copies of the data are transferred to other parties and then a total recall is no longer possible.

Transparency is a prerequisite for any kind of control by the user. The information about the parties in the communication process, their reputation, reliability or responsibilities have to be visible, and represent a significant factor before the establishment of a communication relationship.

6. The identity management standards

When defining the requirements in the implementation phase of IDM systems it is necessary that the evaluation of standards be performed. There are different standards for Web services (SOAP, USDL, UDDI), security (SAML, WSS), the biometrics (BioAPI, CBEFF), etc. A number of these standards are described in this paper.

The SAML (Security Access Markup Language) is a standard aimed at implementing solutions that are based on the authentication and authorization in different systems using the XML code. The SAML uses Identity Provider (IdP) and Service Provider (SP) concepts. The SP concept refers to a third party that stores information about or on behalf of another entity. [8] [9]

The Standard SPML (Service Provisioning Markup Language) is designed to manage the process of application of user accounts within the various systems. The XACML (eXtensible Access Control Markup Language) is an XML specification for the transmission and data processing systems used to access information via the Internet.

The WS-Security (Web Security Service) aims to provide support, integration and standardization of different security models, mechanisms and technologies that will enable interoperability of different systems. The XCBF (eXtensible Common Biometric Format) is a standard method of transmission of biometric identification data, such as eye scan or fingerprint.

7. Identity management in cloud

The development of the cloud systems concept viewed from the perspective of different methodological approaches, technology and business (SaaS, cluster systems, high performance), allows for the Cloud IDM to be viewed as a comprehensive approach to solving all the problems in this area, and beyond. Cloud computing is defined as a distributed computer system, the area within which clients have a highly scalable information and communication capacities. [10] The concept of cloud computing is based on virtualization technology, which replaces the physical computing resources. [11]

IDM in the cloud system has to manage: control points, closed dynamic systems, virtual machines or identity services. Cloud implementation is a dynamic system with servers that run or are canceled, IP addresses are dynamically assigned and change the services that are started, shut down or restarted. When the device or service shuts down, IDM receives information so that it cancells the access to instances. IDM will keep the details of acces to instances stored until the moment when it becomes active again, and then activate the authentication mechanism. Until the access is reactivated, the access details must be stored and kept in an appropriate and clearly defined way. [8] [12]

Cloud systems require a change of approach, compared to the classic IDM, especially in the part related to enabling or cancellation of access, synchronization, granting privileges, identity lifecycle management, etc. So far the only way to ensure the security of sensitive data in the cloud is encryption. A most common solution for data encryption is the PGP (Pretty Good Privacy) encryption product, which offers encryption at any place where data can reside. The advantage of the PGP encryption is centralized product management. This approach enables centralized care of the encryption keys. [13]

The cloud IDM systems distinguish three patterns [14]: trusted IDM pattern, external pattern and interoperable IDM pattern.

Trusted IDM pattern is designed for small or private Cloud systems that require a high level of safety. The level of scalability is extremely low. The main feature of this concept is that the authentication is always implemented in the firewall. Authentication details are forwarded to the IDM components, which encrypts the information and continue through the safe channel of communication, forwards the information to the entity

that will implement authentication. IDM is independent of authentication mechanism, hence the implementation and integration of this pattern are fast and efficient.

After successful user authentication, by any mechanism of the authentication cloud system, the other servers, participants in the system, "trust" the authenticated user. Attributes of users can be shared through concepts such as SAML, while the authorization itself may be implemented using XACML-a. An example is shown in Figure 3.

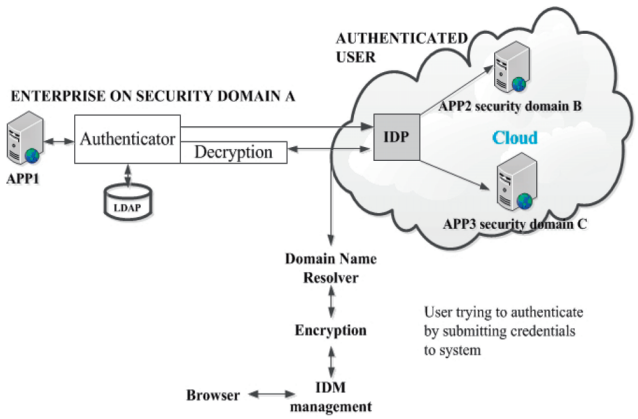


Figure 3: Trusted IDM pattern [14]

External IDM pattern is similar to the previous one, except that the authentication details are directly forwarded to the entity that will implement the authentication. Authentication details can be obtained using a different browser, a protected channel provided by SSL (Secure Sockets Layer).

The External pattern is intended for public cloud systems. IDM is particularly aimed at resolving issues and initiating the domain authentication process by the entity that will implement authentication. The architectural solution is adopted by Ping Identity, where the domain issue is resolved by reference to the appropriate table of valid users, which is always updated. An example is shown in Figure 4.

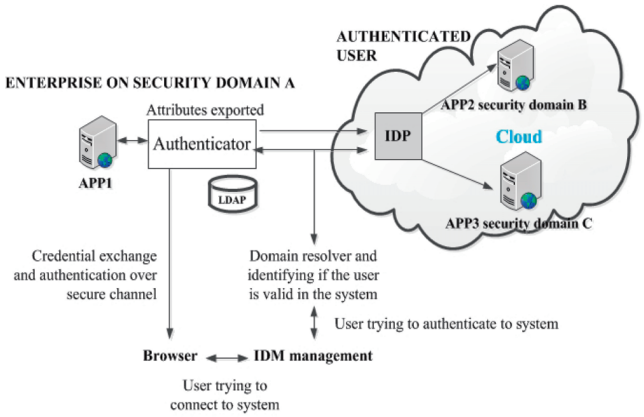


Figure 4: External IDM [14]

Interoperable IDM pattern is used during the implementation of the Cloud2Cloud communication, using OpenID and OAuth. OpenID is an open and decentralized standard for user authentication and access control, which allows users to access various services or servers with the same digital identity. OAuth is an open protocol that allows the user to assign privileges to another user access to the site service provider, without sharing authentication details. This is extremely useful for e-business, where different service providers offer their products / services at one place.

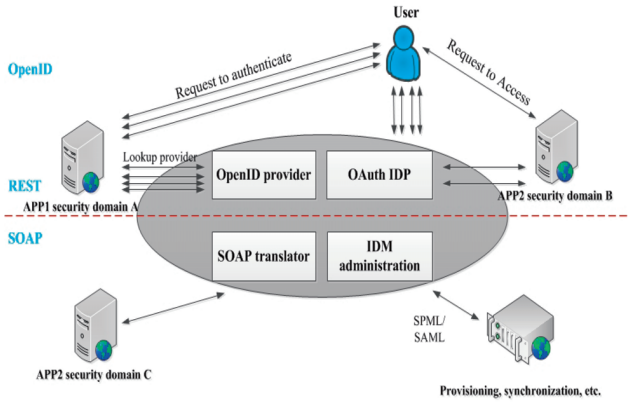


Figure 5: Interoperable IDM [14]

Comparative review of three IDM Cloud patterns is shown in Table 1:

Table 1. Comparative review of the IDM patterns [14]

	Trusted IDM pattern	**External IDM pattern**	**Interoperable IDM pattern**
Security	Very secure	Submitted to IDP network	Depends on authentication mechanism
Interoperability	Interoperable	Interoperable	Interoperable
Type of cloud	Private cloud	Public cloud	Public cloud with multiple technologies
Speed of implementation	Very fast	Fast	Speed depends on the number of claims
Scalability	Not scalable easily	Not scalable easily	Scalable
Example	Google App Engine	Ping identity	Proposed design

Conslusion

This paper describes the basics of IDM systems, from the general terms, to the rules and standards for IDM. The goal of the paper is to present the concept of digital identity, as the basis for implementing a wide range of services in the areas of business on the Internet. As a concept, IDM has been present for a long time, but the rapid development of electronic commerce expanded the possibilities of application of the concept, hence the research in this area are of significant value for both the area of e-business, and for the presence on the Internet in general. The Internet environment and a host of services that are available to users have led to an increased need to pay the digital identity of the entity major attention. Digital identity should be managed in a strategically planned, business-justifiable and controlled manner.

IDM entails a number of security issues. At the time of creating a digital identity, or use of specific solutions for IDM, opportunities arise for performing various illegal and malicious activities, primarily in the form of theft or unauthorized taking of digital identities. The main task of IDM is to ensure that the real identity is used in the right context at the right time.

The use of the cloud system in making the IDM concept should meet the requirements set by the cloud system, as well as fulfill the requirements for future system enhancements. The use of this approach will make the IDM concept simple, fast and efficient to use in relation to large systems, as the activities IDM system will be implemented in the cloud. The description of the IDM gives the advantages and disadvantages of this concept, while the description of the elements of IDM and methodology for implementing such a system outlines the concept, which should serve as basis for further research in this area.

REFERENCES

[1] Windley, P.J. Digital Identity, O'Reilly Media, Inc., Ch2, 2005.
[2] Harrop, M. Identity Management, The Cottingham Group, ETSI Security Workshop, 2009.
[3] Identity Management, The Government of the Hong Kong Special Administrative Region, 2008.
[4] Hansena, M., Pfitzmannb, A. and Steinbrecherb, S. Identity management throughout one's whole life, Information security technical report 13, pp. 83-94, 2008.
[5] Chawdhry, P. and Vakalis, I. Use of ePassport for Identity Management in Network-Based Citizen-Life Processes, Editor(s): Bezzi, M., Duquenoy, P., FischerHubner, S., Hansen, M. and Zhang, G., Privacy and Identity Management for Life, Book Series: IFIP Advances in Information and Communication Technology, Vol. 320, pp. 122-133, 2010.
[6] Glasser, U. and Vajihollahi, M. Identity Management Architecture, Simon Fraser University, Canada, 2008.
[7] Jin, Z.P., Xu, J., Xu, M. and Zheng, N. An Attribute-Oriented Model for Identity Management, International Conference on e-Education, e-Business, e-Management and e-Learning, 2010.
[8] Celesti, A., Tusa, F., Villari, M. and Puliafito, A. Security and cloud computing: Intercloud identity management infrastructure, 19th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2010, Larissa, pp. 263-265, 28-30 June 2010.
[9] Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Ben Othmane, L. and Lilien, L. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing, 29th IEEE Symposium on Reliable Distributed Systems 2010, New Delhi, pp. 177-183, 31Oct-3Nov 2010.
[10] Srinivasa, R., Nageswara, R. and Kusuma, K. Cloud Computing: An overview, Journal of Theoretical and applied Information Technology, Vol. 9, No. 1, pp. 71-76, 2009.
[11] di Costanzo, A., de Assuncao, M.Di. and Buyya, R. Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure, IEEE Internet Computing, IEEE Computer Society, pp. 24-33, 2009.
[12] Sanchez, R., Almenares, F., Arias, P., Diaz-Sanchez, D. and Marin, A. Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing, IEEE Transactions On Consumer Electronics, Vol. 58, Issue 1, pp. 95-103, 2012.
[13] Vučinić, V. Sigurnost u oblacima, Internet ogledalo, No. 126-127, pp. 40-43, 2011.
[14] Gopalakrishnan, A. Cloud Computing Identity Management, SETLabs Briefings, Vol. 7, No. 7, pp. 45-53, 2009.

Receieved: February 2012.
Accepted: May 2012.

About the Author

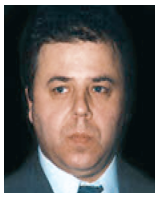
Marko Vulić
Scholar of the Ministry of Education and Science, Faculty of Organizational Sciences, Belgrade
e-mail: marko@elab.rs

Marko Vulić was born in Belgrade, in 1985. He completed his graduate and master studies at the Faculty of Organizational Sciences in Belgrade. Currently, he is a second-year student at the doctoral studies course at the Faculty of Organizational sciences, and a scholar and member of the Ministry of Science and Education of the Republic of Serbia project team. His scientific interest areas are as follows: electronic business, mobile business, the Internet marketing, e-education, e-banking, CRM.

Marko Ranković
EuroPlanet d.o.o
e-mail: mrankovic@euronetworldwide.com

The author's professional interest areas are in project management in the fields of financial services, scientific and research work in the area of electronic financial transaction processing, including methods and techniques of processing, processor organizational structure, the architecture of the transaction processing platform, models and techniques of card payment system protection. Marko Ranković is currently employed as a Project Manager in the EuroPlanet Company.

Vojkan Vasković
Belgrade Business School
e-mail: vaskovic@bvcom.net



Vojkan Vasković was born in Kragujevac, in 1951. He completed his graduate and postgraduate (master) studies at the Faculty of Organizational Sciences, Belgrade, where he also took his PhD degree. At present he teaches at the Belgrade Business School. His professional interest areas are the following: electronic business, e-banking, Internet technologies, mobile technologies, e-Government.