Management and Innovation Models for Digital Identity in Public Sector

Nunzio Casalino[1], Marisa Ciarlo[2], Simone Sassetti[3] and Mattia Panico[4]
[1]*LUISS Business School, Viale Pola 12, 00198 Rome, Italy*
[2]*Invitalia, Via Calabria, 46, 00187 Rome, Italy*
[3]*Sapienza Università di Roma, Via del Castro Laurenziano 9, 00161 Rome, Italy*
[4]*Unfraud, Via Aurelio Saliceti, 10, 00153, Rome, Italy*

Keywords: Business Information Systems, Automation, Innovation, Change Management, Identity Management, Authentication, e-Learning, Security, ICT Adoption, IAM, CIP.

Abstract: This paper is aimed at analysing the international framework, both European and Italian, for the innovative eID operating models, to identify the guidelines to follow for a correct identification of the operational requirements, of the solutions and of the services offered by the model DIMIM – Digital Identity Management and Innovation Model. After the framework' analysis, we will go through the definition of a new set of strategic guidelines customised on to the most interesting and relevant sectors identified by the DIMIM. This step will consist in the highlighting, through to the help of tools such as the SWOT analysis and the priority matrix, of the main constraints and opportunities emerging in the implementation process of the eID operational models. The paper at issue is also aimed at identifying a universal, solid and multichannel authentication system, the "IAM", which will provide each individual with a set of solid and safe digital credentials allowing the access to all the available services, promoting the creation of value-added services.

1 INTRODUCTION

The personal identity is defined as "The set of essential and unique personal characteristics which allow to identify a single individual". In Italy, and in all other European countries, eID is supported by local Government. The implementation of eID support systems is related to the need to dematerialize procedures and documents and to guarantee the access to eGoverment services, eHealth services and to all the residual digital services provided by both public and private authorized entities.

The access to these services is allowed only after an "indisputable identification", inasmuch is necessary for the "user", not only to be identified, but also to get an authentication from a third authorized individual (that could be a third party or the Government entities themselves).

Nowadays, in Italy, eID is a work-in-progress (only few services are supplied through eID), while in other countries, first above all Estonia, eServices are a reality. While the current Italian system still requires time to adjust, in the countries already interested by this revolution, processes and procedures are set and fixed. The first authentication procedure is the most delicate and it often involves a double step authentication and check in governmental databases. The lack of a framework can lead to misuse or, even worse, abuse of eServices because of a poor identification procedure (e.g. one step authentication).

Italian government recently took over the problem and through the "Decree 2.0"[1] clarifies that the first step is the unification of the actual paper-ID card and the social security number, but the road to the proper implementation is long and rocky.

The paper focuses on the identification of the most suitable industries and areas from where start to disrupt the actual schemes and limits of eID. It does not only address the Italian situation (despite clear references to it) but the analysis is supposed to be useful to any country and administration that find

[1] www.mise.gov.it

Casalino, N., Ciarlo, M., Sassetti, S. and Panico, M.
Management and Innovation Models for Digital Identity in Public Sector.
DOI: 10.5220/0006279202250232
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 1*, pages 225-232
ISBN: 978-989-758-247-9

itself in the same condition. Following, some of the most important areas of intervention from a strict governmental point of view[2].

1.1 e-Health

The idea to supply health services (records, prescription, personal history) is something governments are trying to reach to have more control on local infrastructures, to rationalize and better assign public funds. Estonia is a pioneer in eHealth services and it represents the best case concerning digital services and eID. In Estonia, all persons entitled to the NHS, have a national health record to which they have access through credential linked to the eID. Another revolution they introduced regards the doctor-patient relation, and is called ePrescription platform. Through this, all communications, electronic prescriptions and inquiries between them will take place in a secure channel, accessed through credentials. Is it clear how much Estonia invested in these services and how much people believed in these projects.

1.2 e-Government

EGovernment will make all government services available online to citizens, without necessarily appear in person, but using the credentials associated with eID. In this way, the life of the citizen 2.0, would be greatly simplified, from any point of view, but ensure a good level of service in a country such Italy (90 million people), needs the highest level of effort from all public actors and citizens, too. Also in this scenario, Estonia is a successful case that for 10 years now, has provided eGovernment services to its citizens. Italy is trying to keep pace with the most digitalized countries and recently introduces SPID[3] (Digital Identity Public System), but public and administrative deficiencies slow down to innovation process.

2 SECURITY AND EID

One of the biggest challenges that Italy must face, is the issue of system security. It is of primary importance for the proper spreading of eID as Italians already have a strong aversion to technology. EGovernment services are little used while eHealth services are not yet fully available (but is a matter of big interest).

Given the lack of confidence that Italians have towards the digital, it is necessary to provide a lot of information and data about the technologies that are being introduced. Allowing individuals to really understand the technology they are going to use, it is more probable to persuade them and raise the tech adoption rate. Some of the solutions comprehend courses, seminars, free meetings with industry experts, as well as to illustrate, even technically, the functioning of an eID.

The main point remains security: the Government, to succeed in the eID diffusion, must inform citizens about the systems used and the security precautionary measures taken.

2.1 EID Reference Context and Innovative Operative Models

The need to provide tools for the reliable identification of individuals both in the physical and in the virtual world is more and more crucial to eID systems: this will ensure an increase of quality life and better services both from privates and Public Administrations. All this must be compliant with privacy regulations, to protect citizens' privacy and ensure there are no data leaks. In this sense is useful to employ two-way authentication techniques, through a certificate: it is a form of guarantee that the information sent have not been modified or altered during the transfer[4].

The term Identity Management addresses the set of integrated technology systems and the synergy of services, products, policies, and processes that allow both public and private bodies to facilitate - and at the same time control – users' accesses and personal data. An Identity Management (IdM – See Figure 1) is the convergence of different products, previously separated, which now create a unique system and single solution to a long series of issues: they represent a solid security infrastructure, based on a strict authentication framework that allows the adoption of rigorous security policies to control access and to ensure privacy.

These systems can be exploded into layers, where each layer provides services to the next level.

[2] http://www.sviluppoeconomico.gov.it

[3] www.spid.gov.it

[4] https://www.globalsign.com/en/

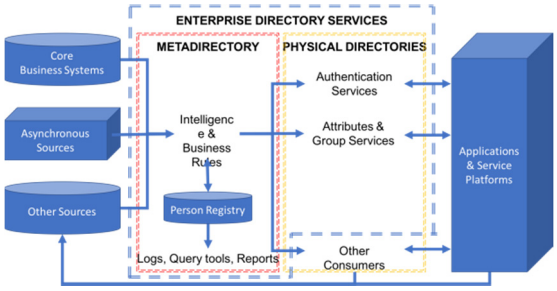

Figure 1: Identity Management Architecture (IdM).

The more users feel safe in terms of security and data privacy, the more he will benefit from the services supplied online by public and private entities. For this reason, the introduction of an eID that uniquely identifies the user and allows him to safely operate in the digital world, will positively influence the behaviours and help the spread of online services for citizens.

The diffusion of IdM systems, pushed companies to encrypt data traveling on the web: this was the beginning of the companies that have made this type of activity their core business, the Certification Authorities: public or private, authorized to issue a digital certificate through a procedure that follows international standards and comply with European (and national) legislation on cyber security. Once issued, the certificate will be used to encrypt and decrypt data (asymmetric and public key)[5].

2.2 Applicability of the Model in Social Networks

Another interesting area, related to the Model presented in this paper, is the Strong Authentication as part of the social network area. It is identified as an important element to consider, due to the pervasiveness of the social networks in the life of almost every citizen. Therefore, this topic must be consistently covered, to have a clear view of all possible scenarios to consider while building a system. The advent of the web, while it has made noticeable improvements in the daily life of each of us, it also triggered the development of new opportunities for fraudsters and criminals: the extensive use of electronic mail, digital monetary transactions, and social networks, has resulted in an increase of the circulation of personal data, making citizens more and more exposed to the risk of identity theft, a renown fraudulent scheme where the stolen ID is afterward exploited for criminal intents.

A long series of surveys have been analysed to investigate this phenomenon and consider the fact that the population has different levels of knowledge and therefore of interaction with internet, that depends on different variables such as age or profession. The surveys have been analysed to learn about the use of ID on the web and computing habits, with attention to the awareness about issues as data theft, ID theft, data leaks and dissemination.

The opinion that prevails from the surveys, especially from young citizens, is that risks associated with ID theft are low, despite their high frequency and propensity in disclosing their personal information online. There is also not enough sensitivity about Information Security in general: some behaviours are more common - the installation of antivirus or the use of different and personalized passwords for different services or sites - some are less common - as reading the term and conditions or the incognito navigation.

If it is true that only 12% of internet users claims to have suffered or be aware of cases of ID theft, it is also true that it is the lack of knowledge that causes the shortage of protection systems: in this sense, the raise of awareness is fundamental and plays an important role in digital security.

Young people access to the Internet mainly from the smartphone (63.2%), although even the laptop and desktop computers remain frequently used tools (respectively 57.4% and 43.9% of cases). The devices are generally shared with other family members, friends, or with the entire household (this is the typical case of desktop computers, laptops and notebooks), while they remain of exclusive use in case of smartphones or gaming consoles. There is also a clear tendency gender: except for laptops and tablets, which are used with equal frequency by both males and females, game consoles, computers and even smartphones remain mostly used by males.

The activities are numerous and diversified by purpose and mode of access to the network: over 90% of users access online to surf the Internet, to access multimedia content and use social networks, both from PC and from smartphones; electronic mail is also frequently used, mostly from desktop computers, while applications download (77% of cases) is largely tied to the possession of a tablet or a smartphone. Only 50% of users download multimedia content from the Internet, or make purchases through direct channels and through purchasing groups: in all these cases always prevails the use of a PC.

[5] https://www.firma.infocert.it

2.3 EID and Blockchain

Blockchain[6] is a technology potentially applicable to revolutionize and have a huge impact on almost any sector. The Blockchain intentionally lacks of a centralized management system, shortening the intermediaries chain, allowing the sending of data quickly, safely and at a low cost. It Blockchain assumes an important role in many sectors but it may be considered virtually opposed to the concept of the eID. This because Blockchain is the result of a long period of deregulation that culminated with the creation of a system that completely cuts-off any central system from the equation.

The actors to be identified and certified should be recognised and labelled as "trusted" by an external party: what happens with Blockchain is that these entities correspond. As a Digital Identity implies citizenship, duties and rights related to the country of belonging, it naturally follows that the issuer should be anyone else but the Government.

For this reason, the Innovation Model here considered, will not further comprehend the Blockchain in the feasible scenarios considered.

3 MAIN REFERENCE INDUSTRIES IDENTIFIED

To date, the Digital Signature is used to identify both the author and the integrity of an electronic document, while it is still difficult to guarantee the identity of an individual connected through the network. In fact, if in daily practices each subject is able to prove its own identity, this is still an obstacle if the identification has to be done on-line or without the physical presence of the individual. From these considerations, according to the latest EU guidelines transposed at national level with the constitution of the Italian Digital Agenda, this document aims to:

- Define a universal and robust authentication system, IAM, that is also multi-channel and federated with the main operators in the sector, to assign secure digital credentials to each individual and allow the access to all available services.
- Design a value-added service called CIP that, according to the cloud computing model, will provide users with an online personal data repository, always accessible from anywhere and anytime. The CIP will fully accomplish to the Digital Identity concept. The CIP will be able to collect all digital documents from a user automatically, even from different sources, and provide value-added services and information.

3.1 Methodology Used to Identify Priority Sectors

The identification of strategic guidelines has been realized using a matrix that, for the application fields of the project, defines the main hypothetic areas to which the project can be applied.

The matrix used defines for each macro-sector, industry and business-sector, the potential revenues, complexities and risks arising from the introduction of the Digital Identity. International best practices (e.g. Estonia, New Zealand), as well as specific studies (e.g. The value of our digital identity, BCG), have been taken into account to enhance the variables considered in the study.

The matrix has been built on the basis of a multitude of variables, able to identify the data to analyse for the realization of the project. The field analysis on market areas, identified more than 5 macro-sectors, that cover more than 60% of the total active enterprises in Italy (>3 million companies). It is important to take into account that the majority of the industries not in the target are, for the most part (about 1.7 million of enterprises), firms in the agricultural sector, considered of marginal importance for the project. The 5 macro-sectors have been subdivided into 22 smaller sectors, that is more than 80 areas in total. A further segmentation has been performed, where appropriate, to better specify the unit reference, as happened with the banking and telecommunication industries, where big enterprises have been distinguished by small/medium ones.

- **Macro-sector:** Main reference industries (Public Administration, Financial Services, TLCs, Energy, Transportation and other services, IT industry);
- **Sector:** Main sectors considered for each Macro-sector, (e.g. in the Financial Services Macro-sector: Banks, Insurance companies, Financial institutions, and so on). The majority of sectors have been considered of interest for the offer examined;
- **Areas/Potentially interested Bodies:** for each sector of interest, have been considered the main bodies and the most interesting companies.

[6] www.blockchain.com

A long series of numerous variables have been used to develop the matrix.

Qualitative evaluation elements:

- **Rational business**: for each area have been evaluated the main benefits that the Digital Identity can bring in the field and/or the reasons that can push companies/bodies to employ IdPs to supply their services;
- **Pricing Model**: have been considered different pricing policies applicable to the context considered based on the assessment of the potential profitability of the sector (per user fee, per-transaction fee, flat fee, initial investment, free trials and so on);
- **National / International Experiences**: Details of any similar experience in Italy or in the world

Potential Business Revenues evaluation elements:

- **Potential Diffusion (DIFF)**: it indicates the diffusion chance of the IdPs in the reference sector, taking into account the high number of businesses, the number of potential users, the amplitude of the reference area and the ease of spread, based on three values (High = x million users; Average = x00.000 users; Low = limited user);
- **Need for Digital Identity (IdPs)**: it indicates the propensity to digital services in the industry and if is required or requested the adoption of IdPs in the reference sector, based on three values (High = The business sector has strong need IdP mechanisms; Middle = There may be opportunity for IdP introduction alternatively to other instruments used (e.g. PIN); Low = little oriented sector to digital and / or IdPs does not apply to the reference sector or there can be used other already established instruments in the area);
- **Business Profitability (REV)**: it indicates the potential profitability of the sector, taking into account the pricing model applicable, the business rationale and users' willingness to pay, based on three values (High, Medium, Low).

Target Market evaluation elements:

- **Competitors Presence (COMP)**: it indicates the presence of competitors in the sector, based on three values (High = High concentration of competitors in the sector; Medium = not significant presence of competitors in the sector; Low = Sector with few or no competitors);
- **Saturated Market (SAT)**: it indicates whether the specific sector of the market is already addressed with reference to the introduction of IdP tools and / or have already introduced alternative tools, based on two values (values: 2 = YES / NO = 1).

Complexity/Risk evaluation elements:

- **Potential costs of planting and marketing (COST)**: it indicates the order of magnitude of the cost needed for the implementation and / or the diffusion of IdPs in the sector, both in terms of product customization and of market distribution, based on three values (High >= € 500,000; Low <= € 100 000);
- **Complexity / Risk (RISK)**: indicates the level of complexity and the degree of risk to face for the diffusion of IdPs in the sector, based on three values (High = High expected level of complexity and risk; Medium = Average complexity and risk values; = Low risk and limited complexity).

Further evaluation elements:

- **Functional Expertise (ExFUN)**: it indicates the level of practical and business expertise needed to develop / promote the product in the sector, based on three values (High = High expected level of expertise and experience; Medium = Competence and experience in average values; Low = Lower need for knowledge of the sector from a functional and business point of view);
- **Technical expertise (Extec)**: it indicates the level of technical and specific expertise needed in the sector, based on three values (High = High expected level of expertise and technical experience; Medium = Average values of competence and experience; Low = Lower need of specific and technical knowledge).

4 MAJOR INTEREST AREAS AND SECTORS FOR DIGITAL IDENTITY (IDP) AND CIP

The choice of priorities has been defined to ease the spreading of the Digital Identity (eID), according to a series of factors:

- Rapid promoting in most “advanced” sectors;
- Attacking of most profitable areas and companies;
- Prioritizing short and medium term revenue policies;
- The trade-off between complexity / risk and market potential;
- The low complexity of competitors and the reference market maturity.

Some areas (INAIL, Energy, Cards, Lottery, Transportation, SMEs) have a big potential in the Medium and Long term, but it will be necessary a specific study to evaluate the opportunity to develop the ID in the national specific context[7]. The synthesis of the result of the matrix can be depicted in the image in the next page (Figure 2). It defines four quadrants, where the top-right area is the most interesting (high potential revenues and low risks) and the lower-left quadrant represents the no-interest area. The other two parts show the areas to be evaluated and explored on an opportunistic basis.

Short term interest areas to promote are:

- Banking and Payment Institutions;
- Life insurance companies:
- Telecommunications Companies;
- Ecommerce/Merchants;
- INPS (National Institute of Social Security)[8];
- Car rental companies;
- Pharmaceutical retail services.

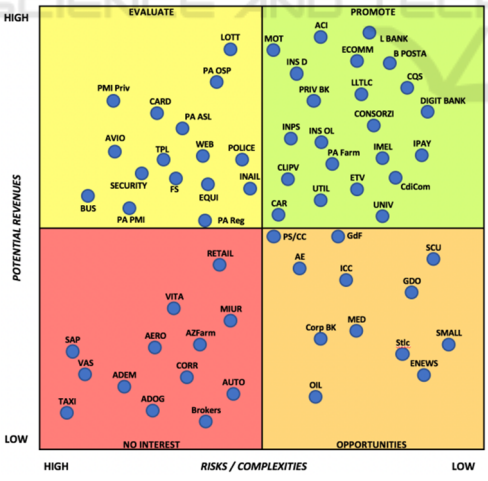

Figure 2: Evaluation Matrix.

- Private clinics and diagnostic centres;
- ACI / DMV, Universities.

No-interest areas to consider with low priority, are defined by the following traits:

- Need for substantial investments in terms of marketing and market complexity;
- Low profitability and high market saturation;
- Presence of established competitors.

Included in this area can be founded:

- Pharmaceutical Companies;
- Ministry of Education;
- Research Institutions;
- Investment Bank, SGR;
- Contact Centres;
- Automotive / TAXI, Delivery / Post;
- Life Insurance branch, Brokers;
- Retail (apparel, food & drink, decor).

5 CONSTRAINTS AND OPPORTUNITIES FOR AN OPERATIONAL MODEL

Within the development of a Digital Society, we should consider both the actions that can contribute to the proactive participation to the European Single Market and the interventions to promote the digital economy. Priorities are the interventions with a focus on the digital market, as the support for the e-Commerce diffusion (both for the demand and for the supply side), the organizational changes in companies for e-business, the ICT vouchers for the introduction of technologies in businesses, the support for web start-ups as part of more general policies for start-ups.

Today we are facing a new kind of "digital enterprise", a kind of enterprise that is unfortunately not classified by companies’ registration offices or by other national bodies. Moreover, they often do not have prerequisites to access public incentives. Particularly important to fasten the digitization of the economy, are the creation of a regulatory framework and the diffusion of effective tools for electronic invoicing (e-Invoicing), electronic payments (e-Payment) and the electronic procurement (e-Procurement). Policies for digital growth, in terms of Research & Innovation and digital market development, require a qualitative leap both for the Public Administrations and for the private business realities. Both should evolve from players that design and provide solutions to proactive partners that make all their assets available, collaborating for the co-design and co-production of solutions and services,

[7] http://www.agendadigitale.eu/identita-digitale

[8] https://www.inps.it/portale/default.aspx?NewsId=3154

thanks to the enabling role of ICT. Institutions and private partners must lead the change considering the interdependent relationship between technology, industry and society, so that the industry can respond to technological progress ensuring all citizens have access to new digital services.

Regarding the areas of intervention identified, the existing synergies between them act on different levels of supply and demand, relating both to the public sector and, indirectly, to the private sector too (through enhancement of public information, open data, information security, digital identities, smart communities, digital skills development).

The development of the digital administration and economy, is not possible without an effective securitisation of networks and information, fundamental to obtain citizens' trust towards the online services provided. This condition is necessary to allow people to autonomously operate and use the services, raising the efficiency of the entire economical system.

The recent and increasing attack rate, both on private and governmental IT systems, injected new life into this topic, especially when key or critical infrastructures are the target of such assaults, such as energy distribution facilities, the banking system and financial institutions.

6 SWOT ANALYSIS

That of digital growth is a cross-cutting topic to any area, from for tourism and culture, to craftsmanship and digital manufacturing. It is very varied in terms of possibilities, ranging from simple "online sales" of products, the complete change of business models, the opening of new markets, to the "makers" movement. The completion of national and international strategies related to ICT as KET in Research & Innovation, is fundamental when designing new policies for digital growth through research and innovation. Such policies should aim at creating a digital ecosystem that is dynamic, competitive, productive, friendly, safe and full of opportunities. This includes initiatives related to the "Living Labs", the research on big data, the theme of entrepreneurial discovery, the development of pre-commercial procurement and the promotion of public-private partnerships, the development of advanced technologies needed for smart communities. A further priority should be the "Entrepreneurial discovery" intended as the process which encourages companies, research centres and universities to work together to identify the most promising areas, but also the weak points that may hinder innovation. ICT and digital ecosystem are key enabling elements for the full development of the potential of entrepreneurial discovery.

It is crucial in this scenario, to be aware that technology evolves exponentially, and social relationships too, but there is need of widespread skills and increasingly powerful technological infrastructure not losing competitiveness and socio-economic growth capacity. Therefore, it is needed the identification of a strategy to recognise strengths and weaknesses, opportunities and threats, which can be synthetically represented in the SWOT analysis that follows.

6.1 Exponential Technology Growth

The technological growth, does not only represents an instrumental element for any country, but it is also the biggest strength to exploit to make eID spread. The creation on a digitalization path, as well as a regulatory framework and a system of priorities is, as previously shown, essential. All progresses should be of course measurable and executed rapidly, to better take advantage of the technology growth. The increase of internet use among citizens, will end the Digital Divide and open to innovations (e.g. Smart Cities).

6.2 Need for Infrastructures and Skills

A digital revolution, can be pursued only when can rely on an adequate infrastructure system and widespread skills. The need of huge investments, both in human and financial capital, represents a weakness to which should be given attention.

All delivery, rollout and dissemination mechanisms, must be set and perfectly working to avoid the risk of duplication and misalignment of confidential information.

6.3 Exploit the Actual Scenario and Social Economic Capacity

The traction of eID can be exploited to start a structured collaboration among all public actors, creating a well-established, clear and common strategy. The rollout of new services, will enable mobile payment, remote access, loyalty programs and peer-to-peer appliances, all based on the attributes contained in CIP. Despite the scenario has good perspective, threats coming from the scarce utilization of economies of scale and synergies (mainly due to fragmentation of resources and

investment duplications), can mine eID. Moreover, must be avoided that third parties without specific characteristics (e.g. Banks) can become IdPs and use their customer base to force government to authorize them. The cost of control, conversion and maintenance of the eID system is high, also in terms of human effort. Last, data leak is a problem that has to be faced with priority in respect to other.

7 CONCLUSIONS

The unique and peculiar characteristics of Italy, which are due to the territorial distribution, the type of culture and demographic factors, equally contribute to the slowing of the large-scale spread of new technologies and digital in general. These considerations can be extended to other countries, too: the uniqueness that characterizes each Nation, is one of the reason why is so difficult to create a unique framework regarding eID. In many areas and sectors, citizens do not even feel the need for a Digital Identity, stressing that the main limitations are coming from culture and mentality. Italy is trying to leverage the advantages that Digital Identity can bring in the life of "Citizen 2.0", but what is needed to make tangible progresses, is a simplification both from the technical and political point of view. Given that these obstacles to eID are real and widespread, the Innovation Model proposed in this paper, considering the Italian specific features, tries to depict a possible solution to all those countries that find themselves in the same conditions, and offers effective tools to adequately address the Digital Identity innovation and pick suitable sectors and areas of application.

REFERENCES

Butler, J., 1999. A practical model for technology and innovation management, Proceedings of the Portland International Conference on Management of Engineering and Technology, PICMET, pp.103-105.

Cardinal, L.B., Alessandri, T.M., Turner, S.F., 2001. Knowledge modifiability, resources, and science-based innovation, Journal of Knowledge Management, Vol. 5, No. 2, pp.195-204.

Carneiro, A., 2000. How does knowledge management influence innovation and competitiveness? Journal of Knowledge Management, Vol. 4, No. 2, pp.87-98.

Casalino, N., 2009. An Innovative Model of Transnational Learning Environment for European Senior Civil Servants - Organizational Aspects and Governance, proceedings 11th International Conference on Enterprise Information Systems - ICEIS, Milan, Italy, INSTICC, pp.148-153.

Casalino, N., D'Atri, A., Manev, L., 2007. A quality management training system on ISO standards for enhancing competitiveness of SMEs, Proc. 9th International Conference on Enterprise Information Systems - ICEIS 2007, June 12-16 2007, Funchal, Madeira - Portugal, INSTICC, pp. 229-235.

Casalino, N., Di Persio, F., 2004. Integrating medical services, training and education: the Hermes project platform, in ATL - Advanced Technology for Learning Journal, ACTA Press Anaheim - Calgary - Zurich, Vol. 1, Issue 2, pp.71-80.

Chesbrough, H., 2003. The New Business Logic of Open Innovation, Strategy & Innovation, 1, pp.11-15.

De Marco, M., 2004. Le metodologie di sviluppo dei sistemi informativi, Franco Angeli, Milan.

Gatti, M., 2000. Organizational innovation and virtual institutes, Journal of Knowledge Management, Vol. 3, No. 1, pp.75-83.

Johannessen, J.A., Olsen, B., Olaisen, J., 1999. Aspects of innovation theory based on knowledge-management, International Journal of Information Management, Vol. 19, No. 2, April, pp.121-139.

Kaplan, S.M., 1999. Discontinuous innovation and the growth paradox, Strategy and Leadership, March-April, pp.16-21.

Kessler, E.H., Chakrabarti, A.K., 1997. Methods for improving the quality of new product innovations, Proceedings of the Portland International Conference on Management and Technology, PICMET, pp.405-408.