université angers

13, allée François Mitterrand
BP 13633
49100 ANGERS Cedex 01
Tél. : +33 (0) 2 41 96 21 06

Web : http://www.univ-angers.fr/granem

Granem
Groupe de Recherche ANgevin
en Economie et Management
UMR-MA n°49

Adoption of new identity services: Proposition of a conceptual model based on TAM, DOI and perceived risks

Caroline Lancelot Miltgen
GRANEM, Université d'Angers

Juillet 2010

Document de travail du GRANEM n° 2010-01-023

AGRO CAMPUS OUEST

Adoption of new identity-based services: Proposition of a conceptual model on TAM, DOI and perceived risks

Caroline Lancelot Miltgen

Document de travail du GRANEM n° 2010-01-023
Juillet 2010
Classification JEL : M15, M31, M14.

Mots-clés : vie privée, données personnelles, identification électronique, modèle TAM, diffusion des innovations.
Keywords : Personal data, electronic identification, consumer privacy concern, TAM, diffusion of innovation.

Résumé : Avec l'introduction des médias numériques, des réseaux et le développement de la société de l'information, la gestion de l'identité est devenue un enjeu majeur aux implications importantes. La gestion des identités est une stratégie complexe dans laquelle les individus, les organisations et les gouvernements s'engagent mutuellement. Dans tous les secteurs de l'économie, il devient nécessaire de bénéficier de moyens efficaces et sécurisés de garantir l'identité des personnes souhaitant accéder à un service, et ce de manière électronique. L'identification est le processus par lequel une entité est reconnue et son identité est clairement établie. Parmi les technologies actuelles en matière d'identification électronique, la RFID ou la biométrie sont parmi les plus connues. Les recherches menées sur le sujet, notamment dans les domaines technologique, économique, social et légal ont apporté des éléments importants pour le développement de ces techniques. Un aspect majeur a toutefois été négligé jusqu'à présent : l'étude des déterminants clés à l'adoption de ce type de technologies par les consommateurs-citoyens. Ce papier cherche à combler ce manque en investiguant les déterminants à l'adoption de services basés sur une identification préalable. Un cadre conceptuel basé sur le célèbre modèle TAM et la théorie de diffusion des innovations est proposé qui inclut de nouveaux déterminants individuels à l'adoption de ce type de services : les risques perçus, la préoccupation pour le respect de la vie privée, l'innovativité et la confiance.

Abstract: With the introduction of digital media, publicly available networks and the development of the Information Society, identity has become a pressing contemporary issue with wide ranging implications. Identity is a complex concept and a problematic issue, in which states, businesses and the public engage. All sectors – whether public or private- are thus requiring increasingly efficient and secure means with which to identify the people behind transactions and to authenticate their identity, especially electronically. Identification is the process whereby an entity is recognized and its identity established. RFID and biometrics are some of the most famous new means of electronic identification (eID). Studies covering technological, economic, social and legal aspects of identification systems, have provided some concrete support to the development of these tools. However, one key aspect for the adoption of eID has not yet been widely studied, if at all: the key determinants of the individual's intentions to adopt such services. This paper aims to fill this gap by investigating key determinants of people's intent to adopt new identity-based services. A conceptual model based on TAM and DOI theories is proposed, including other individual determinants of technology adoption such as perceived risks, privacy concerns, innovativeness and trustworthiness.

Caroline Lancelot Miltgen
Faculté de Droit, Economie et Gestion
Université d'Angers
caroline.miltgen@univ-angers.fr

This study was funded by the European Commission IPTS (Institute for Prospective Technological Studies) Joint Research Centre: EC JRC Contract IPTS n° 150876-2007 F1ED-FR (December 2007 to November 2008, budget: 57000 Euros) with Caroline Lancelot Miltgen as the research project leader in the University of Angers (France).

Adoption of new identity-based services:
Proposition of a conceptual model based on TAM, DOI and perceived risks[1]

1. Introduction

With the introduction of digital media, publicly available networks and the development of the Information Society, identity has become a pressing contemporary issue with wide ranging implications. Information Technology has revolutionized the gathering, processing and use of identity information since more data can be collected, stored and processed into usable information. Governments and commercial organizations are responsible for increasing assaults on people's identity boundaries. Moves towards an Information Society have thus, in most cases, enhanced the central problem of control over access to identity information. This is particularly true in Europe as Information Communication Technology (ICT) has been identified as a key vector for economic development, privacy being a key European citizens' right.

Identity is a complex concept and a problematic issue in the activities and relationships in which states, businesses and the public engage. In the context of information systems, identity can be defined as "*a set of information about an entity (a person) that differentiates one entity from another similar entity*". More precisely, an electronic identity can be defined as "a *unique identifier for an individual which can be stored in an electronic form*". In everyday life, one consistently has to identify oneself. Identification is the process whereby an entity is recognized and its identity established. It can be defined as a "set of approaches, mechanisms and processes involved in the disclosure of identity information in the course of an interaction". More particularly, an electronic identification (eID) system can be defined as "*a system employed by an organization (e.g. a business or a government) for the issuance and maintenance of electronic identities of individuals*". Today, identification of someone mainly occurs with: 1) what he/she knows (e.g. PIN and passwords …), 2) what he/she has (e.g. tokens, eID cards …) or 3) how he/she is and/or behave (e.g. appearance or physical characteristics mainly known as biometrics).

For businesses, identifying consumers is both strategically important and challenging. Important because customer information is today a major source of added value for companies (Mason 1986, Glazer 1991). However data collection is challenging and far from obvious to manage. Many consumers are concerned by their privacy (Lim 2003, Lancelot Miltgen 2009). Firstly, due to the feeling of intrusion into ones intimacy and/or the dislike of self disclosure (Cespedes and Smith 1993). Also, due to fear of its consequence and in particular of an abusive use of the information they have agreed to provide (Cranor and al. 1999). This subject is even more important on the Internet which is known to exacerbate privacy concerns and thus increase apprehension concerning self-disclosure (Richards 1997).

Governments are also increasingly required to embrace electronic means of communicating with citizens. With the evolution of traditional government proceedings to eGovernment services, the remoteness of the users (normally over the Internet) produces a strong and obvious requirement to ensure the persons using the service are indeed who they say they are, and that they are fully entitled to the benefits and services they are using.

The public and the private sectors thus require increasingly efficient and secure means to authenticate the identity of the people with which they are communicating. RFID and biometrics are some of the most famous new means of identification. However, all these identification

[1] This study was funded by the European Commission IPTS (Institute for Prospective Technological Studies) Joint Research Centre: EC JRC Contract IPTS n° 150876-2007 F1ED-FR (December 2007 to November 2008, budget: 57000 Euros) with Caroline Lancelot Miltgen as the research project leader in the University of Angers (France).

technologies seem to bring as many benefits and services to the citizens (e.g. saving times and effort and allowing for convenient and tailored services) as they bring threats and constraints (e.g. privacy intrusion and dataveillance). Thus, one of the aims of this study is to identify the antecedents of identity-based services adoption, and to propose some new or less studied IT adoption antecedents such as associated perceived risks.

In this research, the relationship between willingness to adopt new electronic identification means (such as for example biometrics or RFID technologies) and key determinants with which to do so is examined. Therefore a construct is to be sought that would allow us to predict whether a proposed IT innovation (eID system[2]) may be accepted or rejected by the user population, which consists of European consumers and/or citizens. To date, most studies of IT adoption have focused on the TAM model or on further improvements and/or extensions of this model (e.g. TAM2 and Unified Theory of Acceptance and Use of Technology models). A new insight into the IT adoption literature is proposed, by adding two important determinants to those related to the initial TAM model: perceived compatibility (from DOI theory) and perceived risks, these two components themselves determined by individual variables such as innovativeness, trustworthiness and privacy concerns.

In the following section, prior literature is reviewed and justifies why the TAM model is still useful but not sufficient enough to explain the variable 'adoption intention' of new electronic identification systems. The hypotheses are then discussed and the theoretical model proposed, followed by a presentation of some methodological issues with regards to the sampling and the concepts' measurement. To conclude, this paper finishes with a discussion of some managerial and theoretical implications, as well as directions for further research.

2. Prior literature

This research is concerned with what motivates European citizens' potential adoption of futuristic and simulated electronic identification technologies, provided by unknown public or private service providers. Individuals' possible apprehensions when using such technology are particularly considered, by measuring their perceived risks of (mis)use. A study into how individuals adopt and/or use eID systems would be an ideal complement to this work, once these technologies are in current use.[3]

The technology acceptance model (TAM) (Davis 1989; Davis, Bagozzi and Warshaw 1989) provides a conceptual framework for this study. TAM is a useful model as it suggests the belief-attitude-intention-behavior causal relationship to explain and predict technology (here, eID) acceptance, among potential users. Since its early conception, there have been many improvements and/or extensions of the TAM model (e.g. TAM2 and Unified Theory of Acceptance and Use of Technology models) as well as other models which also took into consideration the technological elements (e.g. Task Technology Fit model, Goodhue and Thompson 1995). However, with the technologies in this study (future eID systems), the identification /judgment by people would be really difficult. For example, the potential output quality of the system (one additional variable from the TAM2 model) or the task technology fit (one variable from the Task Technology Fit model) would hardly be evaluable. Although being an interesting variable from the UTAUT model (Venkatesh et al. 2003), the 'facilitating conditions' construct –which refer to the degree to which an individual believes that an

[2] An eID system will refer to a combination of an eID technology and a correspondent application (cf. Appendix A).
[3] Although the technology already exists, the applications that are studied in this paper have not been developed yet for the general public.

infrastructure (organizational, technical...) exists to support use of the system- would also be difficult to measure for the same raisons proposed above. Moreover, simulated eID systems with no specific service provider are studied (the provider will only be identified by its 'category', e.g. a company, a library …), which will render the potential support very difficult if not impossible to evaluate. Despite its simplicity (which can also be considered as parsimony) and controversy (some authors consider that TAM neglects some important factors of IT adoption such as social influence), the TAM model as a theoretical basis for this research will be thus considered. This model is well adapted for use here as it has been developed for systems in which technology usage is voluntary, which is the case of the eID technologies tested in this research. Additionally, because TAM seems to neglect some individual factors that could influence user preferences in the adoption of the technology, many individual variables will be included in our conceptual framework that will be presented latter in this paper. Finally, although the TAM model has been developed in an intra-organizational context, it has already been tested in other contexts (e.g. e-commerce) and with a public of non-workers (e.g. citizens, students…) (Liaw 2002; Ruiz-Mafé et al. 2009; Padilla-Melandez et al. 2008), authorizing its use here, in a study targeting consumers and/or citizens.

Despite the robustness of TAM however, some researchers suggest that other variables such as trust (Suh and Han 2003; Pavlou 2003; Dahlberg et al. 2003; Chen and Tan 2004; Gefen and Straub 2003) and adoption characteristics (Moore and Benbasat 1991, Venkatesh and Davis 2000; Carter and Belanger 2005; Yi, Fiedler and Park 2006,) may influence attitudes toward using a technology more than usefulness (PU) and ease of use (PEOU) (Van der Heijden and Verhagen 2004, Ha and Stoel 2008). Our proposition is thus to include new potential eID adoption drivers in addition to the TAM concepts.

We first present the eID technologies and applications that will be of interest in this research. The technology adoption model (TAM) which is based on TRA and TPB models [2.2] will then be examined. The Diffusion Of Innovation (DOI) theory will also be detailed in order to evaluate the effect of adoption characteristics on willingness to use new technological system such as eID [2.3]. Variables such as perceived negative consequences of the innovation (Larose and Rifon 2007) will be included as well in our framework [2.4]. Finally, some possible individual antecedents will be presented [2.5].

2.1. The electronic identification (eID) systems

2.1.1. Technologies for identification and authentication of people

One of the aims of this research is to better understand the factors that can lead to a wide adoption of a new electronic identification (eID) system. Understanding technology and its weaknesses/potential risks avoids barriers to the adoption of the system (Elliott, Birch et al. 2007). People often use diverse identification strategies to identify themselves, depending on the context and on the organization asking for their identity. There is indeed no single "best" technology for automatic identification/authentication. Understanding the advantages and the drawbacks of each eID technology, as perceived by the citizens, is important both for systems developers and for governments who want to implement such systems in their country. Furthermore, many identification technologies are currently under development which may change the landscape of identity management in the near future, on one hand facilitating

automatic identification and on the other raising concerns about potential privacy abuse. Below are presented some identification technologies that will be of interest for this research[4].

In knowledge-based identification systems, people may be recognised by demonstrating that they are in possession of information which only they would be expected to know. The PIN/Password is a well established method for authentication of people. This widely accepted and cost-effective technology is the most typical way of authentication, however it is not considered sufficient for some ID management systems. A main drawback is the way users manage their passwords, often sharing them with other people or keeping them in an unprotected way. For systems with high security requirements, like internet banking, single-use passwords are therefore often used (Smith 2005).

A Token is a physical device which serves to confirm the identity of a person through the 'object possession' mechanism, usually taking the form of a credit card. A contact card with electronic chip is the next generation of cards, named 'smart cards', which, although not invulnerable, allow the development of very effective security measures. Contactless cards are used for example for access control to company premises or for payment in public transport. Although the main advantage for the user is increased convenience(it is sufficient to bring it close to the reader), there are a number of privacy and security issues, which are the subject of intensive research in the fields of encryption and Privacy Enhancing Technology (PET) (like anonymization) (Rotter 2008).

Biometrics is a physical or behavioural feature of a person which differs for different people, therefore enabling recognition and authentication of people. The biometric technologies already in use for the identification of people are: face recognition, fingerprints, iris recognition, hand geometry and voice recognition. For a large part of the population, these technologies are however regarded as highly intrusive forms of surveillance (Andronikou, Demetis and Varvarigou 2007). According to Uludag and Jain (2004), the security issues regarding biometric implementations are much more complex than with other IT systems. In the case of biometric encryption (i.e. merging of biometrics with cryptography), the system aims to protect sensitive data and hence acts as a PET (Tomko 1998). Thus, biometrics can simultaneously act for and against privacy and it is the security of the whole system which leads to potential privacy risks or protection. For the purpose of this research, the eID technologies that will be studied are: PIN/password, token and biometrics (see Table 1 presented later in the paper).

2.1.2. Trends in the use of technologies in e-identity applications

Until now, the most important applications for eID systems included access for transportation channel, entering public or private locations, crossing national borders and accessing e-administration or e-commerce services. In the financial sector for instance, by using privacy-enhancing identity management solutions, payment instruments can be designed without the need to reveal the person’s identity. In the healthcare sector, new eID systems help ensure that personally identifiable health information is protected and used only with the patient’s consent and for his or her own benefit. The need to identify and authenticate a person during an e-commerce transaction is also obvious. Many improvements have been made recently to secure transactions and payments in the online environment. However, consumers’ negative perceptions of credit card security, vendor trustworthiness and privacy protection remain an obstacle in

[4]For a whole overview of eID technologies and applications, see IPTS reports (http://ipts.jrc.ec.europa.eu/).

conducting business online. Applications such as eID could enhance trust in e-commerce and thus increase online purchase rates. Concerning the public sector, e-governments also promise enormous savings for public administration and citizens. According to Carter and Bélanger (2005), e-government increases the convenience and accessibility of government services and information for citizens. Most of these services need the people to identify themselves and new eID systems can enhance this process by providing more convenient and secure identification means. However, there is substantial evidence to suggest that, over the past decades, people have become less trusting globally, specifically of the government (O'Hara 2004, O'Neill 2002). The current culture of distrust and suspicion among the population is thus one factor that could shorten the implementation of eID schemes. For the purpose of this research, the main eID application areas to which this paper will refer are access control to: 1/ shared information spaces (such as social networks or virtual worlds), 2/ remote services (like banking, e-commerce or web-based applications for e-government services) and non-remote services available when the user is physically presented (see Table 1)..

2.2. The Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) (Davis 1989; Davis, Bagozzi and Warshaw 1989) is an adaptation of the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975) specifically tailored for modeling user acceptance of information systems. The origin of the TAM model is that computer systems cannot improve organizational performance if they are not used. Unfortunately, resistance to end-user systems by managers and professionals is a widespread problem. The goal of TAM is thus to provide an explanation of the determinants of technology acceptance. The results of studies using the TAM suggest the powerful capability of the model to determine user acceptance, with practical value for evaluating systems and guiding managerial interventions aimed at reducing the problem of under used technology.

According to TAM, perceived usefulness (PU) and perceived ease of use (PEOU) influence one's attitude towards a technological system, which in turn influence one's behavioural use intention. PU is 'the degree to which a person believes that using a particular system would enhance his or her job performance', and PEOU as 'the degree to which a person believes that using a particular system would be free of effort' (Davis 1989). Moreover, perceived ease of use is believed to influence perceived usefulness, as the easier a system is to use the more useful it can be. These constructs reflect users' subjective assessments of a system, which may or may not be representative of objective reality. These two constructs have already been used in studying the intent to adopt ICT and/or specific electronic systems, large and small, such as the intent to adopt new software (Venkatesh et al. 2003), or to adopt toll collection services (Chen en al. 2007). Perceived usefulness and perceived ease of use will thus be considered as potential determinants of intent to adopt new eID technology in our conceptual model, and usefulness will be considered as a mediating variable between ease of use and attitude toward adopting the technology.

Beyond TAM variables (usefulness and easiness) however, other elements could also influence consumer willingness to adopt eID, and this paper proposes that DOI provides a potential explanation/improvement.

2.3. Diffusion Of Innovation (DOI) Theory

Technology adoption depends on the characteristics of both the technology in question and the adopting unit. Regarding the former, the key factor is the content/utility of the technology, that is, whether the technology satisfies a particular need of potential adopters (at the social level). Regarding the characteristics of the adopting unit, technology adoption is shaped by three sets of variables: exposure, capacity to adopt and use, and state policies. Regarding exposure, both the expected benefits (and risks) and levels of exposure to the innovation are important. Concerning the capacity to adopt, technology adoption occurs when adopters enjoy the necessary levels of income to afford the technology, as well as the necessary cognitive skills and technological infrastructures to adopt the technology. Education for example should be an important factor of ICT adoption as the innovation could only be used by those with some skills, which in turn is highly contingent on education levels.

Diffusion of Innovation Theory (DIT or DOI) (Roger 1995) is a well-known conceptual framework to study new products' diffusion and adoption. The original diffusion model provided a probabilistic approach based on the hazard function, which determines the likelihood that a non-adopter of an innovative product will become an adopter in the next temporal unit. Rogers (1962) classifies diffusion into five stages: innovators, early adopters, the early majority, the late majority, and laggards, with 2.5%, 13.5%, 34%, 34%, and 16% of the population respectively.

According to DOI, the rate of technology diffusion is affected by an innovation's relative advantage, compatibility, trialability, observability and complexity. Research suggests that all but the last factors have a positive influence on diffusion (Sonnenwald, Maglaughlin and Whitton 2004; Ferle, Edwards and Mizuno 2002). Rogers (1995) defines relative advantage as 'the degree to which an innovation is seen as being superior to its predecessor'. Compatibility refers to 'the degree to which an innovation is seen to be compatible with existing values, beliefs, experiences and needs of adopters'. Trialability is the 'degree to which an idea can be experimented with on a limited basis'. Observability is the 'degree to which the results of an innovation are visible'. Finally, complexity, which is comparable to TAM's perceived ease of use construct, is 'the degree to which an innovation is seen by the potential adopter as being relatively difficult to use and understand'. Overall, relative advantage, compatibility and complexity are considered as most relevant to adoption research (Tornatzy and Klein 1982; Carter and Belanger 2005; Yi, Fiedler and Park 2006). Moreover, complexity is comparable (in reverse direction) to TAM's perceived ease of use construct, while perceived usefulness and relative advantage are, according to some authors (e.g. Moore and Benbasat 1991; Venkatesh et al. 2003, Carter and Belanger 2005), the same construct. In this study, the well-tested TAM constructs are chosen rather than similar DOI constructs. In addition, some DOI constructs are not necessarily adapted to our model as the eID systems to be studied (e.g. Biometrics), don't really exist (i.e have not yet been used by the public in everyday situations). The constructs of trialability and observability are consequently not useful for this study. As a result, our conceptual framework will only include compatibility as a DOI construct.

2.4. Perceived risks (or negative consequences)

It is well known that TAM and DOI constructs focus on key factors of innovation adoption, mainly measuring perceived advantages of a technology. However, the model should also take into account various obstacles to adoption. Most studies on personal information

disclosure show that consumers' reluctance to disclose information that is personally identifying is theoretically attributable to corresponding differences in the perceived severity of negative consequences (risks) of disclosure (see for example Rifon, Larose and Choi 2005, Milne, Rohm and Bahl 2004, Lancelot Miltgen 2009). But only the expectations of negative consequences of complying with the demands of a specific innovation and not generalized risks should be considered. The perceived risks are linked to particular decisions (for example, the decision to self disclose or not) which can occur in specific circumstances (task, context and time specific). Consequently, as with all innovative technologies, specific risks linked to the adoption of eID technology should be measured in order to address the specific perceptions of people. For example, the adoption of new monetary device includes financial risks which are not so important when considering the adoption of electronic administration. Our framework therefore measures perceived risks in relation to eID applications. For eID systems, safety and psychological risks are often discussed and will therefore be considered here.

A further construct relevant to eIdentity relates to trust, and more specifically to perceived trustworthiness. There is theoretical and empirical support for integrating trust in our model. First of all, many empirical studies incorporate trust into TAM (e.g., Suh and Han 2003; Pavlou 2003; Dahlberg et al. 2003; Chen and Tan 2004; Gefen and Straub 2003). Moreover, studies of e-Government suggest that perceived trustworthiness could impact citizens' intention to use e-gov services (Carter and Belanger 2005). Trustworthiness is 'the perception of confidence in the organization's reliability and integrity' (Belanger, Hiller, and Smith 2002). To adopt new technology, citizens must have confidence in the providers and in the enabling technologies.

Davis (1993) has recommended extending TAM by incorporating 'external variables', to improve not only the viability of TAM in information system research but also information systems adoption. Situational and individual variables are therefore included in the framework. First of all, as for situational variables, eID practical applications may influence public perceptions. For example, whether the system includes or not biometric recognition may give rise to different public perceptions. The type of eID technology tested is thus included in our model as a potential moderator. In order to assess different types of eID system and to test their relative influence in our model, respondents are placed in a simulated situation where eID applications will be described in a written scenario. Four scenarios concerning eID applications (e.g. biometrics, mobile services, etc) have been prepared and will be tested in future empirical test of the model. Secondly, some individual-level variables have also been treated as possible predictors of intention to adopt new technologies in IT literature. Some interesting individual variables that are presented hereafter will thus be added to our model.

2.5. Individual-level variables

Individual-level variables included in our framework belong to four categories.

2.5.1. Demographics

Analysis of most survey results points towards a role of demographic characteristics in influencing people's perceptions towards ICT. For example, in a survey on EU Citizens' trust in ID systems and authorities, Backhouse and Halperin (2007) found that gender features strongly in citizens' perception of trust: in general, male respondents were more negative in their views. Age has also a strong influence: younger people tended to exhibit more openness towards eID cards than older respondents (Backhouse and Halperin 2007). As a result, the following demographic

variables are measured (i.e. controlled) in the questionnaire: nationality, age, gender, settlement size (rural/urban), education level and occupation.

2.5.2. Innovativeness

Because of novelty, adopting an innovation (such a new IT or eID system) inherently involve a risk (Kirton 1976, Bhatnagar, Misra and Rao 2000). Some people are more (or less) likely to take a risk in adopting an innovation due to their differences in innovativeness (Rogers 2003). Therefore the technological fear variable is introduced in our questionnaire, or better still its opposite, the person's innovativeness. Rogers (2003) defines innovativeness as "the degree to which an individual or other unit of adoption is relatively earlier in adopting new ideas than other members of a social system".

Researchers use three mechanisms to classify innovation adopters into adoption categories: the innovativeness construct, a set of consumer behaviours, and "years to adopt". The former deemed a more precise approach. Building upon Rogers' work (1962, 2003), Agarwal and Prasad (1998) proposed a metric for the measurement of domain-specific individual innovativeness. They focused their attention on the adoption of IT and created a scale named 'personal innovativeness in the domain of IT' (PITT), defined as "the willingness of an individual to try out any new information technology". Because this scale is specific to IT systems, it seems particularly adapted to our study.

2.5.3. Experience with the Internet

Online experience is often considered as a strong indicator of consumer's online behavior. Moreover, the consumer's online experience could also impact its intent to adopt other electronic technologies such as eID. For example, an extensive use of the Internet tends to lower negative perceptions toward adoption of a new ID card (Backhouse and Halperin 2007). Consequently, several variables related to usage of and familiarity with the Internet will be included in our model and in the future survey questionnaire: These are Internet length of use and familiarity with and Internet skills.

2.5.4. Attitudes and behaviours in terms of personal data handling and protection

As ICT becomes more embedded in our lives, people are increasingly sharing private details via popular websites or social networks such as Youtube, Facebook or MySpace. However, individuals and groups also want and need to keep certain parts of their lives hidden from public view, and thus retain their privacy. This concept mainly reflects an individual's perceptions of the risks associated with potential privacy violations that may incur during information practices. Numerous studies have consistently concluded that the overwhelming majority of people are 'concerned' or 'very concerned' about threats to their privacy while online, and are willing to act to protect it (Paine and al., 2006). The influence of privacy concern on behavior is widely recognized, whether considering the surfing behavior, the buying behavior or the self-disclosure behavior.

Moreover, privacy concerns could be responsible for most part of the public's fears about adopting new technologies such as eID systems. This is particularly true for biometrics as biometric data are highly personal data with the greatest power and privacy threat deriving from their tight link with their owner's identity and body. For a large part of the population, this

technology is thus regarded as a highly intrusive form of surveillance (Andronikou, Demetis and Varvarigou 2007). As a high level of risk perception of information disclosure leads to less willingness to provide information (Moon 2005), there is strong evidence that privacy concern could influence the perceived risks toward adopting new eID systems. Other indicators of attitudes and behaviors in relation to personal data handling and protection should also be included in the model such as attitude toward regulation and protection measures.

Innovativeness and privacy concerns will be included in the model as key determinants to people's beliefs towards adoption of new eID applications. However, demographics, experience with the Internet and awareness and attitudes towards protection measures and regulation will only be included in the model as control variables. Consequently, no specific hypothesis will be proposed for those variables.

3. Model development

Intention to use advanced eID services is to be studied, services which for the most part do not exist or are in early phases of implementation. Therefore, the research focus is set on intention to adopt, rather than on use of such services. Attitudes and behavioral intentions have been shown to be reliable predictors of behavior across a wide range of domains and provide efficient means of assessing behavioral outcomes. Measuring intention to adopt a new technology (e.g. an eID application) can thus be seen as an effective way to evaluate the potential successfulness of the innovation. That is why intention to adopt the technology (i.e. the eID system) is measured as a key dependent variable of our conceptual framework. Another way to evaluate the consumer readiness to adopt a technology is to measure his intention to recommend this technology to friends Therefore the recommendation intention is added as a second key dependant variable. Moreover, despite the inconsistent findings regarding the effect of ease of use on attitude, attitude toward using the proposed eID technology is recognized as a key mediating variable between beliefs and behavioral intentions [3.5]. The corresponding beliefs are TAM variables [3.1], DOI variable of compatibility [3.2] and trustworthiness in public authorities and in the corresponding technology [3.3]. Some key antecedents of beliefs (i.e. other individual variables) are also incorporated in the model and justified hereafter [3.4].

3.1. The impact of TAM variables on attitude and behavioral intentions

TAM proposes that perceived usefulness and perceived ease of use determine a person's attitude toward adopting a technology (Davis 1989; Davis, Bagozzi and Warshaw 1989). Despite the inconsistent results regarding the effect of ease of use on attitude, some studies finding a significant positive effect (Chen and Tan 2004, O'Cass and Fenech 2003) whereas other founding an insignificant relationship (e.g. Chau and Hu 2001, Townsend et al. 2001), PEOU is incorporated as an antecedent of attitude in our model. Moreover, as previous research has consistently argued that: 1) perceived ease of use influences attitude both directly and indirectly through the perceived usefulness (Dishaw and Strong 1999, Gefen and Sraub 2000, Venkatesh and Davis 2000, Ha and Stoel 2008) and 2), perceived usefulness influences technology adoption intention both directly and indirectly through the attitude (Chen et al. 2007), the hypotheses bellow propose the following:

H1: The greater the perceived usefulness, the more favorable the attitude toward adopting eID

H2: The greater the perceived ease of use, the more favorable the attitude toward adopting eID

H3: The perceived usefulness of the eID technology is positively corelated to its perceived ease f use

H4: The perceived usefulness of the eID technology positively increases the intention of adoption

3.2. The impact of DOI variables on attitude

We included both TAM and DOI constructs in our eID adoption model because DOI constructs have been shown to add significantly to the prediction of adoption intent (Plouffe el al. 2001, Carter and Belanger 2005). Although compatibility is not a variable included in TAM, recent studies on innovation diffusion and technology acceptance suggest that compatibility is an important variable in determining technology adoption outcomes in addition to PU and PEOU (Agarwal and Prasad 1998; Parthasarathy and Bhattacherjee 1998, Sultan and Chan 2000, Yi, Fiedler and Park 2006). Therefore, hypothesis H5 proposes the following:

H5: The greater the perceived compatibility, the more favorable the attitude toward adopting eID

3.3. The impact of perceived risks on attitude

When engaging in an online transaction, consumers are highly concerned by the different types of risks that confront them (Pavlou 2003). It has been shown that perceived risk is associated with lower consumers' intentions to use Internet sites for transactions (Miyazaki and Fernandez 2001; Pavlou 2003). In our study, given the uncertainty of e-identification, it is expected that perceived risks would lower consumers' intentions to adopt a new eID application by negatively influencing the attitude toward adopting the eID technology. For example, fear that the eID service provider has not taken adequate steps to ensure the security of the transaction will negatively affect the attitude toward adopting the eID technology. The possibility of private information theft or illegal disclosure could also put the individual in a less favorable attitude toward adopting the technology. Consequently, hypothesis H6 proposes the following statement:

H6: The greater the perceived risks, the less favorable the attitude toward adopting eID

3.4. The antecedents of beliefs

Trust models suggest that a combination of trust in the technology (here in the Internet as the web is the main platform on which electronic identification systems are available), trust in the organization trying to implement the eID application (whether public or private) and trust in the product or service proposed (the eID application itself) affects overall perceptions of trustworthiness (Lee & Turban, 2001). As the eID service provider will not be clearly identified, instead, trust in the public authorities is an ideal variable to measure. Indeed, it is the entity which 1/ accepts the eID system to be delivered to the citizens and 2/ ensures the legal protection of citizens' security and privacy in relation to personal data handling. These three trust components should be evaluated individually and in combination, within the context of new eID systems' implementation and are therefore all supposed to influence the consumers' beliefs toward this technology.

Trustworthiness is a central tenet in consumers to business relationships and is even more critical in online transactions because of the unique characteristics of the virtual environment. Trust is one of the most effective tools for reducing uncertainty and risks and generating a sense of safety (Pavlou 2003, Suh and Han 2002). Therefore, consumer trust in public authorities and technology (Internet and eID)[5] is believed to play a pivotal role in consumers' intentions to adopt the eID technology (Carter and Belanger 2005) by reducing the perceived risks and uncertainty associated with the adoption (Pavlou 2003). Consequently:

H7a: Consumer perceived risks of adopting new eID technology is negatively related to trust

Trust in technology doesn't only influence the perceived risks associated with adopting the technology. Prior studies also incorporate trust in TAM in several ways. Results support trust as an antecedent of 1° ease of use (Pavlou 2003), as it allows consumers to become vulnerable to the e-service provider (Chircu el al. 2000) and 2° usefulness (Dahlberg et al. 2003, Pavlou 2003), as it reduces the need for the consumer to control the situation, facilitating the transaction and making it effortless (Chircu et al 2000). Consequently:

H7b: Consumer trust[6] is positively related to the perceived usefulness of a new eID technology

H7c: Consumer trust is positively related to the perceived ease of use of a new eID technology

Consumers' information is at risk when they identify themselves while surfing and/or completing transactions online. While identity theft has traditionally occurred offline, online collection of online identities is both easier and more efficient for thieves (Katyal 2001). Consumers who do business with online organizations (whether public or private) are thus highly vulnerable as their personal data can be compromised and misused. Privacy concern reflects an individual's perceptions of the risks associated with potential privacy violation associated with the information practices (Rifon, Larose and Choi 2005). Therefore, consumers with higher privacy concerns will perceive lower risks in giving their personal identity online. For the eID technology, hypothesis H8 is proposed:

H8:Consumers with higher privacy concerns will perceive more risks of adopting the eID technology

Innovativeness captures an individual's predisposed tendency to try out a new technology. This variable has been shown to be a significant predictor of behavioral intention to use new technologies such as online buying and PDA (e.g. Yi, Fiedler and Park (2006). However, it was recently suggested that individual innovativeness might be a direct predictor of TAM and DOI variables (Lewis et al. 2003). Yi, Fiedler and Park (2006) confirmed that, regardless of the measure or the innovation acceptance settings, innovativeness directly determine 3 innovation characteristics, namely the perceived usefulness, ease of use and compatibility, which are also 3 mediating variables of our model. Due to this result, the following hypotheses are postulated:

H9: Consumers with higher personal innovativeness will perceive the eID technology characteristics of usefulness (a), ease of use (b) and compatibility (c) more positively

[5] In this research, consumer trust will thus refer to 3 kinds of trusting entities/technologies

[6] We will only refer here to the trust in technology (Internet and eID system).

3.5. Attitude influencing consumers' intent to adopt and recommend the technology

TAM proposes that the beliefs about a new technology determine a person's attitude toward using the technology which in turn determines their intention to use it. Therefore, for the eID system, hypothesis H10 postulates the following:

H10: Consumer's attitude toward adopting a new eID system positively influences the intention to adopt the technology

If consumers usually rely on word-of-mouth (WOM) to judge the quality of a product, a service or a website, they can also produce some recommendations (File, Diane, Cermak and Prince, 1994). Consumers having received favorable information on a merchant, a product or a service (i.e., a positive WOM) will have a more positive perception of the object and/or the subject. Those consumers with a positive attitude will then be more inclined to recommend the product/service and/or provider to their social circle (family, friends…). Moreover, as the positive relationship between behavioral intentions and actions is extensively described in the TRA and TPB models, consumers with high intention to adopt a new technology are assumed to be early adopters – or innovators following Roger's (1962) model - of the innovation. Following the 'diffusion of innovation' models, influenced by both internal (i.e. mass media) and external (WOM) communication means, other consumers (i.e. the early adopters and the early majority) will also adopt the innovation at later stages. Positive WOM of innovators (people with high intention to adopt the innovation at early stages) can thus positively influence the behaviors of later adopters. Consequently, both consumers' positive attitude and/or high adoption intention can influence the intention to recommend the technology to their social circle. Hypothesis H11 postulates the following:

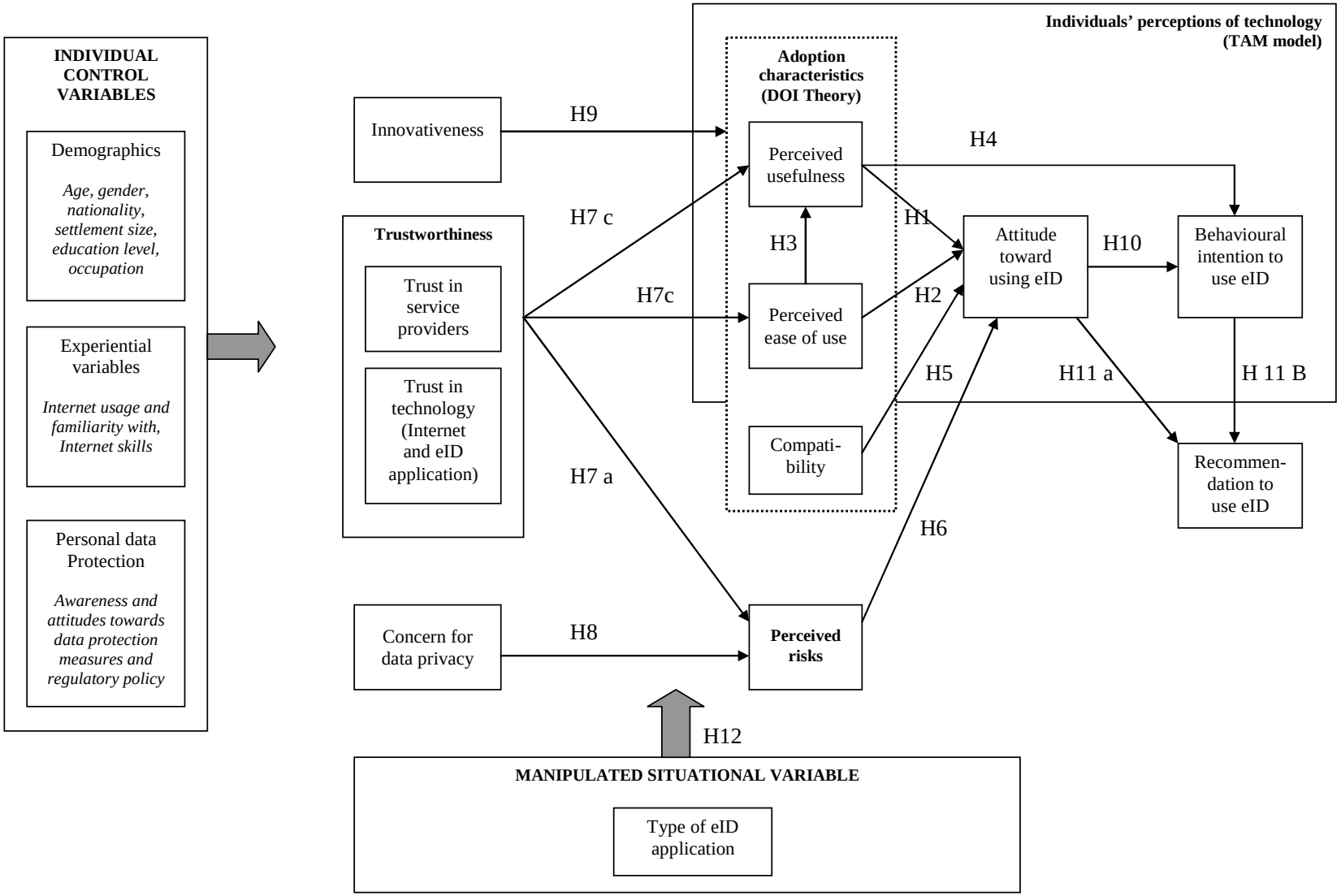
H11: Consumer's attitude toward adopting a new eID system (a) and intention to adopt the technology (b) both positively influence the intention to recommend the technology to others

As said before, eID practical technologies and applications may influence public perceptions and should potentially moderate some of the links that are proposed in the model. For example, whether the system includes or not biometric recognition may engender different public perceptions in terms of trustworthiness, risks and compatibility. The type of eID system is thus included in our model as a potential moderator. Practically, different eID systems (considered as a combination of technology and application) will be proposed to the participants (in the form of written scenarios) and tested in the future empirical test of the model in the form of multi-groups analysis. Consequently only a general hypothesis is formulated for this variable:

H12: the eID system tested is likely to influence the links proposed in the model

We present the conceptual model of our research in Figure 1.

Figure 1 Proposed theoretical framework



4. Methodology

4.1. Choice of the eID technologies to test

There are numerous types of eID technologies and applications, some of them already used nowadays (e.g. PIN/password to access personal devices and data) and others for future use (e.g. RFID implants to access restricted space). Appendix A provides a table matching the eID technologies and applications often used today and which will be used in 5 to 15 years (IPTS 2008). Because it isn't possible to study the potential adoption of all of technologies individually (there are 30 possible combinations of eID technologies/applications) nor globally – as a means of all possible combinations - (the influence of the factors may greatly depends on the type of eID technology/application studied), 4 different e-services situations are suggested using 3 kinds of eID technologies (i.e. biometrics, tokens and single sign-on) and 3 types of applications (see Table 1).

(insert Table 1 with Scenarios here)

Because Internet users' actual and future behaviours are predominantly investigated, an survey online is conducted, using a scenario method in which respondents are presented with written scenarios describing a simulated situation in which a friend has the possibility to adopt a specific combination of eID technology/application. This approach seems suitable for eliciting beliefs and attitudes in typical situations, especially in relation to moral dilemmas (Seawright & Sampson 2007; Bateson & Hui 1992; Wang & Manning 1999). Furthermore, respondents should not offer socially approved answers, because social pressure is diminished with online questionnaires administered individually (Morahan-Martin & Schumacher 2003). Four questionnaires were built in which only the scenario proposed to the respondent (one taken at random in the 4 scenarios) changed. This choice increases the external validity of our results as people's perceptions, attitudes and intentions to adopt are evaluated on different types of eID systems. This choice enables the 'control' of the influence of the eID system to be studied and to study its influence on the model and potentially on all the links tested.

4.2. Sampling

Young people (15-25 years old) have embraced new information technologies in large numbers. They use the Internet widely for many of their daily activities. For example, 88% of the 16-24 years old of EU27 are connected to the Internet versus 60% of all the EU27 individuals (Eurostat, 2009). Young people's activities online are also often ahead compared to the average European Net surfers. Consequently they probably represent the Net surfers of tomorrow. Moreover, they correspond to possible opinion leaders in the area of IT. It is thus important to understand their opinion toward eID services in order to evaluate the future impact of electronic identification systems on the Internet population as a whole, and on the future Net surfers in particular. As they are people who have grown up with these new technologies, they undoubtedly better reflect the behavioural patterns of the future society (especially concerning the adoption of technologies that will only be available to the average European citizen in 5 to 10 years) since: 1) they are future adult citizens; 2) they have a high level of IT literacy; 3) they tend to grasp new technologies rapidly. Additionally, as young people aged 15-25 years make up 11 to 16% of the European population, depending on the country considered, they represent quite a large proportion of the population.

4.3. Administration of the questionnaire

A preliminary questionnaire was presented and discussed during an expert workshop. On the basis of experts' recommendations, a revised version of the questionnaire was proposed and tested through a small-scale field trial (pre-test) which involved 117 young people in the United Kingdom. The results of this pre-test were used to amend, remove and reformulate some questions. A total of 12,143 young (15-25 years old) Europeans from 4 European countries (France, England, Spain and Germany) took part in the final survey. Emails with invitations were sent to 531, 443 people, retrieved from a selected set from a Net Surfers database managed by the 1000mercis French company through its Elisa program. Overall, Elisa comprises 9, 000, 000 members living in Europe and 500, 000, 000 criteria. This database offers the advantage of being multi-cultural, efficient (good response rate) and allows the researcher to obtain a representative sample of young European people. The sample for our survey was selected in the Elisa database by using quotas. In particular, the quotas were based on Eurostat data in each of the four countries and 2 criteria that were mainly used were: gender (male/female) and age (split into two groups 15-18 year olds and 19-25 year olds). This sampling method should implicate the relative representativeness of the sample based on the above criteria. This choice is preferred over a convenience sample (e.g., students) whose specific characteristics (e.g., age, education level) might limit generalisations of the results to a broader population. Being able to generalise permits the increase of the results external validity. Participants in the study were diverse in nationality, gender, age, professional status and education level. This choice meets the criteria of Mason's (1996) concept of being 'theoretically generalisable', in that 1° there is no reason to assume that our sample of participants is specifically atypical (e.g. all middle class) and that 2° the analysis is rigorous and systematic. In respect to these points, the findings presented here can be taken to indicate current young European (i.e. French, English, Spanish and German) attitudes towards ICT in general and the adoption of specific identification systems in particular[7].

4.4. Description of the sample

Out of the 12, 143 respondents, 37% were French, 27% Spanish, 22% English, and 14% German. 56.3% of the respondents were male and 43.7% were female, this proportions being quite different in some countries, notably in Spain and in the UK. The majority of people surveyed were between 15 and 18 years old (45.6% of them), 29.1% between 19 and 21 and 25.3% of youngsters were more then 22 years old. Globally, nearly half were students (with more students in the UK and fewer in Spain) and around 30% of the youngsters were 'blue collar' (from a working class environment). Concerning the education level, only 2 % had a Doctorate and 18 % a masters degree (this percentage was smaller in the UK and Germany). The education level most encountered was 'license' or Bachelors (three years of higher education) which represents 40.9% of the sample. Most of the young participants did not have an Internet connection at home (64.3%), the participants were however still present online. 62.6% had used the Internet for more than five years and a majority of them went online several times a day

[7] To ensure that there is no bias in the sample selection, we compared the profiles of full and partial respondents. The results of chi-tests show that full and partial respondents are quite different in their profile (e.g. full respondents are mainly from France, UK and Germany and use the Internet for more than 5 years) but that they do not differ in terms of Internet trust level, informational privacy concerns and attitude toward adopting the proposed eID system, which shows that there is no big non-response bias.

(76.9%) with fewer people doing so in Spain and more so in France and Germany. Appendix B shows the sample characteristics.

4.5. Measurement

To test our conceptual framework, major constructs with multi-item scales (Appendix C) are measured. Most items use seven-point scales ranging from "strongly disagree" (1) to "strongly agree" (7) with some items measured in five points scales (e.g. attitude, privacy concerns). The majority of the scales used in the questionnaire come from the literature or integrate statements from existing scales (e.g. all scales for TRA and DOI) with others (e.g. perceived risks) proposed by the authors on the basis of the results from a previous qualitative study and the expert workshop. As the questionnaire was very long and in order to decrease any bias in the answers due to the respondents' fatigue, the shortest scales found in the literature were applied.

To ensure their content validity, all scales were validated by the experts and pre-tested. Furthermore, the scales on the basis of exploratory and confirmatory factor analyses were validated.

5. Conclusions

5.1. Academic and managerial implications

Based on famous IT literature (TAM and DOI models) and proposing an integrated and extended conceptual framework of key determinants of new technology adoption, this research offers important implications for researchers, managers and policy makers.

On the academic level, this paper contributes to existing literature pertaining to technology acceptance theories and completes existing models with new key determinants such as trustworthiness and innovativeness.

We also suggest including many individual variables as control variables and the type of eID application tested as a manipulated and moderating variable. Finally, development of the existing intent to adopt models is proposed, by incorporating a new key dependant variable: the capacity to recommend adopting the technology. This extends DOI theory by studying the potential recommendation power.

Several practical implications also emerge.

Firstly, this model encourages managers to be particularly attentive to both specific risks and benefits in adopting the technology. Some people could be encouraged to adopt a new application because of its ease of use but could finally refuse to use it because of high perceived risks, especially in relation to security and privacy. Secondly, public authorities should address citizens' concerns in relation to new identity based services. Undoubtedly, privacy concerns will highly influence the perceived risks toward adopting the technology. Government should thus find useful means to reassure people if they want these new technologies to be adopted.

5.2. Limitations and suggestions for further research

This research is not without its limits that should encourage further research in this area.

First of all, this paper only proposes a conceptual framework that should now be tested in order to see if all hypotheses postulated are verified. This should be done on samples as representatives as possible of the population in order to have useful results.

Secondly, of the many situational factors that might influence responses, only the type of eID technology and application is considered. Probably the organization which offer the application and the functionalities of the application itself also influence the decision to adopt (or not) a new eID technology. Additional research should thus investigate these other factors and some ways of manipulating them.

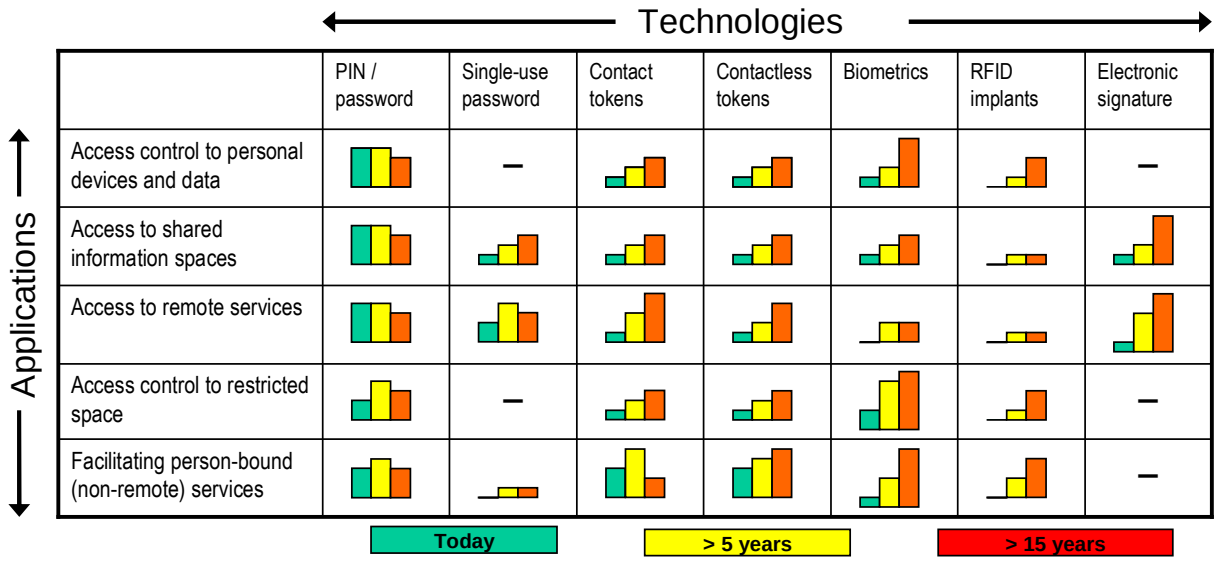
We focused our research on the citizens' adoption of eID systems. However, it would also be interesting to study the public entities' motivations and perceived risks in encouraging the implementation of such eID systems in one geographical area and/or in adopting themselves these systems (e.g. e-government initiatives, e-passport …).

Finally, measuring TAM and DOI using only some of the original variables undoubtedly is restrictive; other elements such as trialability and observability could also have important effects.

Table 1. The eID scenarios tested in the research (one scenario per participant)

SCENARIOS	eID Technology	Applications
Your friend **Claudia** is 16 and always busy hanging around with her friends. A company offers her a service to keep in touch with her friends and know new people. To help her identify people she may like to meet and friends feeling like the same in the vicinity (bars, clubs, gym and university), the service requires some of her personal data, such as age, gender and location. The service is accessible through her mobile phone, based on the SIM card. If Claudia switches on the service her whereabouts and current activities are charted, to match other people's whereabouts.	Communicating device (SIM)	Access to shared information spaces
Your friend **Max** is 18; he moved from his village to Dublin to work in a call centre during the summer. To keep in touch with his friends and manage his new life, he needs to access his email accounts and mobile devices, and make use of a range of websites such as Facebook, Skype, online banking, paying tax online, online grocery shopping etc. As he has no internet at home, he uses a close-by internet café. The owner of the café offers him to manage all his activities (social, leisure and financial) from a single website, using a single login and password.	PIN/password	Access to remote services (SNS, e-commerce)
Your friend **Alice** is turning 18, and is planning a 3-months trip abroad over the summer. She will carry her electronic passport to visit all the countries she has in mind. A company offers to add to the passport chip additional information of her choice, such as her travel preferences, food tastes, her digital signature, some emergency money etc. With this enhanced chip she could access a range of services without carrying around additional documents. For instance, shopping malls could advise on clothes she may like as she walks past them; travel agents may suggest additional sights seeing based on her route, and credit could be added to the card in case of medical emergency.	Contactless token	Access to Remote services (e-commerce)
Your friend **Alex** is 17. Every day he goes to the library to practice for his driving test on one of the driving simulators provided by the local council. To enter the library he could join the queue at the counter, which is half-dozen people long, including people he knows, and have his library card scanned. In this case, the librarian will look at his file, ask him a few questions and allocate the right simulator. Alternatively, he could use the eye-scan machine at the entrance. This automatically allocates him a simulator to use, based on his previous test results and on his preferences. The second procedure will probably take him less time.	Biometrics	Facilitating person-bound (non-remote) services

Appendix A. Matching eID technologies and applications



Source: IPTS, eID expert Workshop, Sevilla, April 2008

Appendix B. Main characteristics of the sample (demographics and internet use)

Main demographic characteristics of the sample

		France	UK	Spain	Germany	Total
Country responses		37	22	27	14	100
Sex	Male %	60	65	78	53	56
	Female %	40	35	22	47	44
Age	15-18 %	59	30	45	37	46
	19-21 %	31	29	27	29	29
	22-25 %	10	41	28	34	25
Professional status	Student %	56	75	20	54	48
	Self-employed %	1.5	4	9	3	4
	Manager %	1.5	4	3	1	2
	Other white collar %	5	7	6	5	5
	Blue collar %	27	3	51	30	31
	Unemployed %	9	8	11	7	9
Education level	Baccalaureate %	32	62	34	67	39
	Licence %	46	31	37	28	41
	Master %	21	6	22	5	18
	Doctorate %	1	2	8	0	2

Internet use characteristics of the sample

		France	UK	Spain	Germany	Total EU
Internet connection type	Broadband at home	95%	66%	80%	95%	66%
	Other connections	5%	34%	20%	5%	34%
Internet length of use	< 1 year	3%	5%	3%	3%	5%
	1-3 years	14%	20%	13%	14%	20%
	3-5 years	22%	19%	23%	22%	19%
	+5 years	61%	56%	61%	61%	56%
Surf online	Several times per day	85%	64%	80%	85%	64%
	Once a day	10%	26%	11%	10%	26%
	A few times a week	5%	9%	8%	5%	9%
	Less than once a week	0%	1%	2%	0%	1%

Appendix C. Instruments measure

1. INDIVIDUAL VARIABLES

	Gender	Male / Female						
	Age	Your year of birth						
	Professional situation	What is your actual professional situation?						
	Education	What was your full time last year education level? (to adapt to each country)						
	Settlement size	You live in…	Metropolitan zone	Other urban zone	Rural zone			
	Internet length of use	How long have you been using the internet?	Less than one year	Between 1 and 3 years	Between 3 and 5 years	More than 5 years		
	Connection frequency	How often do you connect to the Internet?	Several times a day	Once a day	A few times a week	Less than once a week	Less than once a month	Never
Yi, Fielder and Park (2006)	Innovati-veness	How would you place yourself, in relation to your peers?	Strongly disagree	To	Strongly agree			
	I1	I am among the first to try out new technologies	1		7			
	I2	When I hear about a new technology, I look for ways to adopt it	1		7			
	I3	I like to experiment with new technologies	1		7			

2. DEPENDENT VARIABLES

	Recommendation	Would you recommend that your friend subscribes to the service?	Strongly recommend (1)	To	Strongly discourage (5)
Yu et al. 2005	Intention of eID adoption	What else would you recommend to your friend?	Strongly disagree	To	Strongly agree
	IA2	He/she should apply this service as soon as possible	1		7
	IA3	He/she should use this service soon after it is launched	1		7
	IA4	He/she should wait until some friends use it / get detailed information before subscribing	1		7

3. INDEPENDENT VARIABLES

Taylor and Todd (1995)	Attitude	Overall, do you think that	1	To	5
	ATT1	Using this service would be:	A good idea		A bad idea
	ATT2	Using this service would be:	A wise idea		A foolish idea
	ATT3	Using this service would be:	Attractive		Non attractive
	ATT4	The idea of using this service	You like it		You dislike it
	PEOU1	The service requires a minimum of effort	1	2	3
Davis (1989),	PEOU2	It would be easy to get this service to do what you want it to do	1	2	3
	PEOU3	Learning to use such service would be easy for me	Strongly disagree	To	Strongly agree
	PEOU4	I would find this service easy to use	1		7
Adapted from Davis (1989),	PU1	This system would enable to identify oneself more securely	1	2	3
	PU2	This system would provide a valuable service	1	2	3
	PU3	This system would make it easier to identify oneself	1	2	3
	PU4	This system would make him/her effectively control its personal data	1	2	3
Pavlou (2003)	Trust in technology 1	I would trust the system	1		7
	Trust in technology 1	I think the service would be reliable	1		7
Vijayasara-thy (2004)	Compati-bility 1	I think using this system would fit well with the way that I like to identify myself	1		7
	Compati-bility 2	Using this system would fit into my lifestyle	1		7

Bélanger & Carter (2008)	Risks	What are the potential risks?	Strongly disagree	To	Strongly agree
	R1	Your activities may be monitored	1		7
	R2	Information may be collected that could be used against you in future life	1		7
	R3	Someone may hack into the system and steal your personal information	1		7
	R4	You may get unauthorized charges on credit card	1		7
	R5	Someone may use your identity instead of you	1		7
	R6	You will receive unwanted commercial offers	1		7
	R7	Your privacy may be at risk, resulting in embarrassment	1		7
	R8	Your privacy may be at risk, resulting in serious personal consequences	1		7
	R9	Your personal data will be shared with unauthorized persons	1		7
McKnight et al. (2002)	Trust in Internet	More generally, concerning the Internet, you would say that…	Strongly disagree	To	Strongly agree
	TI1	The internet has enough safeguards to make me feel comfortable giving my personal details online	1		7
	TI2	The internet is now a robust and safe environment in which to transact.	1		7
	TI3	The internet provides a trusted environment in which to make transactions for leisure, work and business	1		7
	TI4	The internet is safe enough to preserve my privacy as I carry out leisure, business and personal activities	1		7
	TI5	I am confident that I can protect my privacy online	1		7

Fogel & Nehmad (2009)	Privacy concerns	How concerned are you about the following risks in relation to your personal information	Very concerned	To	Not at all concerned
	PC1	Companies possess information about me that I consider private	1		5
	PC2	My personal information is used without my knowledge	1		5
	PC3	My personal data is shared with third parties without my agreement	1		5
	PC4	My behaviour and activities can be monitored online	1		5
	PC5	My online personal data is used to send me commercial offers	1		5
	PC6	My identity is reconstructed using personal data from various sources	1		5
Bélanger & Carter (2008)	Trust in public authorities	For each of the following statements, please state if you tend to agree or not	Strongly disagree	To	Strongly agree
	TPA1	In [country], my personal data are properly protected	1		7
	TPA2	[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	1		7
	TPA3	I believe that the systems used by the public authorities to manage the citizens' personal data are technically secure.	1		7
	TPA4	I believe that citizens will be able to keep a good level of control over their personal data	1		7
	TPA5	I will always be able to rely on public authorities for help if problems arise with my personal data	1		7
	TPA6	I believe that the authorities that manage my personal data are professional and competent	1		7

REFERENCES

Agarwal and Prasad (1998), A conceptual and operational definition of personal innovativeness in the domain of information technologies, Information Systems Research, 9 (2), 204-215

Ajzen, I (1991). The Theory of Planned Behavior. Organizational Behavior & Human Decision Processes, 50 (2), 79-212

Andronikou, V., Demetis, D.S., and Varvarigou, T. (2007). Biometric implementations and the implications for security and privacy. http://journal.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf.

Backhouse J. and Halperin R. (2007). A Survey on Citizen's trust in ID systems and authorities'. Fidis Journal, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.5.a_survey_on_EU_citizens_trust.pdf

Bateson, J.E.G. & Hui, M.K., 1992. The Ecological Validity of Photographic Slides and Videotapes in Simulating the Service Setting. *The Journal of Consumer Research*, 19(2), 271-281.

Bélanger, F. & Carter, L., 2008. Trust and risk in e-government adoption. The Journal of Strategic Information Systems, 17(2), 165-176.

Belanger, F., Hiller, J.S. and Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes The Journal of Strategic Information Systems 11, (3-4), 245-270.

Bhatnagar, A., Misra, S., and Rao, H.V. On Risk, Convenience, and Internet Shopping Behavior. *Communications of the ACM*, 43(11), 2000, 98-105

Carter, L. and Bélanger, F. (2005). The Utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1) pp.5-25

Cespedes F. V. et Smith J. H. (1993), Database marketing: new rules for policy and practice, *Sloan Management Review*, 7-22

Chau P.Y.K. and Hu P.J.H., Information technology acceptance by individual professionals: A model comparison approach, *Decision Sciences* 32 (2001) (4), pp. 699–719

Chen and Tan, 2004 L.-D. Chen and J. Tan, Technology adaptation in e-commerce: Key determinants of virtual store acceptance, Eur Manage J 22 (1) (2004), pp. 74–86.

Chen C.-D., Fan Y.-W. and Farn C.-K., "Investigating Factors Affecting the Adoption of Electronic Toll Collection: A Transaction Cost Economics Perspective," Proceedings of the 40th Annual Hawaii International Conference on System Sciences (IEEE Computer Society, 2007)

Chircu, Alina M; Kauffman, Robert J, Limits to value in electronic commerce-related IT investments, JMIS, Vol. 17 No 2, 2000, 59-80

Cranor L. F., Reagle J. et Ackerman M. S. (1999), Beyond concern: understanding net users' attitudes about online privacy, *ATT Labs – Research Technical Report*, 99.4.3

Dahlberg T., Mallat N. et Öörni A. (2003), Trust enhanced technology acceptance model - consumer acceptance of mobile payment solutions, Mobility Roundtable Conference, May 22-23, Stockholm,

Davis, F. D. (1993). User acceptance of information technology: Systems characteristics, user perceptions and behavioral impacts. International Journal of Man-Machine Studies, 38, 3, 475-487.

Davis, F.; Bagozzi, R.; and Warshaw, R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, Volume 35, 1989, pp. 982-1003.

Davis, F.D., 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

Dishaw, M.T. and Strong, D.M. Extending the Technology Acceptance Model with Task-Technology Fit Constructs,. Information and Management (36:1), 1999, pp. 9-21.

Ferle, C., Edwards, S.M. and Mizuno, Y. (2002), Internet diffusion in Japan: cultural considerations. Journal of Advertising Research, 42 (2), 65-79

File, Karen Maru, Dianne S. P. Cermak, and Russ Alan Prince. 1994. "Word-of-Mouth Effects in Professional Services Buyer Behaviour."Service Industries Journal 14 (July): 301–314.

Fishbein M.., Ajzen, I. (1975). Belief, Attitude, Intention and Behavior. An introduction to theory and research. Addison-Wesley, Reading, MA

Fogel, J. & Nehmad, E., 2009. Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior, 25(1), 153-160.

Gefen D. & Straub D. The Relative Importance of Perceived Ease-of-Use in IS Adoption: A Study of e-Commerce Adoption, Journal of AIS (1: 8, October), 2000, pp. 1-30

Gefen, D. and Straub, D., 2003, Managing User Trust in B2C e-Services. *e-Service Journal*, 2 (2), 7-23.

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. IEEE Transactions on Engineering Management, 50(3), 307-321.

Glazer, R. Marketing in an information-intensive environment: strategic implications of knowledge as an asset. *Journal of Marketing*, 55 (October 1991), 1-19.

Ha, S. & Stoel, L. 2008. Promoting Consumer-Retailer Relationship Building: Influence of Consumer Trustworthiness of Customer Loyalty Program Marketing. *Journal of Customer Behaviour*. Vol. 3, no. 7: 215-229.

Katyal, Neal Kumar. 2001. Criminal Law in Cyberspace. University of Pennsylvannia Law Review, 149 (4): 1003-1115.

Kirton, M. 1976. Adaptors and Innovators: A description and measure. Journal of Applied Psychology, 61(5): 622-629.

Korgaonkar, Pradeep K. and Lori D. Wolin (1999), A Multivariate Analysis of Web Usage, Journal of Advertising Research, 39 (2), 53-68.

Kramer, R. M. (1999) Trust and Distrust in Organizations: Emerging Perspective, Enduring Questions, Annual Review of Psychology, 50, 569-598.

Lancelot Miltgen C. (2009), Propension à fournir des données personnelles mensongères sur Internet : une étude exploratoire, *Systèmes d'Information et Management, 14 (3)*

LaRose R. and Rifon N. J. Promoting i-Safety: Privacy Warning Boxes, Privacy Seals and Online Privacy Behavior, *The Journal of Consumer Affairs*, Vol. 41, No. 1, Summer 2007, 127-149

Lee, M.K.O., and Turban, E. (2001) A Trust Model for Consumer Internet Shopping. International Journal of Electronic Commerce, 6 (1), 75-92.

Lewis et al., 2003. Sources of influence on beliefs about information technology use: an empirical study of knowledge workers. MIS Quarterly. v27. 657-678

.Liaw, S., 2002. An Internet survey for perceptions of computers and the World Wide Web: relationship, prediction, and difference. Computers in Human Behavior, 18(1), 17-35.

Lim, N. Consumers' Perceived Risk: Sources versus Consequences. *Electronic Commerce Research and Application*, 2, 2003, 216-228.

MacKenzie, S.B., Lutz, R.J. & Belch, G.E., 1986. The Role of Attitude Toward the Ad as a Mediator of Advertising Effectiveness: A Test of Competing Explanations. Journal of Marketing Research (JMR), 23(2), 130-143.

Mason R. (1986), Four ethical issues of the information age, *MIS Quarterly*, 10, 1, 5-12

McKnight, D.H., Choudhury, V. & Kacmar, C., 2002. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research, 13(3), 334-359.

Milne,G.R., Rohm, A.J. and Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. Journal of Consumer Affairs, 38 (2), 217-232.

Miyazaki, A.D. and Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. Journal of Consumer Affairs, 35 (1), 27-45.

Moore, G.C., and Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Information Systems Research, 2(3), 192-222

Morahan-Martin, J. & Schumacher, P., 2003. Loneliness and social uses of the Internet. Computers in Human Behavior, 19(6), 659-671.

O'Cass, A and Fenech, T. (2003) WEB retailing: A study of Internet users adoption of the WEB as a retailing medium, Journal of Retailing and Consumer Services, 10, 81-94.

Padilla-Meléndez, A., Garrido-Moreno, A. & Del Aguila-Obra, A.R., 2008. Factors affecting e-collaboration technology use among management students. Computers & Education, 51(2), 609-623.

Pagani, M., 2007. A Vicarious Innovativeness Scale for 3G Mobile Services: Integrating the Domain Specific Innovativeness Scale with Psychological and Rational Indicators. Technology Analysis & Strategic Management, 19(6), 709-728.

Paine C., Reips U.D., Stieger, S., Joinson A., Bichanan T. (2006). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. International Journal of Human-Computer Studies (65), 526-536

Parthasarathy, M., & Bhattacherjee, A. (1998). Understanding post-adoption behavior in the context of online services. Information Systems Research, 9(4), 362-379.

Pavlou, P.A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3), 101-134.

Pavlou, P.A., 2003. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 101-134.

Plouffe, C.R.; Hulland, J. S. and Vandenbosch, M. (2001), Research Report: Richness Versus Parsimony in Modeling Technology Adoption Decisions, Understanding Merchant Adoption of a Smart Card-Based Payment System. Information Systems Research, 12 (2), 208-223.

Richards J. I. (1997), Legal potholes on the information superhighway, *Journal of Public Policy and Marketing*, 16, 319-326

Rifon N.J., Larose R.and Choi S.M. (2005), Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures, The Journal of Consumer Affairs, 39, 2, 339-362

Rogers, E. M. (1962). Diffusion of Innovations. Glencoe: Free Press.

Rogers, E.M. (1995). Diffusion of innovations (4th ed.). New York: The Free Press.

Rogers, E.M. (2003). Diffusion of Innovations, 5th edition, NewYork, Free Press.

Ruiz-Mafé, C., Sanz-Blas, S. & Aldís-Manzano, J., 2009. Drivers and barriers to online airline ticket purchasing. Journal of Air Transport Management, 15(6), 294-298.

Seawright, K.K. & Sampson, S.E., 2007. A video method for empirically studying wait-perception bias. Journal of Operations Management, 25(5), 1055-1066.

Sonnenwald, D. H., Maglaughlin K. and, Whitton M. C. Designing to support situation awareness across distances: an example from a scientific collaboratory. Information Processing and Management. 40(6): 989-1011 (2004)

Steel, J. L. (1991). Interpersonal correlates of trust and self-disclosure. Psychological Reports, 68, 1319-1320.

Suh, B. and Han, I., 2003, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce", *International Journal of Electronic Commerce,* 73, 135-161.

Sultan, F., and Chan, L. "The Adoption of New Technology: The Case of Object-Oriented Computing in Software Companies," IEEE Transactions on Engineering Management (47:1), 2000, pp. 106–126.

Sweden.Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly 13, 319-339.

Tornatzky, L. G., & Klein, R. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. IEEE Transactions on Engineering Management, EM-29, 28-45.

Townsend.M., Demarie S.M. and Hendrickson A.R., Desktop video conferencing in virtual workgroups: anticipation, system evaluation and performance, Information Systems Journal 11 (2001), pp. 213–227

Van der Heijden, H. & Verhagen, T. 2004. Online store image: conceptual foundations and empirical measurement, Information and Management, vol.41, no.5, pp.609-617

Venkatesh, V. & Davis, F. D. (2000). Why don't men stop to ask directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly* 24. 186-204.

Venkatesh, V. & Davis, F.D., 1996. A Model of the Antecedents of Perceived Ease of Use: Development and Test. Decision Sciences, 27(3), 451-481.

Venkatesh, V. & Davis, F.D., 2000. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186.

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003). User acceptance of information technology: toward a unified view. MIS Quaterly, 27 (3), 425-278.

Vijayasarathy, L.R., 2004. Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. Information & Management, 41(6), 747-762.

Wang, B. & Manning, R.E., 1999. Computer Simulation Modeling for Recreation Management: A Study on Carriage Road Use in Acadia National Park, Maine, USA. Environmental Management, 23(2), 193-203.

Yi,M.Y., Fiedler,K.D. and Park, J.S. (2006) Understanding the Role of Individual Innovativeness in the Acceptance of IT-Based Innovations: Comparative Analyses of Models and Measures. Decision Sciences, 37 (3), 393-426.

Youn, S. (2005). Teenagers' Perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach. Journal of Broadcasting & Electronic Media, 49 (1), 86-110.

Les autres documents de travail du GRANEM accessibles sur le site Web du laboratoire à l'adresse suivante : (www.univ-angers.fr/granem/publications) :

Numéro	Titre	Auteur(s)	Discipline	Date
2008-01-001	The Cognitive consistency, the endowment effect and the preference reversal phenomenon	Serge Blondel, Louis Lévy-Garboua	Théorie du Risque	octobre 2008
2008-02-002	Volatility transmission and volatility impulse response functions in European electricity forward markets	Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	octobre 2008
2008-03-003	Anomalies et paradoxes dans le cas des choix alimentaires : et si les carottes n'étaient pas oranges ?	Serge Blondel, Christophe Daniel, Mahsa Javaheri	Economie Expérimentale	octobre 2008
2008-04-004	The effects of spatial spillovers on the provision of urban environmental amenities	Johanna Choumert, Walid Oueslati, Julien Salanié	Economie du Paysage	octobre 2008
2008-05-005	Why do rational people vote in large elections with costs to vote?	Serge Blondel, Louis Lévy-Garboua	Théorie du Risque	novembre 2008
2008-06-006	Salaires, conditions et satisfaction au travail	Christophe Daniel	Economie du Travail	novembre 2008
2008-07-007	Construction communicationnelle du stock de connaissances de la compétence collective – Contribution à partir d'une conversation.	Nicolas Arnaud	Gestion des Ressources Humaines	décembre 2008
2008-08-008	On the non-convergence of energy intensities: evidence from a pair-wise econometric approach	Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	décembre 2008
2008-09-009	Production of Business Ethics	Guido Hülsmann	Economie Politique	décembre 2008
2008-10-010	Time preference and investment expenditure	Guido Hülsmann	Economie Politique	décembre 2008
2008-11-011	Le marché de la photographie contemporaine est-il soluble dans celui de l'art contemporain ?	Dominique Sagot-Duvauroux	Economie de la Culture	décembre 2008
2008-12-012	The newsvendor problem under multiplicative background risk	Benoît Sévi	Microéconomie de l'Incertain	décembre 2008
2009-01-013	Complémentarité de la collaboration électronique et de l'investissement relationnel : étude de cas exploratoire d'un SIIO dans le secteur du meuble	Redouane Elamrani, Nicolas Arnaud	Organisation	avril 2009
2009-02-014	On the realized volatility of the ECX CO_2 emissions 2008 futures contract: distribution, dynamics and forecasting	Julien Chevallier, Benoît Sévi	Finance	mai 2009
2009-03-015	The communicational making of a relation-specific skill: contributions based on the analysis of a conversation to strategy-as-practice and resource-based view perspectives	Nicolas Arnaud	Stratégie	juin 2009
2009-04-016	Le droit d'auteur, incitation à la création ou frein à la diffusion ? Une analyse empirique du cas de la création télévisuelle	Françoise Benhamou, Stéphanie Peltier	Economie de la Culture	septembre 2009
2009-05-017	Diversity analysis in cultural economics: theoretical and empirical considerations	Françoise Benhamou, Renato G. Flôres Jr., Stéphanie Peltier	Economie de la Culture	septembre 2009
2009-06-18	L'épargne retraite en entreprise : un état des lieux au regard de l'expérience américaine	Fabrice Pansard, Bruno Séjourné	Finance	septembre 2009
2009-07-19	Options introduction and volatility in the EU ETS	Julien Chevallier, Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	septembre 2009
2009-08-20	Modeling strategic interactions between firms and local authorities – The case of a biotechnology cluster	Alain Berro, Isabelle Leroux	Economie des réseaux	septembre 2009
2009-09-21	The strategy adopted by non-profit care services organizations in dealing with the new French regulatory system: strategic coalitions and reterritorialisation of activities	Isabelle Leroux, Laurent Pujol, Eric Rigamonti	Economie Sociale	novembre 2009
2009-10-22	Une nouvelle lecture du territoire par la limite	Jean-Claude Taddei	Territoire	novembre 2009
2010-01-23	Adoption of new identity-based services: Proposition of a conceptual model based on TAM, DOI and perceived risks	Caroline Lancelot Miltgen	e-marketing	juillet 2010