What is Trust in e-Government? A Proposed Typology

Panagiota Papadopoulou
University of Athens
peggy@di.uoa.gr

Maria Nikolaidou
Harokopio University of Athens
mara@hua.gr

Drakoulis Martakos
University of Athens
martakos@di.uoa.gr

Abstract

Trust in e-government is of vital importance for the effective adoption and use of electronic public services. Understanding the concept of trust and the different types it involves in the e-government context is a key challenge for both research and practice. Aiming to address this need, this paper proposes a parsimonious yet comprehensive typology of trust in e-government. Trust in e-government is analyzed into seven different types conceptualized around the different targets they are related to. Each trust type is further delineated into its composing dimensions and the approach by which it can enabled. The paper continues to present an example of the practical applicability of the proposed typology by showing how the identified types of trust have been addressed in an online taxation portal.

1. Introduction

E-government has recently witnessed an increasing diffusion and adoption worldwide. On average, over 30% of citizens in OECD countries used the Internet for interacting with public authorities in 2007. In this year, 43% of EU15 enterprises used the Internet for returning completed forms to public authorities, with this figure exceeding 70% in certain countries such as Greece, Finland and Iceland (OECD, 2008). Despite these positive results, e-government has not yet reached its full potential. The use of technology will not maintain and truly reap the benefits of e-government, if factors such as trust are overlooked (eGovRTD2020, 2007).

The establishment of trust becomes a critical success factor for e-government adoption (Park, 2008). Trust is characterized as critical in legitimating the investment in e-government services and in creating the conditions for widespread usage of services (Blakemore and Lloyd, 2008). The i2010 e-government Action Plan of the European Commission (2006) dictates as part of one of the five major objectives for e-government that by 2010 all citizens benefit from trusted services from European public administrations. According to eGovRTD2020 (2007), a European Commission co-funded project setting a roadmap of e-government research, trust in e-government is characterized as a key research theme, which includes questions such as what is trust and what kind of trust impacts e-government. This calls for an identification of the different kinds of trust related to e-government.

In an attempt to address this need, the objective of this paper is two-fold. First, it aims to identify the various types of trust of e-government around the different targets with which trust is associated and propose a typology of trust in e-government. The paper offers an analysis and categorization of trust types in e-government that aims to assist in gaining a collective and cumulative view of the concept of trust in e-government. Rather than examining factors that influence the development of trust in e-government, our focus is on exploring trust as a concept and analyzing it into its structural elements so as to provide for an overall approach facilitating the conceptualization of trust in e-government. We believe that our categorization, although parsimonious, can serve as a framework for enhancing our understanding on trust in e-government and as a guide for further research. Second, the paper intends to show the practical applicability of such a typology by presenting an illustrative example of how these types of trust have been addressed in the design and deployment of an online tax system.

The structure of the paper is organized as follows. The next section provides the theoretical background on the concept of trust and a comprehensive review of the literature of trust in e-government. The third section presents our categorization of trust types in e-government, each analyzed into dimensions and technology support. The section that follows describes the practical approach of the proposed trust types through the design and deployment of an online tax system. The paper ends with concluding remarks.

2. Background

Trust is a highly complex, multi-dimensional (Lewis and Weigert, 1985; Butler, 1991; Barber, 1983) and context-specific (Luhmann, 1979) phenomenon. It has traditionally been a concept that is difficult to define and measure (Rousseau et al., 1998; Wang and Emurian, 2005). Trust has been a topic of research in diverse disciplinary fields, such as psychology, social psychology, sociology, economics and marketing. Central to all kinds of exchange, it is a multi-faceted concept, applying to different kinds of relationship and

involving a variety of objects it refers to. This has lead to a collection of multiple, diverse definitions of trust, which is evidenced across all disciplines where trust has been studied. The difficulty in defining trust and identifying the elements that compose it is present in offline as well as online contexts, including e-government (Grabner-Krauter and Kaluscha, 2003; Wang and Emurian, 2005; Horst et al., 2007).

In all disciplines, a common and important characteristic of trust is that it involves a dyadic relationship between two parties, a *trustor*, i.e. the party that trusts, and a *trustee*, i.e. the party to be trusted. The trustee, the target of trust, is fundamental in identifying what trust is and discerning the different facets that it is comprised of. Studies on trust have focused on different objects. For example, in the context of e-commerce, research has examined trust in an online vendor, in the internet channel, in the online shopping process, in the e-commerce system, in the institutional environment.

In line with research in offline as well as online settings, trust has recently emerged as an important research topic in e-government. The augmenting research literature on trust in e-government emphasizes the value and need of trust for the successful adoption and use of e-government (Park, 2008). A growing number of studies have proposed models for trust in e-government (Warkentin et al., 2002; Horst et al., 2007; Hung et al., 2006; Tan et al., 2008; Carter and Belanger, 2005). In these models, trust has been addressed as a single construct, referring to e-government in general or to specific objects associated with it. Warkentin et al. (2002) have proposed trust in e-government as an overall belief influencing intention to engage in e-government. In some studies where trust is identified and empirically found as an important factor for e-government adoption, the conceptualization of trust is not clear in terms of the trust object it involves (Gilbert et al., 2004; Park, 2008).

Other studies are more specific with respect to the conceptualization of trust and the object it targets. Horst et al. (2007) have studied trust in e-government, referring to e-government services, as a predictor of perceived usefulness of e-government services. Carter and Weerakkody (2008) also address the e-government service as the target of trust, influencing citizen intention to use e-government. In Tan et al.'s study (2008) on citizen trust and adoption of e-government services, the object of trust is the e-government website. Hung et al. (2006) examine trust in terms of an online tax filing and payment system, affecting the attitude to using the e-government system. In Carter and Belanger (2005), trust is analyzed into two subconstructs, trust in the internet, in terms of the institutional environment for online transactions, and trust in the state government. Trust in government has also been examined in several works as an important variable associated with e-government and affected by it (Grimsley and Meehan, 2007; Welch et al., 2005; Parent et al., 2005).

It can be noted that, in the context of e-government, trust may pertain to a number of objects and can be specific to them. Arguably, a conceptualization of trust in e-government can be more concise when the object of trust is identified as part of this conceptualization. Since the objects of trust in e-government can vary, it follows that there are various types of trust in e-government that can be identified.

Based on the above, it is evident that the concept of trust is manifold and can be addressed with respect to different targets, including the *e-government service*, the *e-government system*, the *government organization* and *institution-based trust*. In addition, Horst et al. (2007) posit that the risk in e-government services can be attributed to two sources, information sent electronically and information stored electronically. Milloy et al. (2002) make a similar distinction proposing that trust development in e-commerce involves data in transit and data usage and access. As such, it can be suggested that trust in e-government also includes trust in *stored data* and trust in *transaction*.

3. Research framework

Drawing on trust literature from various disciplines, we analyze the concept of trust in the context of e-government, identifying the types it involves with respect to the object of trust. On this basis and in line with current research on trust in e-government, we propose that trust can be conceptualized and addressed with respect to the following referents: *stored data*, *transaction*, *service*, *system/infrastructure*, *government organization* and *institutional system*. Each trust type is delineated into its dimensions, thus providing a set of requirements that should be met for the establishment of the respective trust type. Based on these dimensions, we further proceed to approach trust from a technical perspective, showing how each type of trust can be practically enabled. Each trust type is mapped on technological solutions and mechanisms which provide support for its requirements.

Although the proposed types of trust are separate and distinct facets of e-government trust, involving different targets, they are also interrelated, with several dependencies among them. Institution-based trust is important for establishing other types of trust, particularly trust in stored data and trust in transaction. Trust in the system is needed for trust in stored data, trust in transaction and trust in service. Trust in

government can facilitate trust in service, trust in stored data, trust in transaction and trust in the system.

The proposed trust types and dimensions describing them are summarized in table 1 and analytically discussed in the following sections.

Trust type	Definition	Dimensions/Requirements
Trust in Stored Data	*Trust in the specific e-government stored data management (data in storage / data access and usage)*	Authentication, Authenticity, Authorization, Identity management, Confidentiality, Privacy, Integrity
Trust in Service	*Trust in the specific e-government service*	Problem responsiveness, Transparency, Efficiency, Communication, Usefulness, Ease-of-use
Trust in Information	*Trust in the information provided by e-government (information quality)*	Information Reliability/validity, Information Adequacy, Information Relevance, Information Understandability , Information Accuracy, Information Currency
Trust in System	*Trust in the system / infrastructure of the government organization*	Correctness, Availability, Security, Failure, Accountability, Response time
Trust in Transaction	*Trust in the e-government transaction (data in transit / data transmission)*	Integrity, Confidentiality, Non-repudiation, Privacy, Security
Trust in Government Organization	*Trust in the specific government agency*	Benevolence, Competence, Integrity, Predictability
Institution – based trust	*Trust in the institutional system supporting e-government*	Legal and regulatory framework, Third-party guarantees, International standards, Directives, Escrows

Table 1: E-government trust typology

3.1. Trust in stored data

Trust in stored data refers to the extent that a citizen can trust that the data collected and stored are effectively protected from potential threats. Taking into account the value and significance of the type of data stored in an e-government system, trust in stored data can be an important aspect of trust in e-government (Horst et al., 2007). It includes the assurance of data privacy and the elimination of the risk that the data stored can be accessed, disclosed, altered and used by unauthorized parties and for purposes other than the ones for which they were collected. Such threats can emanate from entities that are external to the government organization storing the data as well as from government staff who are malicious users of the data. Thus, trust in stored data is not only technology driven but is also dependent on policies defining data access control and use.

Dimensions

Trust in stored data management should include the following dimensions:

- *Authentication.* The verification of user identity
- *Authenticity.* The verification of the actual identity of the user as claimed
- *Authorization.* Ensuring that access control is in place so that access to stored data is permitted only to entities that are entitled to and according to the entity's privileges/rights of use
- *Confidentiality.* Ensuring that information is accessible only to those authorized to have access
- *Privacy.* Assurance that the data collected will be solely used for the intended purpose and that it is protected from unauthorized use/disclosure
- *Integrity.* Assurance that stored data are protected from unauthorized manipulation/alteration, either accidentally or intentionally and that they are in their original and intended state.

Approach

Trust in stored data and the underlying dimensions can be effectively enabled by available technological means. Trust in stored data dimensions can be addressed through mechanisms such as password-based authentication and expiration, role-based authentication, certificates and use of PKI, smart cards, biometric devices as well as through the definition and application of security and privacy policies. Such mechanisms may require a supporting infrastructure including a certification authority or special equipment, such as smart card readers. Some of these mechanisms can collectively ensure multiple dimensions of trust in stored data and can be combined to offer an integrated solution. For example, role-based authentication can provide support for authentication, authenticity, authorization and confidentiality, and can be complemented with a privacy policy which defines authorization and privacy levels.

3.2. Trust in Transaction

A major aspect of trust in e-government involves the communication channel through which services are delivered online and data are transferred. According to Carter and Belanger (2005) trust in the internet is required for e-government, as it represents the technology through which electronic transactions are executed. In e-government, transactions entail a considerable risk (Horst et al., 2007), which can be deemed as equal or even higher compared to that faced in e-commerce. This risk can involve monetary loss, in case of transactions related to financial issues or actual fund transfers, such as tax payment, which can usually be higher than payment for an online purchase. In addition, e-government transaction risk can also involve loss of data which are of high importance to the citizen, beyond typical privacy concerns faced in e-commerce, such as tax or health information. Therefore, trust in transaction can be identified as an important aspect for e-government. Trust in transaction refers to trust in the security and protection of data while in transit during a transaction, mainly in terms of data integrity and confidentiality. It entails that data is not accessed, tampered or distorted, either accidentally or maliciously while being transmitted.

Dimensions

Trust in transaction can be analyzed in the following dimensions:

- *Confidentiality*. Ensuring the protection of the data in transit from unauthorized access
- *Integrity.* Assurance that there is protection from unauthorized manipulation of data during transmission
- *Non-repudiation.* Ensuring that when a transaction is made, none of the parties involved in the transaction cannot repudiate, or refute the validity of the transaction
- *Privacy.* Assurance that data are not collected, stored or shared without the user consent
- *Security*. Ensuring that data are not lost while in transit and reach their destination in the original state

Approach

Trust in transaction is critical to guarantee, however, it is a type of trust which can be relatively straightforward to address with the use of current technology. Measures for establishing trust in transaction and its dimensions include the use of standard security protocols, such as SSL, TLS, HTTPS, S-HTTP and S/MIME, the use of certificates, digital signatures, cryptography/encryption algorithms and PKI. Such mechanisms have been widely used for web transactions and are mature enough to be considered as sufficiently effective in ensuring integrity, security or other dimensions of trust in transaction, while most of them, such as certificates, are adequate to jointly ensure several of these dimensions. In addition, trust in transaction and in particular, dimensions such as non-repudiation or privacy, can also require policies and business procedures.

3.3. Trust in Service

Another type of trust in e-government involves trust in the government service provided online. Carter and Weerakkody (2008) have found that trust in an e-government service is an important antecedent of citizens intention to use it. According to Horst et al. (2007), trust in e-government services is a determinant of perceived usefulness of e-government services. Citizens should trust that an e-government system will offer services that are required and that a requested service will be delivered. To be trusted, a service should be perceived as useful and easy-to-use. It should also be time and cost effective for the user, to a sufficient degree in comparison with the traditional government service channels.

Dimensions

Trust in Service involves the following dimensions:

- *Problem responsiveness.* The provision of services which effectively respond to the problem in question.
- *Transparency.* The provision of services which enable government accountability and knowledge ability of citizens regarding government policies and decisions
- *Efficiency*. The provision of services which are delivered in a time and cost effective way.
- *Communication.* The provision of services which enable a direct, bidirectional communication between the government and the citizen
- *Usefulness.* The provision of services which are useful to the citizen for the intended purpose and facilitate their tasks
- *Ease-of-use.* The provision of services which are convenient and easy-to-use

Approach

A joint effort integrating business and technical issues is needed in order to establish trust in an e-government service. Such issues pertain to the services available (e.g. problem responsiveness) as well as to the way these services are provided by the e-government application (e.g. ease-of-use). Services might imply a need for rationalization of processes, from a business viewpoint, before being technically enabled by the e-government applications so as to be trusted. The functionality of the e-government applications should be then such that allows for a full provision and support of government services and accommodate all aspects that compose trust in an e-government service. For example, an online service for tax filing should be

equivalent to that available offline, meaning that the result from using the online service should be of equal validity to that of the offline counterpart. In addition, the citizen should perceive such a service as useful, efficient and easy-to-use in order to trust it. In addition, trust in an e-government service and the dimensions associated with it should also be technically approached through applications with an appropriate interface design offering interactivity and user support.

3.4. Trust in Information

Trust in information reflects the extent to which the information obtained in an online environment can be trusted. Chopra and Wallace (2003) identify trust in information as an important type of trust in electronic settings, largely manifested through information quality indicators, such as accuracy, currency and coverage. Information quality has been found as an antecedent of trust in e-commerce (Kim et al., 2008).The quality of information provided by e-government systems is also of paramount importance for building trust in e-government According to Gilbert et al. (2004), information quality is a significant determinant of the willingness to use e-government services. Thus, trust in e-government will be largely dependent on the trust that citizens can exhibit in the information made available to them. This entails that the information is reliable, accurate, relevant and adequate for the purpose needed.

Dimensions

The dimensions of trust in information focus on:

- *Information Reliability*. The provision of information which is valid and complete so as to be reliable
- *Information Adequacy.* The provision of adequate information for the purpose requested
- *Information Relevance*. The provision of information which is relevant to the purpose requested
- *Information Understandability.* The provision of information which is understandable
- *Information Accuracy.* The provision of information which is accurate
- *Information Currency.* The provision of information which is current and up-to-date

Approach

Trust in information and its dimensions can be established through appropriate information architecture supported by integrated information and database systems. In order to be trusted, information has to be consistent in every government agency system that it may reside. In particular, information reliability, accuracy and currency require that additional technical measures and procedures are in place to ensure that the information available is always valid and up-to-date. These involve procedures for quality control of information which is uploaded on the e-government system, either manually or as input from other systems. In conjunction with standard DBMS techniques, such procedures can guarantee information validity, completeness and accuracy. Mechanisms such as time stamps of last modification should be used for information currency. Other dimensions of trust in information, such as information adequacy, relevance and understandability, are more subjective and dependent on user perceptions. These dimensions are established through an appropriate interface design and presentation of information. Finally, monitoring and continuous assessment of information quality will further facilitate trust in information.

3.5. Trust in System

Trust in the information system is recognized as an important trust domain within electronic environments (Chopra and Wallace, 2003). Hung et al. (2006) have examined this type of trust in the context of e-government with respect to an online tax filing and payment system. Trust in the system/infrastructure refers to the perception that the proper operation of the e-government system can not be compromised. It implies that the system will exhibit availability, fault tolerance and that its security and correctness is guaranteed. In addition, this type of trust involves stability in terms of system response time, as for example in case of heavy traffic load which can be possible on deadlines for tax payments.

Dimensions

The dimensions of this type of trust are:

- *Correctness*. Assurance that the system works properly and produces the correct output
- *Availability*. Assurance that the system is up and running, is fully functional whenever needed and is protected from denial of service
- *Security.* Assurance that the system is protected against intrusion threats
- *Failure.* Assurance that the system is protected against loss of user data in case of failure
- *Accountability*. Actions of an entity are traced (auditing) to allow for non-repudiation, intrusion detection and prevention and legal action
- *Response time*. The system responds to requests within a short and acceptable time period

Approach

Trust in the system and the dimensions that underpin it can be addressed through a wide range of diverse technical approaches and solutions. These include the integration and interoperability of information systems (including legacy systems) as well as the deployment and use of replication mechanisms, audit logs,

firewalls, intrusion prevention/detection mechanisms, backup utilities, recovery mechanisms and anti-virus software.

3.6. Trust in Government Organization

Trust in e-government requires trust in the government organization providing electronic services (Carter and Belanger, 2005). According to Welch et al. (2005), trust in government constitutes an important facet of trust in e-government settings. They found a bilateral positive association with satisfaction with e-government, in which trust in government is a significant contributor to e-government satisfaction and vice-versa. Similarly, Horst et al. (2007) have found trust in governmental organizations as an antecedent of trust in e-government. Therefore, the government organization is an object of trust which should be taken into account for e-government services. Since a government organization is the actual provider of e-government services, citizen attributions and perceptions of trust regarding the government organization are essential for trust in electronic government.

The concept of trust has been widely studied under the notion of beliefs about trust relevant attributes of the trustee, largely referring to the perceived benevolence, competence, integrity and predictability of the trustee. These trusting beliefs are the most frequently investigated trust construct in the empirical trust literature in e-commerce, in line with research on trust in traditional settings (Grabner-Krauter and Kaluscha, 2003; Gefen, 2002). A large stream of research in e-commerce views trusting beliefs as dimensions of an overall trust construct or as separate trust dimensions (e.g. Wang and Benbasat, 2005; Gefen et al., 2003; McKnight et al, 2002) whereas in several studies, trusting beliefs are distinguished from trust, as they are defined as dimensions of the vendor trustworthiness and are viewed as antecedents of trust (Cheung and Lee, 2006; Gefen 2002; Belanger 2002). In either case, trusting beliefs about an online vendor or other trustee constitute a key trust construct. Applying trusting beliefs in the e-government context, trust in government organization can be analyzed with respect to the perceptions raised regarding its benevolence, competence, integrity and predictability. In specific, these can be defined as follows.

Dimensions

- *Trusting Belief - Benevolence* is the belief that the e-government organization cares about the citizen and is motivated to act in the citizen interest and not opportunistically.
- *Trusting Belief - Competence* is the belief that the e-government organization has the ability or power to do for the citizen what the citizen needs done.
- *Trusting Belief - Integrity* is the belief that the e-government organization makes good faith agreements, tells the trust and fulfills promises.
- *Trusting Belief - Predictability* is the belief that the e-government organization's actions (good or bad) are consistent enough that the citizen can forecast them in a given situation.

Approach

Trust in government organization and the dimensions that compose it can not be viewed as issues that can tackled with mere technical solutions. A holistic approach, that combines technical and business aspects, is instead more suitable, to allow for an e-government system that can convey benevolence, competence, integrity and predictability of the government organization in question. Such an approach can involve an online availability of all equivalent offline services and a careful formulation and implementation of policies regarding procedures and services. As a result, a need for a reengineering of existing business processes and systems is probable to emerge. Citizens trust as well as their specific beliefs regarding a government organization can also be shaped by other factors that are not strongly related to technological enablers. Such factors include the reputation of the government organization and the previous experience of citizens with this organization. Although these factors emanate from prior knowledge from the offline environment they are important in forming citizen trust in a government organization and thus should be taken into account for e-government. Therefore, trust in a government organization can be established through a cumulative effort aggregating trust drivers from both online and offline context, with technology being only one part of them.

3.7. Institution – based trust

Institution-based trust refers to the belief that the needed conditions are present to enable one expect a successful outcome from an endeavor (Luhmann, 1991; Lewis and Weigert, 1985; Shapiro, 1987; Zucker, 1986). Rooted in sociology and economics, institution-based trust has been identified as an important type of trust, which is based on guarantees, regulations and mechanisms provided by third parties. According to Zucker (1986) it is one of the three modes of trust production in an economic environment, and is the most vital one in the absence of previous interaction and in the case of trustors with heterogeneous characteristics. As such, institution-based trust can be an important trust element in the context of e-government, especially since this context is a rather new one where the user population is diverse in terms of characteristics and has no significant prior experience.

Institution-based trust has already been transferred to the online setting where it influences trust in an e-commerce vendor (McKnight et al., 2002). Pavlou and Gefen (2004) have shown that institution-based trust in terms of feedback mechanisms, third-party escrow services, and credit card guarantees is critical for trust in online marketplaces. Cheung and Lee (2006) examined institution-based trust with respect to two constructs, legal framework and third party recognition, showing that they affect customer trust in Internet shopping. Further, Ratnasingham (2005) illustrated that institution-based trust is an important driver of trust in online inter-organizational relationships. In the context of e-government, Welch et al. (2004) highlight the importance of institution-based trust and suggest that it can be established with the use of transaction protocols that conform to general business norms on the Internet and use of third-party standards such as TRUSTe. Similarly, Warkentin et al. (2002) have proposed institution-based structures to have a positive impact on trust in e-government. According to them, institution-based trust involves third party certifications and escrows providing guarantees for the trustworthiness of an e-government agency and the expected outcome of online transactions. Overall, institution-based trust encompasses legal and technical mechanisms that enable a trustworthy and reliable e-government transaction environment. These include institutional structures providing assurance such as laws, regulations, policies, licenses, as well as technical solutions with adherence to protocols, standards and procedures.

Dimensions

- *Legal and regulatory framework.* The existence and application of laws, policies and regulations regarding online transactions and related mechanisms, such as the use of digital signatures and certificates. The aim is to provide for a legally protected environment for e-government through the implementation of clear rules and their actual enforcement.
- *Third-party guarantees.* The provision of trusted third parties offering guarantees for the identity and rights of transaction parties, such as certification authorities
- *International standards.* The use of established protocols, standards and mechanisms for online transactions
- *Directives.* The compliance with EU or other bodies directives and guidelines for online transactions
- *Escrows:* The provision of third party guarantors ensuring and verifying the expected outcome of a transaction, such as escrow services for the authorization of payments only after verifying the correctness of a transaction.

Approach

Due to its nature, institution-based trust needs to be approached from both a technical and legal perspective, as these two are intertwined for this type of trust. For example, institution-based trust might entail the use of certification authorities for using certificates and digital signatures. This also requires that a legal framework be in place, accepting such electronic means as a legal form of transaction. The institutional context associated with providing government services online should be carefully examined and taken into account before proceeding with the technical implementation and deployment of electronic services. A government organization should identify legal requirements, explore the adequacy of existing institutional structures and safeguards and propose additional measures, if needed, to ensure that online services are provided in a valid and purposeful manner. For instance, the provision of an online tax filing system, beyond adhering to current legal framework and directives, may call for new, complementary legal adjustments in order to guarantee that the use of the online system is equally valid to that offered offline. Such adjustments to the legal and regulatory environment are required for institution-based trust and should be enforced in advance of the release of the e-government system rather than considered as an afterthought. Focusing on the technical facet, examples of how institution-based trust can be technically sought are the use of international standards and protocols, certification authorities, PKI, trusted third parties (TTP) and third-party seals.

4. Promoting trust: A Taxation Portal Example

In the following, we apply the proposed E-government trust typology in the context of a taxation portal. The portal is supported by the National Ministry of Economy and Finance of a European country, which provides taxation e-services to citizens and businesses for over a decade, aiming to minimize the need of citizens' presence and enable them to carry out more than 90% of the provided services through the Internet. It is rated as the most popular e-government service in the country.

The portal has more than a million and a half registered users, while, as the number of on-line services increases, there is an average 20% increase of the portal users per year over the last three years.

The portal facilitates on-line transactional services and ensures on-line access to the databases of the legacy information system. User certification and

authorization, security, data integrity, confidentiality were some of the main issues explored during the portal implementation of the system. Provided e-services include:

- *Declaration Services.* They cover the majority of the declarations a tax payer has to submit in a periodic basis.
- *Tax payer Profile.* The e-service user is able to retrieve relative to him/her data from the legacy database.
- *Certificate Requests.* The e-service user is able to request tax certificates, for example the tax clearance certificate.
- *Added-Value Services.* These services offer citizens the ability to request and obtain personalized tax information and track the status and the progress of their cases. Moreover, a number of added value services focus to the battle against fraud, providing tools for determining the validity of presented data and documents.

The identification the proposed trust types in the taxation portal content and the actions taken to promote each one of them during the portal design and deployment phases are discussed in the following paragraphs.

Trust in Stored Data

As discussed in section 3.1, trust in stored data may be ensured through the proper adaptation of existing technology, already applied in e-commerce and e-banking sites and electronic marketplaces as well. PKI technology, role authentication and widely accepted access control and monitor schemas were adopted during the deployment of the portal. It should be noted that, since data is directly stored in the legacy information system, the authentication and authorization policies were redesigned to address data integrity issues in a uniform fashion for both Intranet (through the legacy system applications) and Internet (through the portal) users.

Trust in Transaction

As discussed in section 3.2, trust in transaction may be enabled through the proper use of current technology. Security issues, promoting trust in transaction, were handled using standard security protocols, such as SSL and HTTPS, and PKI encryption.

Although system designers couldn't take into consideration the proposed trust typology, while designing the portal a few years ago, required technologies were integrated into the portal deployment. Confidentiality and privacy of information and non-permutation of transactions are also regulated by corresponding directives and legislation, frequently issued by the Ministry as new e-services are becoming available.

Trust in Service

To be trusted an e-service should be useful and easy-to-use. As Web technology, especially the Web 2.0, is considered a standard by most Internet users, their perception of ease-of-use constantly changes. The taxation portal is maintained by a small group of experts focusing on constantly refreshing user interface without altering the portal structure. Personalized services are also provided.

Regarding usefulness, it is important to ensure that certificates issued by on-line transactions have exactly the same validity as the one's issued by corresponding authorities processing the transaction off-line. Issuing and renewing corresponding directives to maintain equivalency of validity is a task that should be regularly performed.

Trust in Information

In the e-government era, public agencies should be able to easily and accurately exchange information in an effort to provide integrated services. One of the main difficulties encountered, while upgrading the portal, is related to the provision of integrated services involving other public agencies as well. Though there are specific services, provided as web services through the Portal for other agencies to use, this is characterized as a pilot application. The main reason for the current lack of integrated e-services is the lack of trust in information quality received by other agencies.

Trust in System

As discussed in section 3.5, trust in the system may be ensured through the proper adaptation of existing technology. Regarding taxation portal, it should be noted that technology upgrades are widely publicized. Although the reasons of this policy are not related specifically in building trust, such activities contribute towards this direction.

Trust in Government Organization

Building trust in a specific Government Organization has more to do with its reputation than technology. Though, since the use of technology, as e-services, may reduce service time and promote citizen satisfaction, e-services are regarded by citizens as alternative means to communicate with the organization. Based on usability studies performed for the taxation portal, one could claim that there is a significant number of citizens considering the portal as a more reliable way to submit taxation declarations and request certificates than visiting regional taxation offices.

Institution-based Trust

Existence and consisted upgrade of a strict legal and regulatory framework promote the usage of Taxation Portal over the years. Although there are no studies connecting this fact with trust, one could safely assumed that this may be a prerequisite for the portal usage increase monitored over the last three years. Provision of almost every new e-service is regulated by complementary directives focusing especially on the electronic provision of the service and possible implications.

Conclusions

Understanding trust and the different types it involves is critical for both research and practice in the e-government context. This paper contributes to current e-government literature in a number of ways. First, it proposes that the concept of trust in e-government is manifold and identifies seven types of trust related and specific to certain targets. As such, it suggests that trust in e-government can not be treated as a general or monolithic concept but should rather be addressed as a multidimensional one which involves different types of trust, each associated with a particular referent. In this direction, the proposed typology of trust in e-government serves as a first step towards facilitating our understanding regarding the conceptualization and types of trust in the context of e-government.

As a second contribution, the paper indicates that technology, is a key enabler for trust in e-government, but is not sufficient alone. All types of trust in e-government, although to a varying degree, require a joint approach that combines technical solutions and business or legal issues.

Finally, the paper posits that the difficulty of establishing trust in e-government varies from type to type. Trust in stored data, transaction, information and system can be relatively straightforward to establish with current technology, while trust in the e-government organization, service and institution-based trust are more complicated to address.

References

Barber, B. (1983). *The Logics and Limits of Trust*. New Rutgers University Press, Brunswick, NJ.

Belanger, F., Hiller, J. and Smith, W. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes, *Journal of Strategic Information Systems*, Vol. 11, pp. 245-270.

Blakemore and Lloyd (2008). Think Paper 10. Trust and Transparency: pre-requisites for effective eGovernment. Available at: http://www.ccegov.eu/

Butler, J. K. (1991). "Toward Understanding and Measuring Conditions of Trust: Evolution of the Conditions of Trust Inventory", *Journal of Management*, Vol. 17, pp. 643-663.

Carter, L. and Belanger, F. (2005). The Utilization of e-Government Services: Citizen Trust, Innovation and Acceptance Factors, *Information Systems Journal*, 15, pp. 5-25.

Carter, L. and Weerakkody, V. (2008). E-government adoption: A cultural comparison. *Information systems Frontiers*, 10, pp. 473-482.

Cheung C. and Lee, M.K.O., 2006. Understanding Consumer Trust in Internet Shopping: A Multidisciplinary Approach. *Journal of the American Society for Information Science and Technology*, Vol. 57, No. 4, pp. 479-492.

Chopra, K. and Wallace, W. (2003). Trust in Electronic Environments. *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, January 6-9, Waikoloa, Hawaii.

Commission of the European Communities (2006). i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All.

eGovRTD2020 (2007). *Roadmapping eGovernment Research: Visions and Measures towards Innovative Governments in 2020*. Codagnone, C. and Wimmer, M.A. (eds.). http://www.egovrtd2020.org/

Gefen, D. (2002). Customer Loyalty in E-Commerce, *Journal of the Association for Information Systems*, Vol. 3, pp. 27-51.

Gefen, D. Karahanna, E. and Straub, D. (2003). "Trust and TAM in Online Shopping: An Integrated Model", *MIS Quarterly*, Vol. 27, No. 1, pp. 51-90.

Gilbert, D., Balestrini, P. and Littleboy, D. (2004). Barriers and Benefits in the adoption of e-government. *The International Journal of Public Sector Management*, Vol. 17, No. 4, pp.296-301.

Grabner-Kraeuter S. and Kaluscha, E. (2003). Empirical Research in On-line Trust: A Review and Critical Assessment, *International Journal of Human-Computer Studies*, 58, pp. 783-812.

Grimsley, M. and Meehan, A. (2007). e-Government Information Systems: Evaluation-led design for public value and client trust. *European Journal of Information Systems*, 16, pp. 134-148.

Horst, M., Kuttschreuter, M. and Gutteling, J. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands, *Computers in Human Behavior*, 23, pp. 1838–1852.

Hung, S.-Y., Chang, C.-M. and Yu, T.-J. (2006). Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly*, 23, pp. 97–122.

Kim, D.J., Song, Y.I., Braynov, S.B., Rao, H.R. (2005). A multidimensional trust formation model in B-to-C e-commerce: A conceptual framework and content analyses of academia/practitioner perspectives, *Decision Support Systems* 40 (2), pp. 143-165.

Kim, D.J., Ferrin, D.L. and Rao, H.R. (2008). A Trust-based Consumer Decision Making Model in Electronic Commerce: The role of Trust, Perceived Risk, and their Antecedents, *Decision Support Systems*, 44, pp. 544-564.

Lewis, J. D. and Weigert, A. J. (1985). "Trust as a Social Reality", *Social Forces*, 63, pp. 967-985.

Luhmann, N. (1979). *Trust and Power*, John Wiley and Sons, Great Britain.

Milloy, M., Fink, D. and Morris, R. (2002). Modeling online security and privacy to increase consumer purchasing intent. In *Proceedings of the Informing Science & IT education conference*, pp. 1093–1101.

McKnight, D. H., Choudhury, V. and Kacmar, C. (2002). "Developing and Validating Trust Measures for E-Commerce: An Integrated Typology", *Information Systems Research*, Vol. 13, No. 3, pp. 334-359.

OECD (2008). The Future of the Internet Economy; A Statistical Profile. *Organization for Economic Co-operation and Development*. Available at http://www.oecd.org/dataoecd/44/56/40827598.pdf

Parent, M., Vandebeek,, C. A. and Gemino, A. C. (2005). Building Citizen Trust through e-Government. *Government Information Quarterly*, 22, pp. 720–736

Park, R. (2008). Measuring Factors That Influence the Success of E-government. In *Proceedings of the 41st Hawaii International Conference on System Sciences*, January 7-10, Waikoloa, Big Island, Hawaii.

Pavlou, P.A. and Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, Vol. 15, No. 1, pp. 37–59.

Ratnasingham, P. (2005). Trust in inter-organizational exchanges: a case study in business to business electronic commerce. *Decision Support Systems*, 39, pp. 525– 544.

Rousseau, D., Sitkin, S., Burt, R. and Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust, *Academy of Management Review*, Vol. 23, No. 3, pp. 393-404.

Tan, C.-W., Benbasat, I. and Centefelli, R. (2008). Building Citizen Trust towards e-Government Services: Do High Quality Websites Matter? In *Proceedings of the 41st Hawaii International Conference on System Sciences*, January 7-10, Waikoloa, Big Island, Hawaii.

Wang, W. and Benbasat, I., (2005). Trust in and Adoption of Online Recommendation Agents. *Journal of the Association for Information Systems*, Vol. 6, No. 3, pp. 72-101.

Wang, Y. D. and Emurian, H. H. (2005). An Overview of Online Trust: Concepts, Elements, and Implications. *Computers in Human Behavior*, 21, pp. 105–125.

Warkentin, M., Gefen, D. Pavlou, P. and Rose, G. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets*, Vol.12, No. 3, pp. 157-162.

Welch, E.W., Hinnant, C.C. and Moon, M.J. (2005). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory*, Vol. 15, No. 3, pp. 371-391.

Zucker, L. G. (1986). "Production of Trust: Institutional Sources of Economic Structure, 1840-1920", in *Research in organizational behavior*, Staw, B.M. and Cummings, L.L. (eds.), Vol. 8, pp. 53-111, JAI Press, Greenwich, CN