Safety net? Trust and e-government.

Panos Hahamis
Mike Healy
Jennifer Iles

Westminster Business School

This is an electronic version of a paper published in the Proceedings of the 5th European Conference on e-Government (ECEG 2005), 16-17 June 2005, Antwerp, Belgium. Academic Conferences International, pp. 119-130. ISBN 190530501X.

Safety Net? Trust and e-government

Panos Hahamis, Mike Healy and Jennifer Iles
Department of Business Information Management and Operations
Westminster Business School, University of Westminster
35 Marylebone Road, London NW1 5LS, UK
P.Hahamis01@wmin.ac.uk, Healym@wmin.ac.uk, Iles@wmin.ac.uk

Abstract: Although the use of e-government by citizens is uneven, states are pressing ahead with e-government programmes despite the concerns of online users about areas such as privacy, the security of online transactions and fraud. Issues of trust and e-government are explored by looking at the Greek experience. Evidence is presented of a mismatch between the perceived importance of the trustworthiness of e-government websites and the actual priorities set by the authorities. Recommendations are made for the enhancement of public trust and confidence in government, and a model is proposed for determining the trustworthiness of e-government sites.

Keywords: e-Government, online trust, security, data protection, ICT, Greece

1. Introduction

E-government has been defined as ‘a transformation of public-sector internal and external relationships through use of information and communication technology (ICT) to promote greater accountability of the Government, increase efficiency and cost-effectiveness and create a greater constituency participation’ (United Nations, 2004). According to this definition, e-government covers a wide range of activities and can embrace local, national and international government and agencies. It would be beyond the scope of this paper to consider e-government in this totality; this paper will focus on the interaction between the broadly defined array of e-government institutions and the e-citizen, and will do so by looking at a range of e-government websites in Greece and the United Kingdom.

Any consideration of the effectiveness of e-government, at whatever level and in whatever form, needs to take full account of three crucial factors. The first is the current state of e-government diffusion within the EU. While there has been significant growth in e-government within the EU in certain sectors and certain countries, current evidence indicates that there is a significant mismatch between the aims and aspirations of e-government strategies and their implementation in reality. As has been ably outlined elsewhere (Europe’s Information Society 2005, Hahamis *et al* 2005), despite a myriad of e-government policies initiatives emanating from EU governments focused on e-government, the evidence from the EU indicates that the realisation of this vision is uneven, inconsistent and a long way from interactive, one-stop online government even in those countries considered to be in the vanguard of e-government (Wimmer 2002).

As Figures 1 and 2 indicate, there are significant technical problems to overcome before e-government can be described as widely diffused throughout the EU.

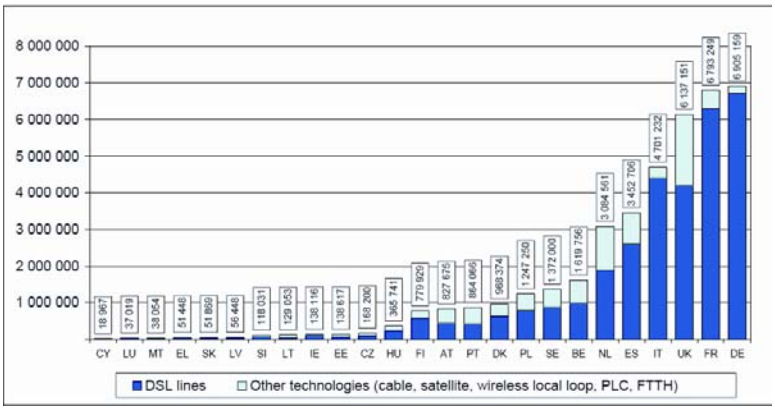


Figure 1. EU broadband penetration rate: lines per 100 population
Source: European Commission, 2005

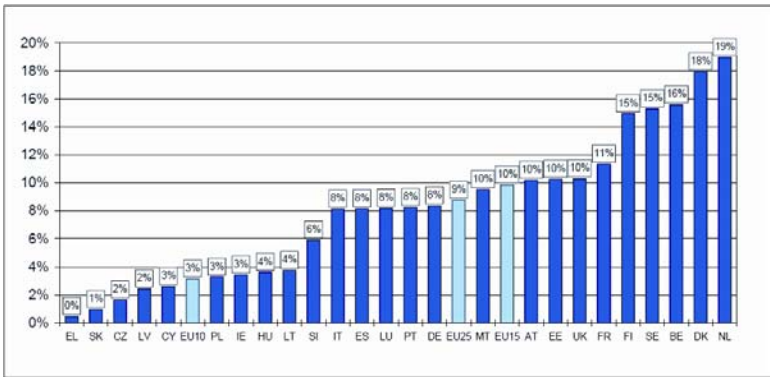


Figure 2. EU broadband lines by member state, January 2005
Source: European Commission, 2005

The low level of penetration can be seen as a weakness but it could also be viewed as an opportunity for the knowledge of non-technical issues gained from the wider experience of e-commerce to be applied to e-government projects.

The second crucial factor is an acknowledgement that consumers in the e-commerce environment are citizens in the context of e-government, and there is no Chinese wall preventing their experiences in one circumstance informing attitudes and behaviours in another.

The third factor is the environment within which e-government websites are developing. They are emerging at a moment when online trust is facing a crisis. The results of a recent set of surveys point to a developing crisis of online trust. Todos (2004), in its survey of 1200 Internet users in Sweden and the UK, found that 25% did not feel Internet banking sites were secure with 20% of UK respondents saying that had been victims of online fraud. In addition, the survey revealed that 63% of UK Internet users would consider entering their social security number online and 21% would not provide credit card details.

A study by the Gartner group and research commissioned by TNS NFO and The Conference Board (Finextra, 2005a) indicate that there has been a perceptible change in the behaviour of online users of e-commerce. The first study found that almost a third of online banking users are losing confidence in online systems and 33% of buyers online are tending to use the Internet less frequently than in the past because of security concerns. This finding has been supported by the NFO research which indicated that 41% of online users are now buying less online. In addition, a recent Forrester Research report indicates that just 30% of Web users are confident of the security of financial data when used to make transactions online (Finextra, 2005b). The significance of these and other studies is that sizable numbers of online users are beginning to consider using the Internet less for those transactions that demand inputting credit card or other personal information details. E-commerce has had to respond to these developments, and many online financial institutions are moving beyond the credit card as the prime mechanism of identification towards two-factor authentication. While these findings have immediate issues for those wishing to conduct e-commerce, they also are of direct relevance for e-government websites, particularly those that seek to encourage the online payment of various public services (Corbitt *et al*, 2003).

In addition to employing an array of technical solutions to underpin online security, there is now a strong recognition among commercial organisations about the need to adopt codes of ethics and codes of conduct, and to publicise these on their websites. The purpose of this openness with regard to ethical issues is to publicise an appreciation of the impact commerce may have on society as a whole and at the same time assure users that the organisation is socially aware.

While current research indicates the urgent need for e-commerce to address issues of online security, the issue of trustworthiness has not always been a significant aspect of commercial website development. Previously methods used to determine the effectiveness of an e-commerce website have included system design factors, users' perception and site performance with sales volume being seen as the primary measure of success (Kim & Lee, 2002). While these may have been appropriate measures during the early and developing phases of e-commerce, in a mature e-commerce environment, customer retention and trustworthiness need to be incorporated into an assessment of success.

The e-Commerce Trust Study Joint Research Project (1999) recognised the need for building trust into commercial websites if they were to succeed, and recommended six “building blocks” as the “primary components” of trustworthiness. These were seals of approval, brand recognition, navigation, fulfilment, presentation, and technology. More recent e-commerce research indicates that market orientation; site quality, technical trustworthiness and users’ web experience are seen as key elements in developing online trust (Corbitt *et al*, 2003).

Research on issues of trust in the context of e-commerce can be applied in the context of e-government. Some remarks on branding are appropriate because brand influence is seen as an increasingly important part of building online consumer confidence. The difficulties associated with trust building from a branding perspective in e-government at local, national and international levels is compounded by contentious political and social policies that at first sight appear tangential to the e-government project but which in reality have a profound impact on the e-citizen’s view of e-government. Three examples will suffice to illustrate the argument. The recent votes in France and Denmark rejecting the EU constitution were in effect a rejection of the economic policies enshrined in that constitution. Voters did not have confidence in the motives behind and policies of the EU economic strategy. In the UK, there is widespread opposition to the introduction of identity cards by a government perceived as untrustworthy following its involvement in the war and occupation of Iraq.

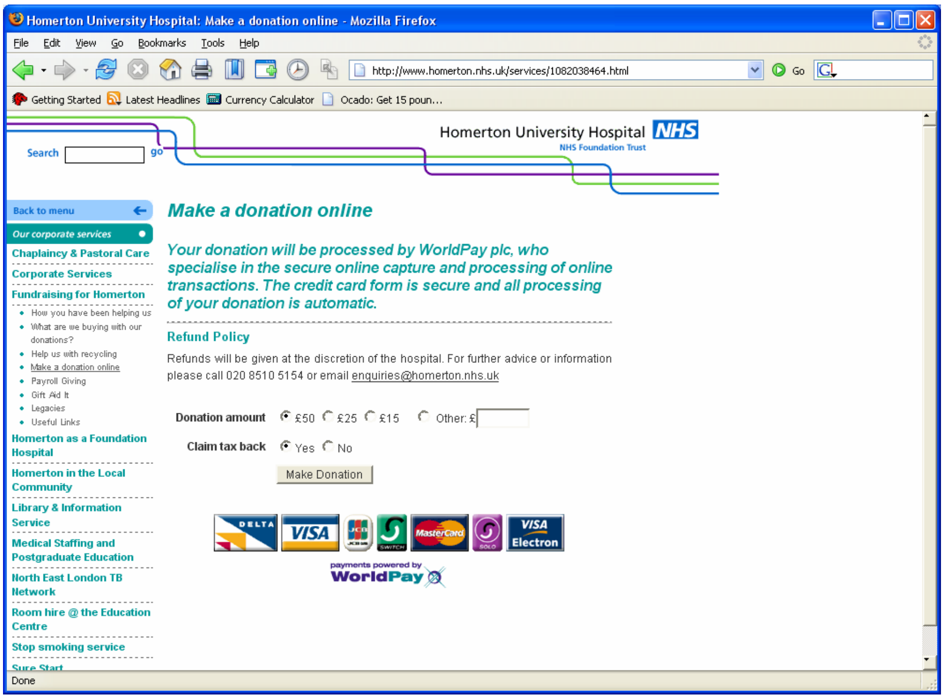
While the problems associated with both these instances are essentially political, both rely on the extensive use of ICT to successfully outcome the projects. The development of an extensive ICT network throughout the EU is seen as crucial for the delivery of the Lisbon strategy[1], and a deeper, wider integration of Europe. Similarly, the UK’s identity card scheme depends upon the implementation of biometric storage and reading devices linked to an all-embracing database. In both cases, dubious political decisions and associated technical developments are perceived as being the problem. At a local level, attitudes towards a local government website are bound to be influenced by the impact of council policy generally. If, say, a local authority is refusing to publish details of its contracts with private companies because of so-called commercial confidentiality, it cannot convincingly claim to be supporting transparency on its website.

Mention has already been made of how e-commerce websites are increasingly highlighting symbols, images or content that re-enforce the ethical stance of these organisations. However, e-government websites often fail to carry or emphasise any references to such codes or policies, thereby encouraging the belief that such codes do not exist. For example, of the websites for the London local government boroughs, only 14 out of 32 had links to a privacy policy on their home page. In addition, the overwhelming majority of those with a privacy link had buried it right at the bottom in the footer of the home page. A further, perhaps more profound, weakness from a trust building perspective was the absence from all but one website of any sign or symbol denoting a secure site. This is a serious problem for two reasons. The first is that all the websites encourage users to make online payments for a range of services without indicating how secure the site is for handling such payments. Secondly, the absence of secure payment symbols can be interpreted as indicating that this issue was not considered as important, if it was considered at all, when the site was designed and published online.[2]

This problem is not one simply restricted to local government websites in the UK. Figure 3 shows a page taken from the Homerton Hospital NHS Trust website. The problem with this page is that while it seeks to assure users that providing credit card details online is safe, a statement of some dubious nature as the discussion above indicates, there is very little else on the page that encourages a sense of trustworthiness. The inclusion of a name rather than an anonymous phone number and e-mail address would have been a step in the right direction.

[1] The European Summit at Lisbon in June 2000 set the strategic goal of improving employment and social cohesion and making the European Union the most competitive and dynamic knowledge-based economy in the world. In June 2000, the Feira European Council launched eEurope, a plan to harness the potential of the information society to meet the goals of the Lisbon strategy.

[2] Evidence obtained from an examination of the local government websites for London including the GLA.



Homerton University Hospital: Make a donation online - Mozilla Firefox

http://www.homerton.nhs.uk/services/1082038464.html

File Edit View Go Bookmarks Tools Help
Go
Getting Started
Latest Headlines
Currency Calculator
Ocado: Get 15 poun...
Homerton University Hospital NHS
NHS Foundation Trust
Search
go
Back to menu
Our corporate services
Chaplaincy & Pastoral Care
Corporate Services
Fundraising for Homerton
How you have been helping us
What are we buying with our donations?
Help us with recycling
Make a donation online
Payroll Giving
Gift Aid It
Legacies
Useful Links
Homerton as a Foundation Hospital
Homerton in the Local Community
Library & Information Service
Medical Staffing and Postgraduate Education
North East London TB Network
Room hire @ the Education Centre
Stop smoking service
Sure Start
DELTA
VISA
JCB
SWITCH
MasterCard
SOLO
VISA Electron
payments powered by WorldPay
Done

Make a donation online

Your donation will be processed by WorldPay plc, who specialise in the secure online capture and processing of online transactions. The credit card form is secure and all processing of your donation is automatic.

Refund Policy

Refunds will be given at the discretion of the hospital. For further advice or information please call 020 8510 5154 or email enquiries@homerton.nhs.uk

Donation amount ● £50 ○ £25 ○ £15 ○ Other: £

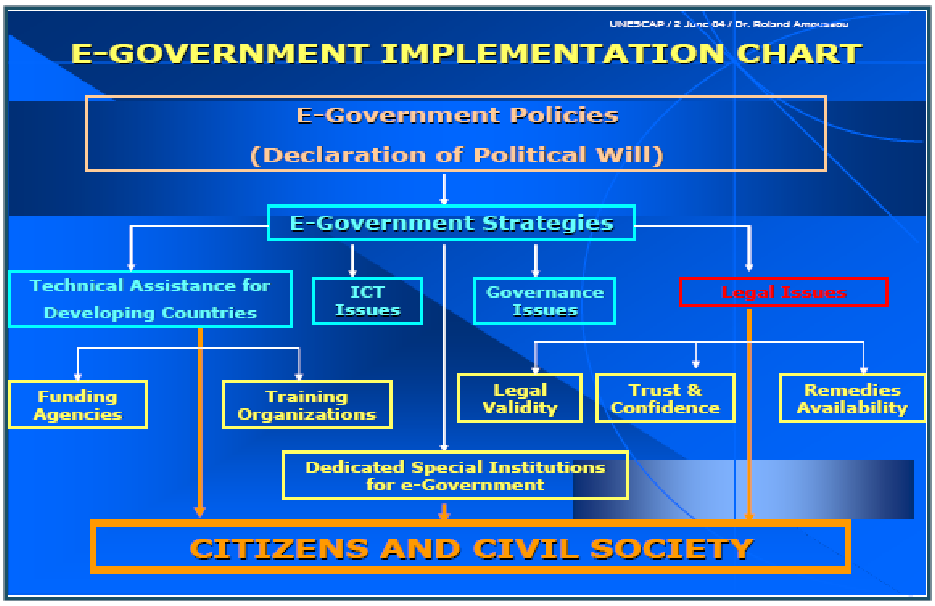
Claim tax back ● Yes ○ No

Make Donation

Figure 3. Hospital online donation web page

The above examples illustrate the problems emerging with e-government. If it is valid to generalise from these experiences, it would seem that e-government websites appear to replicate the weaknesses of early commercial websites as well as those currently exhibited by intranets.

It is however encouraging to note that references to the issue of online trust are beginning to appear in policy documents associated with the development of e-government. The United Nations (2004) recognised in Bangkok that e-government systems need to be trustworthy. “Security, privacy, reliability and business intelligence were needed for trustworthy computing. A responsible leadership on public policy issues was required and an openness of the system was also needed.” Figure 4 is indicative of the way in which trust and confidence issues are increasingly seen of some importance in this arena. However the discussion often lacks a full appreciation of the trust factor, even when an attempt is being made to develop a holistic approach to the problems associated with e-government.



UNESCAP / 2 June 04 / Dr. Roland Amoussou

E-GOVERNMENT IMPLEMENTATION CHART

E-Government Policies

(Declaration of Political Will)

E-Government Strategies

Technical Assistance for Developing Countries

ICT Issues

Governance Issues

Legal Issues

Funding Agencies

Training Organizations

Legal Validity

Trust & Confidence

Remedies Availability

Dedicated Special Institutions for e-Government

CITIZENS AND CIVIL SOCIETY

Figure 4. E-government implementation chart
Source: United Nations (2004)

E-government websites could facilitate, encourage and strengthen the relationships between the e-citizen and a wide range of governmental and quasi-governmental institutions at national and local levels. At the very centre of this relationship is the experience of the e-citizen. The problem is that this approach runs counter to the current dominant philosophy of e-government, which focuses on the delivery of public services with an increasing emphasis on facilitating inter-agency relationships.

2. e-Government in Greece

2.1. Background

A White Paper published by the Greek Government (2002) states: "Freedom of information and privacy protection are inherent characteristics of the democratic structure and organisation of society". According to the European Commission's Interoperable Delivery of European government Services to public Administrations, Businesses and Citizens (IDABC, 2005), there is currently no dedicated e-government legislation in Greece. There is however legislation on Data Protection/Privacy (Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data as amended on 2001), on e-Commerce (Presidential Decree 131/2003 on e-commerce) and on e-signatures/e-identity (Presidential Decree 150/2001 on digital signatures).

There is also a dedicated Administrative Authority in Greece, namely the Hellenic Data Protection Authority. Its mission is: "to supervise the implementation of Act 2472/97 and the totality of regulations pertaining to the protection of the individual with respect to the processing of personal data," (HDPA 2001).

2.2. Research methodology

In order to collate data, it was decided to use a combination of methods. As Mingers (2001) argues, different research methods focus on different aspects of reality and therefore a richer understanding of a research topic will be gained by combining several methods together.

A content study by direct observation of local government websites in Greece was conducted between 10th and 18th August 2004. The Hellenic Agency for Local Development and Local Government (EETAA) maintains a database of all local authorities in Greece that have a web presence, on its website.[3] It has five categories of authorities, and in each category, authorities are listed in alphabetical order. Only the websites listed for the categories of Prefecture Authorities (Νομαρχίες), Municipalities and Rural Communities (Δήμοι και Κοινότητες) were visited. Although Municipalities and Rural communities were listed in two separate categories, for practical reasons, the results of this research were merged.

Subsequent to the content study, interviews with the major players for the e-government in Greece were carried out. They were mainly semi-structured interviews which enabled the collection of detailed data that would probably not be accessible using techniques such as questionnaires.

The secretary general for the Information Society was interviewed and, following his recommendation, the manager of the Operational Programme for the Information Society in Greece (OPIS) was interviewed too. The Information Society Secretariat General is a Ministry of Economy and Finance Agency and thus responsible to promote the Information Society in Greece as well as handle all European Union funding destined for these programmes. Telephone interviews were also conducted with officials from the Hellenic Agency for Local Development and Local Government, the Central Union of Municipalities and Communities of Greece and the General Secretariat of Public Administration and E-Government (an Agency of the Ministry of the Interior).

For the survey, among the reasons an online questionnaire was chosen, accompanied by e-mail invitation to the respondents to participate, was the response speed and survey cost as well as the distance. It was impractical and financially unfeasible to access the sample in Greece.

The questionnaire was based on the February 2003 Haart/Teeter (2003) national public opinion survey of government workers on e-government, conducted on behalf of the US Council for

[3] www.eetaa.gr/cgi-bin/msql/foreis/01

Excellence in Government. Its target group was employees of government/local government agencies and authorities in Greece.

Among the questions asked was how important is it for government agencies or divisions to communicate clearly to the users the privacy and security policies that apply to their websites. Another asked what should be made government's top priority for government websites, and a further question asked about perceived obstacles to e-government.

The purpose of conducting a survey is not only to gather information about the subjects surveyed, but ultimately to be able to make statements about a larger group or population. In order that the inferences made about the population are accurate, a representative sample is vital. The sampling strategy used was probability sampling, with a combination of random and systematic sampling. Respondents were chosen at random from the alphabetical lists of local authorities in Greece who have a web presence, which the Hellenic Agency for Local Development and Local Government maintains on its website. Other respondents were added from the list of the Regional Authorities which the Central Union of Municipalities and Communities of Greece maintains on its website. In addition, a small percentage of respondents were added whether for information only or out of courtesy for their help or contribution to this research.

An e-mail was sent to the respondents explaining the purpose of this survey, how the sample was chosen and containing contact details as well as a disclosure statement that the questionnaire is confidential, anonymous and there is no obligation arising upon its completion. There was also an attachment to the email of the questionnaire as an MS Word form that could be downloaded. Thus, three choices of completing and returning the questionnaire were given: online, by e-mail and by post.

A study of the existing (admittedly sparse) academic literature was undertaken, and a number of surveys of the population's use of ICT and the Internet penetration in 2003 in Greece were studied and analysed.[4] European Commission, National Government and Government Agencies' White Papers and other studies were also examined.

2.3. Data Analysis

According to the Central Union of Municipalities and Communities of Greece (ΚΕΔΚΕ, 2004), there are two tiers of local government and regional administration in Greece, as a result of the recently reform under the Kapodistrias Municipal Code 1995 which came into force in 1999:

- 13 regions (peripheries)
- 51 prefectural authorities, including 3 extended prefectural authorities and
- 1,031municipalities (130 urban municipalities – dimi and 901 rural communities – kinotites)

Under the Kapodistrias reform, the number of local authorities was reduced from 5,775 to 1,031 in order to create a strong first-tier local government. Out of the 1,031 local authorities, 641 were listed on the EETAA database but only 335 had a website, 32% overall. The operational state of these 335 websites was as follows: 76% working, 21% not working and 3% under construction. On the other hand, out of the 51 prefectural authorities, 46 were listed, all with websites, 90% overall. Four (4) websites were not working, whilst 1 was under construction. Most of the authorities listed, provided an email contact address on the EETAA list. Nevertheless, it was discovered subsequently that not all were operative, as 16% out of 248 emails bounced back whilst trying to administer the survey questionnaire.

The website content study showed that only one rural community had a privacy and data protection statement link on its website but even that returned an error page. Four prefectural authorities had some kind of privacy and data protection statement and/or a disclaimer on their websites with one of them being mainly a disclaimer. Notably, both Athens prefecture and Athens municipality authorities did not have any kind of statement on their websites. In general, website design was outsourced with a few exceptions where the internal IT department or the relevant Municipality Development Agency was commissioned. Most of the websites therefore had links of the type 'contact the webmaster' or 'feedback form'. None of the websites studied had a sign or symbol denoting a secure site.

[4] Including ebusinessforum.com <http://ebusinessforum.com>, the National Statistical Service of Greece <http://www.statistics.gr/Main_eng.asp > and a research company AGB Hellas <http://www.agb.gr>

An examination of the online e-government survey evidence shows that the adoption of a website by municipal and rural community authorities in Greece is a recent phenomenon. The response rate of the survey (18%), along with the lack of or limited responses from Regional and Prefectural Authorities indicates that there is a different perception of e-government in different levels of local government. Furthermore, although the majority of the respondents were working for Municipalities and Rural Communities, there were a number of responses from Ministries as well the National School of Public Administration & Local Government and the Hellenic Agency for Local Development and Local Government. These respondents however have a stake in promoting e-government as they are responsible for the proliferation of ICT in public administration. The majority of the respondents were administrative personnel, in elected mayor-run councils as this is the current structure of local government in Greece, although there were some technical personnel and an elected respondent. As Moon (2002) has argued, managers in council-manager municipal governments tend to be more proactive in introducing technological innovations such as web technology to the public sphere than mayors who are elected officials and tend to hold political views. The fact that replies were made up to the end of November 2004 (way beyond the deadline given to the respondents) could be attributed to the reluctance of employees of authorities and local authorities to act without prior authorisation from above.

Online security and privacy were rated highly on the agenda by the respondents, both in terms of informing and reassuring the citizen, and as a top priority for their authorities' websites. Other priorities included the need for a wider participation and openness and providing more user-friendly interfaces. After all, "Small to medium sized public organisations (SMPOs) share some of their e-Government requirements with their larger counterparts, such as the pending needs for interoperability, security and user friendliness," (Kaliontzoglou *et al*, 2005). The survey results suggest that there are serious institutional obstacles to e-government evolution such as the lack of familiarisation of employees to new technologies and lack of management support. The lack of financial resources and the issue of security/privacy are considered to be major obstacles too. These barriers, in combination with the inability to recruit qualified personnel and the entrenched operating procedures, highlight the need for institutional change and re-engineering of the business processes.

According to a survey by AGB Hellas (2004), the overwhelming majority of Internet users in Greece is between 25-34 years old (four in ten), hold at least a Lyceum Certificate (further education) and been in the cyberspace during the last three years (68.7%), whilst allocating at least one hour daily (71.4%) for their surfing on the Internet. The majority of users (76.5%) appear to be using the Internet in order to search for information and 59.4% for communication. It is interesting however to note that whilst 63.8% of the users surveyed are reluctant to use their credit card for transactions online, and 41.9% worries about data protection issues, 59.6% resort to the Internet in order to conduct banking transactions and pay utility bills online. Finally, 57% of the users send their own message to the government asking for more electronic services.

A number of surveys examined show that broadband and Internet penetration rates are very low in Greece. It is currently a top priority for the Secretariat for the Information Society to bridge the gap and reduce the digital divide, by adapting a number of policies within the OPIS. One of them is the project 'Go on- line'[5] which has been launched by the Ministry of Development and aims to introduce 50000 SMEs to the digital economy (Priftis, 2003).

2.4. Findings

There were concerns expressed in this study about the security and privacy issues that derive from a fully transactional e-government implementation as well as the interoperability standards that any authority's online presence has to conform to.

There is not a coherent national strategic framework in place, outlining the objectives, milestones, funding and potential for a uniform e-government adoption by the local authorities apart from the OPIS programme.

Despite the sparse legislation already in place in Greece, the adoption of measures to safeguard privacy and security during online transactions with the citizen is slow. The General Secretariat for Information Systems at the Greek Ministry of Finance (GSIS) along with the City of Edinburgh Council

[5] www.goonline.gr

(CEC) participate on the implementation of a ‘Framework for e-Government Services’ of which one of the main outcomes is a project called *Smart Gov* by the European Commission’s Information Society Technologies (IST) Directorate. “The framework encompasses models that support cooperation and models that support the acceptance of online transaction services, focusing on issues such as privacy, trust, and satisfaction” IST (2005). The GSIS however is a central government authority.

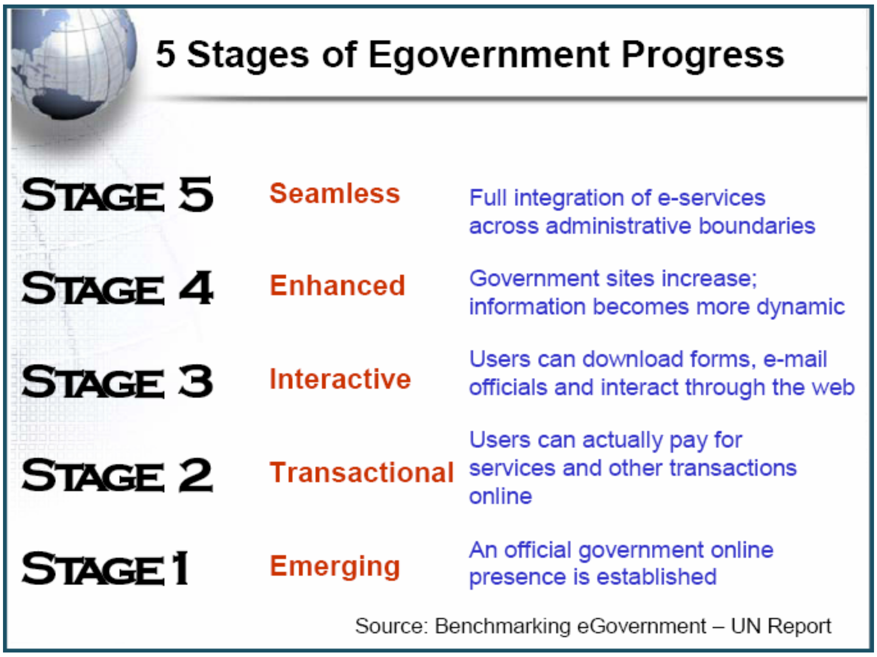
Local government in Greece has encountered and will continue to do so, a number of obstacles to the adoption of e-government. The most important ones are the lack of financial resources, lack of support from the management and elected leaders, technology familiarization and the issue of security/privacy.

3. A model for assessing trustworthiness

Having identified a number of insights into the nature of the problem, the next step is to suggest possible tools for assessing trustworthiness of e-government websites. Thus the paper will now discuss the use of a model that can help e-government website designers develop strategies for creating, implementing, monitoring and up-dating the success of those elements that seek to stimulate trustworthiness.

It is appreciated that while will be a degree of overlap between some of the components; it is possible to delineate clearly identifiable building blocks that contribute to website trustworthiness.

Figure 5 is indicative of the problem in that it usefully lays out a possible road map for designing an ongoing e-government project. However, progress is essentially determined by the success of an e-government strategy from a technical perspective.



5 Stages of Egovernment Progress

STAGE 5	Seamless	Full integration of e-services across administrative boundaries
STAGE 4	Enhanced	Government sites increase; information becomes more dynamic
STAGE 3	Interactive	Users can download forms, e-mail officials and interact through the web
STAGE 2	Transactional	Users can actually pay for services and other transactions online
STAGE 1	Emerging	An official government online presence is established

Source: Benchmarking eGovernment – UN Report

Figure 5. Stages of e-Government progress
Source: United Nations (2004)

Absent from the above model is any discussion about the extent to which an e-government facility is considered trustworthy from a user’s perception. This tends to be a common omission from diagrams seeking to layout guidelines for effective e-government websites. There is a weakness even as the diagram stands in that from a solely technical perspective, it fails to include reference to appropriate security technology. As been mentioned above, the problems associated with the vulnerability of online credit cards have led financial institutions to adopt a two-factor approach to online authentication. It appears that this lesson has yet to be learned by the builders and managers of e-government websites. It could be argued that the overall effectiveness of an e-government website would be itself promoting trustworthiness. While such a view may have some validity, it ignores the need to address the developing crisis of online confidences referred to above and the need to include clear and overt signals that a given website can be trusted.

The model shown in Figure 6 attempts to shift a focus away from what should already be good website design practice onto the issue of trustworthiness. This should not be taken to mean that other issues, such as the use of appropriate security technology and website navigation and so forth, are neglected; on the contrary, these should be rigorously enforced. The model includes a number of key elements that go to make up website trustworthiness such as the presence of relevant symbols and icons indicating that a site is secure and is designed to be applied in a number of contexts. Many e-government websites are at different stages of development and the relative importance of each element most be calculated with this in mind. Thus for a non-interactive website that simply delivers information, issues such as personalization and ownership cannot be seem as important. However, even at this early stage, the prominent references to policies governing privacy are critical for engendering trust. As the website matures, matters such as ownership, feedback, and personalization become extremely relevant.

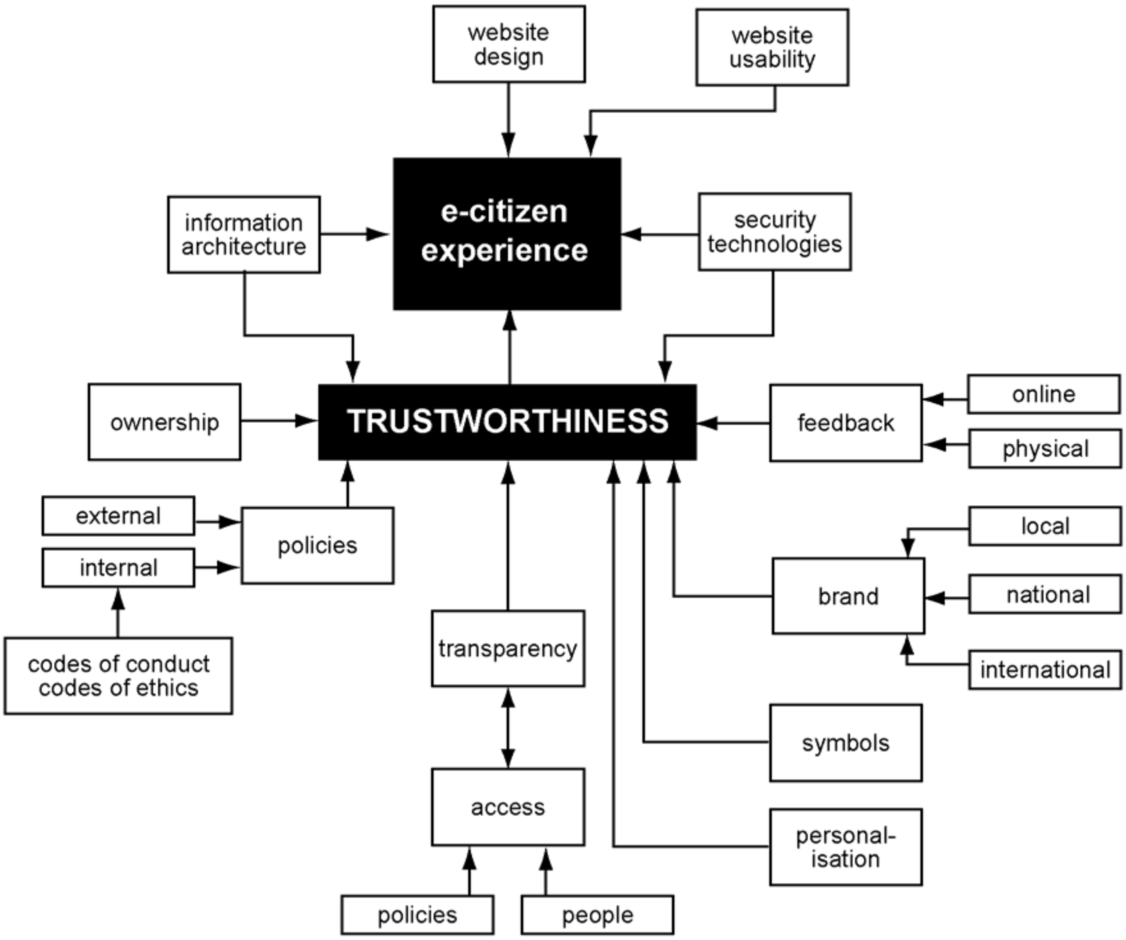


Figure 6. Elements of website trustworthiness

The model needs to be tested and it should inform the next stage in the process of assessing trustworthiness by guiding the construction of measures designed to gauge how far a site can be described as trustworthy. It is beyond the scope of this paper to develop this theme and it will be the subject of subsequent research and further papers. All good website design recognizes the iterative process and the same must be said of building trustworthiness. Thus, it is likely that the model suggested above will require refining and expanding as the research proceeds and as the context within which e-government develops also changes.

However, the defining principles governing the emergence of e-government must now flow from the experience of the e-citizen. And at the heart of that experience must be a positive relationship based on trust.

References

AGB Hellas (2004) Survey for the Use of the Internet in Greece. *The Who is Who of the Greek User* Online at http://www.ert.gr/eidiseis/newsDetails.asp?ID=67547 [accessed 07/08/04].

Corbitt, B. J., Thansanki, T. and Yi, H. (2003) 'Trust and e-commerce, a study of consumer perceptions' *Electronic Commerce Research and Applications*, Vol. 2, Issue 3, Autumn 2003 pp. 203-15.

e-Commerce Trust Study Joint Research Project (1999) Cheskin Research and Studio Archetype/Sapient

European Commission (2005) Communications Committee working document: *Broadband access in the EU: situation at 1 January 2005*, online at http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/broadband/broadband_data_01012005.pdf [accessed 30/05/05].

Europe's Information Society (2005) Culture and Society: eGovernment: *Better Public Services*, online at http://europa.eu.int/information_society/soccul/egov/index_en.htm [accessed 18/07/05].

Finextra (2005a) 'Phishing and security breaches are damaging consumer trust in e-commerce' online at http://www.finextra.com/fullstory.asp?id=13875 [accessed 28/06/05]

Finextra (2005b) 'UK banks to establish two-factor security standard' online at http://www.finextra.com/fullstory.asp?id=13529 [accessed 26/06/05].

Greek Government (2002) White paper: *Greece in the Information Society: Strategy and Actions*. Athens: Greek Government. Online at http://en.infosoc.gr/content/downloads/WPEngFINAL.pdf [accessed 15/0505].

Hahamis, P., Iles, J. and Healy, M., 2005. e-Government in Greece: opportunities for improving the efficiency and effectiveness of local government. *5th European Conference on E-Government (ECEG 2005), 16-17 June 2005 Antwerp*.

Hart/Teeter (2003) *National Public Opinion Survey for the Council for Excellence in Government* (Study #6943b).

HDPA (2001) Hellenic Data Protection Authority: *Mission*. Online at http://www.dpa.gr/authority_eng.htm [accessed 15/07/05].

IDABC (2005). *eGovernment Factsheet – Greece – Legal framework*. Online at http://europa.eu.int/idabc/en/document/1172/397 [accessed 15/07/05].

IST (2005) Features: *Easier online transactions for e-government*. Online at http://istresults.cordis.lu/index.cfm?section=news&Tpl=article&BrowsingType=Short%20Feature&ID=62569 [accessed 15/07/05].

Kaliontzoglou, A., Sklavos, P., Karantzias, T. & Polemi, D. (2005) A Secure e-Government platform architecture for small to medium sized public organizations. *Electronic Commerce Research and Applications*, Vol. 4, Issue 2, pp. 174-86

ΚΕΔΚΕ (2004) General Data. *Central Union of Municipalities & Communities of Greece*. Online at http://www.kedke.gr/generalData_english.htm [accessed 08/08/04].

Kim, J. & Lee, J. (2002) 'Critical design factors for successful e-commerce systems'*, Behaviour and Information Technology*, Vol. 21, No. 3, pp. 185-99.

Mingers, J., (2001) Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research,* 12 (3), pp. 240-59.

Moon, M. J. (2002) The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review*, 62 (4), pp. 424-33.

Priftis, A. (2003) *Request for Information on Policies to Reduce the Digital Divide – Greece*, Special Secretariat of the Information Society, pp. 1-11.

Todos (2004) Press release: *One out of four do not trust their Internet bank.* Online at http://www.todos.se/Todos/news/pressreleases/Pressrelease041125.pdf [accessed 15/04/05]

United Nations (2004) *Implementing e-Government: Report of the Regional Workshop Bangkok, 31 May–4 June 2004*. Online at http://unescap.org/icstd/Pubs/st_escap_2342.pdf [accessed 30/05/05].

Wimmer M. A. (2002) ‘A European Perspective towards online one-stop government: the eGOV project’, *Electronic Commerce Research and Applications*, Vol. 1, pp. 93-102.