European and Mediterranean Conference on Information Systems (EMCIS) 2006,
July 6-7 2006, Costa Blanca, Alicante, Spain

GENERATING CITIZEN TRUST IN E-GOVERNMENT USING A TRUST VERIFICATION AGENT: A RESEARCH NOTE

Rana Tassabehji, School of Management, University of Bradford, UK
r.tassabehji@university.ac.uk

Tony Elliman, Information Systems Evaluation and Integration Network Group (ISEing)
School of Information Systems, Computing & Mathematics, Brunel University, UK
tony.elliman@university.ac.uk

Abstract

This is an eGISE network paper. It is motivated by a concern about the extent to which trust issues inhibit a citizen's take-up of online public sector services or engagement with public decision and policy making. A citizen's decision to use online systems is influenced by their willingness to trust the environment and agency involved. This project addresses one aspect of individual "trust" decisions by providing support for citizens trying to evaluate the implications of the security infrastructure provided by the agency. Based on studies of the way both groups (citizens and agencies) express their concerns and concepts in the security area, the project will develop a software tool – a trust verification agent (TVA) - that can take an agency's security statements (or security audit) and infer how effectively this meets the security concerns of a particular citizen. This will enable citizens to state their concerns and obtain an evaluation of the agency's provision in appropriate "citizen friendly" language. Further, by employing rule-based expert systems techniques the TVA will also be able to explain its evaluation.

1 INTRODUCTION

The major aim of this paper is to present the case for building a trust verification agent (TVA) to bridge the gap in interpretation of security information between e-government service providers and citizens. This paper defines e-government and the context in which the TVA will operate, which involves both citizen facing front-end and back-end e-government services. A review of the literature and empirical studies on e-government identifies the criteria for adoption of e-government from a citizen and government perspective, which highlights trust and security as major factors. An examination and classification of trust models for e-commerce and government are consolidated to define trust and security in the context of this project. Having established that security and its dissemination to citizen users of e-government service is an important factor in building trust, the concept of the trust verification agent is presented. The TVA will provide citizens with the ability to judge the level of security provided by an e-government application. This will enable them to take critical decisions about their ability to trust the service and increase citizen take up of services. Technical descriptions of the security infrastructures are complex and difficult for the citizen to understand and this project will bridge the gap by developing an independent TVA that can translate these descriptions into appropriate language for the citizen.

2 DEFINITION OF E-GOVERNMENT

According to the UN World Report on the Public Sector, "E-government at the Crossroads", 173 out of 191 member countries, over 90%, operate government websites (Swartz 2004). E-government is closely linked and shares similar characteristics with, the field of e-commerce and e-business in terms of the use and implementation of Internet technology; re-engineering inter and intra-organisational processes and structures;

and generating new services, products and channels for the end-users or consumers. The main drivers to implement "e-government" emanate from the exemplar of the private sector's implementation and use of e-commerce and e-business. Customers/citizens expect the same level and type of service from government that they receive from the private sector, while government itself anticipates increased efficiency, productivity improvements and cost savings similar to those experienced by the private sector (Stamoulis et al. 2001, Clark, 2003).

Despite these similarities, e-government is unique because of its role in the interaction between government and its citizens and the governance of nations. It is a complex mix of a variety of issues from a range of disciplines, such as social and political science, management of change and innovation, information technology and information systems, law and international studies to name but a few. Grant and Chau (2005) capture the essence of this complexity on their definition of e-government as,

"A broad-based transformational initiative enabled by leveraging the capabilities of information and communication technology;(1) to develop and deliver high quality, seamless, and integrated public services; (2) to enable effective constituent relationship management; and (3) to support the economic and social development goals of citizens, businesses, and civil society at local, state, national, and international levels. (Grant and Chau, 2005:9)

3 CONTEXT OF E-GOVERNMENT

Research from practitioners and academics see the development of e-government in stages (Deloitte Research 2000; Watson 2001; Finger & Pecoud 2003; Marchionini et al. 2003; Clark 2003; Tan & Pan 2003; West 2004; Shackleton et al. 2004; Ke & Wei 2004; Vriens et al 2004) similar to those identified in e-commerce literature (Earl 2000; Tassabehji 2003). From a review of the literature summarised in table 1, the development of e-government can be seen as undergoing four major phases. These can be identified as the application of e-technology to government services which is a basic informational stage, followed by transactional stage involving more two way interactions with citizens. Both of these stages focus on the front-end customer interfacing aspect of e-government services. The next stages include the integration of systems to provide "joined up" seamless e-government service and ultimately reaching a transformational stage where there is a complete assimilation of e-technology and management processes into the organisation that it is no longer "e" government, but becomes government per se. These later stages focus on back-end systems development to facilitate delivery of efficient and effective service to citizens. A review of the different e-government services and the frequency of their adoption was carried out based on the UN e-Government Readiness report 2005 ….. and examples of the services that fall into the different phases are summarised in table 1.

Stages	E-government Services	Status*
Information	Information, brochures, leaflets, downloading forms	1
Transaction	e-voting, completing forms on-line, filing taxes online, renewing driver's licenses, applying for passports, unemployment benefit; obtaining birth certificates/marriage licences	2
Integration	Integrating front and back-end systems across all departments to enable information sharing and a single point of access for citizens to multi-layered government services.	3
Transformation	At this stage there will be personalisation of e-government services and a 1:1 relationship with government across all departments	4
**** Status of Implementation of e-government across the world*** ***1=Widely implemented 2=Patchy implementation of some of these services 3= Rare implementation in some progressive and single layer governments 4= Not yet implemented***		

Table 1. Prevalence of E-government Services

Although the stage model implies a chronological progression, this is not strictly the case, as the speed with which technology is advancing enables organisations to implement e-government at any stage dependent on their commitment, strategy and available resources. The project here will be dealing with all the stages of e-government both from the front end and back end perspectives.

4 ADOPTION OF E-GOVERNMENT SERVICES

The majority of e-government empirical studies from practitioners such as Accenture, and international organisations such as the UN and OECD, focus on descriptive analyses of the "state of e-government", "e-government readiness" in nations, or barriers and drivers to its implementation and advancement (Swartz, 2004). From an academic perspective, empirical studies have been largely focused on deeper understanding of adoption of e-government services using Davis' Technology Acceptance Model (TAM) and Theory of Planned Behaviour (TPB). Abundant empirical evidence suggests that theory of planned behaviour effectively explains individual intentions and behaviour in adopting new technologies (Hung et al. 2006), where TAM focuses on perceived benefits but TPB enables positive as well as negative beliefs. E-government is not an exception to this rule, but as we will see later, is more complex. From a review of this literature, we can summarise the factors influencing the adoption of e-government services from two perspectives. Namely:

- ***The citizens' perspective*** **-** The factors for adoption include familiarity or experience with e-services and government; ease of use; perceived usefulness; trust in the organisation and service for example interacting with government on-line and the perceived safety/risk of providing information to government; perceived quality of information and service; and perceived behavioural control and subjective norms (Clark 2003; OECD Observer 2003; Shetty 2003; Gilbert et al. 2004; Rohleder and Jupp 2004; Skok and Ryder 2004; Swartz 2004; Carter and Belanger 2005; Horst et al. 2006; Hung et al. 2006).
- ***The government's perspective*** **-** The barriers to adoption are the complexity of the department/agency paradigm; poor IT infrastructure; HR constraints such as lack of skilled personnel; and lack of financial resources; a reluctance and fear of sharing resources across departments and organisation (Clark 2003; OECD Observer 2003; Shetty, 2003 Rohleder and Jupp 2004; Swartz 2004; Norris and Moon 2005). While the main drivers were strategies to improve customer satisfaction with on-line government services; customer demands for new or better services. In a report by Accenture, over 92% of government executives that responded rated superior services as a business imperative for e-government initiatives (Anonymous, 2003). In one instance in the US, the driver for introducing e-government was to "revolutionise" the way government departments operate internally and with citizens (O'Hara, 2000).

The criteria for adoption are relatively clear and consistent from the above findings of existing empirical studies. We can see that security, privacy and trust are consistent criteria to the adoption and full implementation of e-government for both government and citizens and is thus a major factor for encouraging inclusion. This being the case, we need to clarify what trust is in this context in order to address perceptions of security and trust.

5 TRUST IN THE CONTEXT OF THIS PROJECT

The concept of trust is extremely complex, attracting much attention from a number of different perspectives including the technological approach, social, institutional, philosophical, behavioural psychological; organisational, economic, game theoretic approach, e-commerce and managerial (Lewicki and Bunker 1996, Riedl 2004; Kim et al 2005) . Trust itself is very difficult to observe and measure directly, and in more recent times, has developed from being a static phenomenon (Rousseau et al. 1998) to a more dynamic concept with different developmental stages or phases each with specific characteristics (Lewicki and Bunker 1996, McKnight et al. 1998, Chen and Dhillon 2003).

This dynamic view of trust has led to the development of different trust models that identify different relationships and actors in the process of building trust. One such model developed by Shapiro et al. (1992) and later modified (Lewicki and Bunker 1996; Ratnasingham 1998) proposed a hierarchical development of trust which takes place in three stages: deterrence and reward where a calculation of risks and benefits is made; development of a trust-relationship where the behaviour of the trustee can be predicted by the trustor based on her knowledge and experience of past interactions; identification based trust where a mutual understanding of the other parties' motives and preferences and a mutual empathy and identification often manifested in creating a collective identity or physical closeness has been developed. Not all relationships reach the three stages, and there is a potential decline or dissolution of trust that is possible at any time (Shapiro et al. 1992).

Kim et al (2005) draw on a number of trust models and theories to develop their own multidimensional trust formation model which captures and portrays the complex phenomena of trust formation in e-commerce transactions. They focus in particular on the process involved in trust formation and build on Johns (1996) and Moorman (1993) to posit that a process trust model is based on trustors assimilating information, including

perception of the trustee's situation; then processing the information to form a belief regarding trustworthiness of the trustee. If the trustee is found to be trustworthy, then a relationship is entered into. Finally the consequences of entering into a trusting relationship are developed and fed back into the assimilation stage. There are several other models for trust in e-commerce which describe the interplay of trust building factors. A summary of the major trust building factors for e-commerce from the models is presented in table 2.

Models for Trust	Trust building factors for e-commerce
McKnight et al. 2002	Trust building levers: perceived site quality and reputation Trust in vendor: trusting beliefs, trusting intentions Institutional and structural factors: structural assurance, perceived web risk Behavioural intention of the customer:
Egger 2000	Pre-interactional filters: general intention to trust, general attitude towards e-commerce, reputation, impact of peer opinions Interface properties: appeal, usability Information content: privacy, security, communication
Kim et al. 2005	Consumer behavioural aspects: demographics, culture, privacy experience Institutional attributes: reputation, accreditation Information of web content: accuracy, currency usefulness Product/service attributes: reliability, availability, quality Transaction delivery and fulfilment Technology: hardware, software, that delivers security and effectiveness
Riedl 2004	Technical security Protection of privacy Trustworthiness of supplier: trusting beliefs, trust property Reputation of supplier Certification by trusted third party Quality Skills of consumers
Milloy et al. (2002)	Trust in transit : related to the infrastructure Trust in usage and access: related to the organisation and its handling of the information

Table 2. Major Factors for Building Trust in E-commerce from Trust Models

From this we can see that there are several overlapping and consistent factors that impact the building of trust. For the purpose of this project, we can categorise these into two major categories, that then feedback into the trust building relationship. The factors which form a part of these categories are defined as:

i) **Pre-interactional factors**:
   a. ***Individual Citizen/Consumer Behavioural attributes***: which include subjective norms, individual demographics, culture, past experiences, attitudes to e-commerce (or e-government); general intentions to trust and use e-services; influence of peer opinions
   b. ***Institutional attributes***: which include organisational reputation, accreditation, and general perceived trustworthiness of the organisation
   c. ***Technology***: which includes hardware and software, that delivers security and effectiveness such as interface design, public key encryption, integrity and the like

ii) Interactional Factors:
   a. ***Product/service attributes***: which includes reliability, availability, quality and usability
   b. ***Transactional delivery and fulfilment of services:*** which includes usability, accuracy and quality
   c. Information content attributes: which includes accuracy, currency, quality

Trust building is a cumulative process where the level of trust in the earlier stages affect level of trust in the later stages and impact on the development of a trust relationship that can potential move into the highest echelon of information based trust.

While the phenomenon of trust is difficult to observe in a commercial context, it is even more so in the context of government as there are more layers of complexity in the trust formation dynamics for e-government. Thomas (1998) classifies trust in government as emanating from three main factors: a) characteristic based – produced through expectations associated with the demographic characteristics of a citizen b) institutions, who must create trust either directly through adoption of professional standards or codes of ethics or indirectly through the administration of laws and regulations c) process-based trust which results from expectations of reciprocity in which the giver obligates the receiver to return goods or services of equivalent intrinsic or economic value. From this classification we can see there is a link with the classification of trust developed above, where the characteristic based trust in e-government links to the consumer behavioural attributes; the institutional links to the institutional aspect and the process based trust links to the technology and the interactional factors.

While the factors identified above for trust in e-commerce can be transferred to e-government, from a review of the normative literature on trust in government, the predictors of trust focus on socio-cultural, economic and political aspects. Building of trust in e-government also incorporates building political capital with citizens; performance of the economy where citizens evaluation of the economy rise and fall accordingly; citizen perception of government efficiency or wastefulness; "mis" allocation of tax "dollars" and/or spending tax on the "wrong things"; policy alienation and government ineffectiveness and (Riedl 2004; Parent et al. 2005). These factors that are among those that have been empirically proven, impact largely on the pre-interactional perceptions of citizens, but also to a lesser extent on the interaction factors such as usability and communication facilities.

6 TRUST AND SECURITY

In a number of studies, there has been a link between trust and perceived security rather than security itself (Riedl 2004; Akhtar et al. 2005,2006). In an EU study, Benchmarking Security and Trust in the EU and US, individual concerns about lack of trust and confidence in services provided electronically was found to be a significant barrier to the development of e-government and e-commerce. The eEurope 2005 Action Plan stresses the importance of on-line security and trust for IS developments: "*without good performance indicators (for security) … firms, security suppliers and consumers will be unable to make informed decisions about current or desired level of security and privacy*".

While they acknowledge that defining trust in a measurable way is not possible, they suggest that trust should involve 3 components: a) symbols informing users of an ensured level of security; b) brand fulfilment (promise to deliver specific attributes) and c) navigation, presentation and technology where technology solutions are used to imply quality and professionalism. In their survey, it was found that awareness of security features of websites were important factors for deciding to transact online for 74% of EU citizens. However, in a comparison of US and EU users, more than 40% of regular US Internet users were aware of security features of websites, such as the deployment of anti-virus protection, while in the European Union, this figure was lower than 20%. The impact of this lack of awareness is even more important as the survey also reported that over 60% of respondents were unlikely to interact with e-government initiatives because of security fears and lack of reliable information and data about the service and the security of their transactions.

7 SECURITY AND E-GOVERNMENT

Having identified the importance of raising awareness and providing knowledge about security measures to citizens, as a major factor in developing trust, this project will focus on how information about the security of technology infrastructure being used by the citizen can be collated accurately and presented in a way to citizens that enables them to make an informed decision and choice about taking part in e-government transactions. Figure 1 illustrates the different entities that are involved in e-government security.

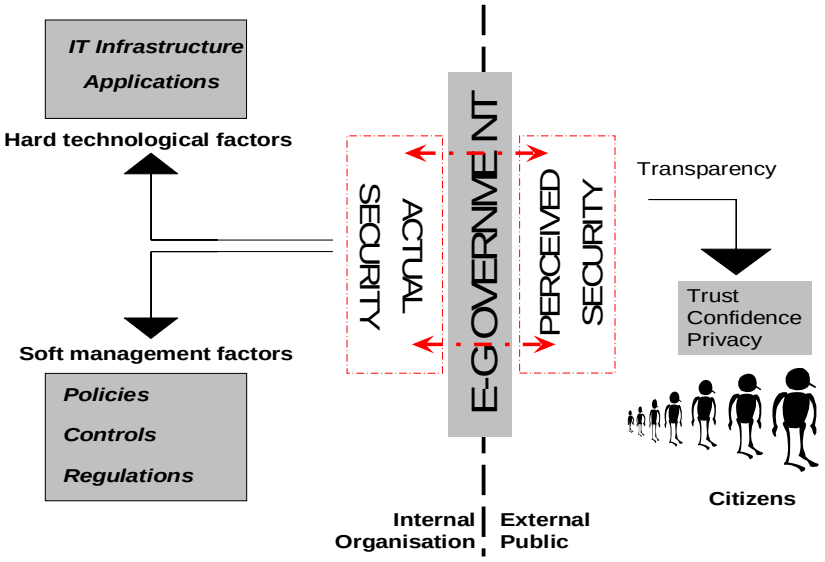

Figure 1. Entities of E-government Security

On the internal organisational government side, security is actual and real and needs to be implemented on two major levels. Firstly, hard technological factors incorporate the hardware and software needed to protect systems and information. Secondly, the soft management factors that incorporate management and organisational policies, controls, regulations, legislature, human resource management and training and the like. A crucial part of managing information security is having a framework and set of standards to which all the necessary areas of information security in the organisation adhere. There are a number of different international standards and best practice guidelines, which are summarised in table 3. Many of these underline the same areas of importance to be addressed and the majority use the British Standard BS7799 now ISO 17799 as their foundation. A security audit will be developed based on a review of the Security Guidelines and standards summarise below, and the organisation's own guidelines and standards

On the external and public side, as already discussed, the perception of the security implemented within e-government needs to be disseminated to its citizenry (organisations as well as individuals). There needs to be transparency in the e-government process that engenders trust and confidence in the services being provided, as well as assurances of the citizen's privacy (Marchionini et al. 2003; Grant 2004; Lauer 2004; Vriens and Achterbergh 2004).

Security Standard or Guideline	Description
ISO/IEC 17799; BS 7799-1 Code of Practice for Information Security Management BS7799-2:2002 Specification for Information Security Management	The British Standards Institute published a code of practice for managing information security following consultation with leading companies. Part 1 incorporates a broad range of security practices and procedures that can be adopted by any organisation of any size and in any industry sector. It is organised in 10 sections which include security policies; management framework to identify security roles, processes and access controls; asset classification and control; procedures for personnel security and responsibility; physical security access and responsibility; security communications and operations management; business continuity planning testing and ensuring that systems can still function in the event of an interruption; compliance checks with legal regulations, contractual obligations or upgrades. BS 7799 is now being adopted internationally as ISO/IEC 17799 Once the BS7799 management system is fully implemented the next stage is BS7799-2:2002. Part 2 is an Information Security Management System (ISMS) that adopts a systematic approach to managing sensitive company information, which encompasses people, processes and IT systems. This is under revision and is expected to be complete in the late 2004 early 2005 timeframe.
Control Objectives for Information and related Technology (COBIT)	Designed to be an information technology governance (IT Governance) aid to management in their understanding and managing of the risks and benefits associated with information and related technology. It is intended that CobiT provide clear policy and good practice for IT Governance throughout the organisation.
"Generally Accepted System Security Principles (GASSP)	Developed by the US National research council. GASSP considers the terms policy, rules, procedures, and practices that relate to organisational implementation of physical, technical and administrative information security that practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of information and systems. It incorporates the consensus at a particular point in time as to accepted information security principles, first within the GASSP Committee, followed by international IT community review. As IT changes rapidly, GASSP are expected to evolve accordingly. http://web.mit.edu/security/www/GASSP/gassp021.html it
ISO 13335 - Guidelines for the Management of IT Security (GMITS)	A five part series of technical reports, which adopts a more holistic philosophy of security management. It provides guidance on the management of IT security, presenting a foundation to assist organisations in developing and enhancing their internal security architecture, and also a means to establish commonality between organisations. At present, the GMITS project consists of 1) *Concepts and Models* for IT Security independent of the organisation 2) *Managing and Planning IT Security*, highlights issues an organisation must tackle before establishing or altering its IT Security program 3) *Techniques for the Management of IT Security*, presents different approaches to IT security risk assessment 4) *Selection of Safeguards* that are relevant to different national legislation 5) *Safeguards for External Connections*, highlight issues for developing a "trust boundary" between organisations. Parts 4 and 5 are in development and have not yet been published. http://www.it-security.sk/iso_13335_an.htm
The Information Security Forum (ISF) Standard	First released in 1996 by PriceWaterhouseCoopers, the information security standards are based on the extensive knowledge and expertise of ISF Members, and other international and national standards (such as ISO 17799) and the results of earlier ISF Information Security Status Surveys. Participants can make a quantitative and comprehensive assessment of how well they conform with the Standard.
Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE)	OCTAVE provided details of accepted best practices for evaluating security programmes.

Table 3. Information Security Standards, Benchmarks and Guidelines

8 DEVELOPING THE TVA

In order to assimilate the information collected from the e-government security audit into a format and language that addresses the needs of citizens and informs them about the security infrastructure, we first need to understand the language used to define the concepts within the two communities. Much has been written on formal security audits or frameworks as show in Table 3 above. However, the more demanding investigative activity will be to understand the lay or citizen views of security. Thus the development process needs to begin with a field investigation – focus groups and surveys – to establish the preferred language and scope of statements about perceived security provisions.

Without having completed these studies it is only possible to conjecture about the structure and content of the two views. At this stage it is assumed that the likely outcome of such investigations will be that:

- Citizens will tend to express their security concerns in terms of the risks or threats to themselves or their data,
- Agency audits will tend to be expressed in terms of the technologies, strategies and procedures deployed to protect the system and the integrity of transactions,
- Citizens will tend to quantify or prioritise their concerns with linguistic variables like "Critical", "High", "Good", "Low", "Must", "Should" etc.
- Where relevant agencies will tend to quantify security provisions with numeric probabilities or percentages.

Given the two disparate views of security provided by the audit structures on the one hand and the citizens concerns on the other, the problem is to map one into the other. This will provide the basis for an automated agent – the trust verification agent (TVA) – that can carryout the mapping for any particular agency.

Since the TVA is intended to serve the citizen's needs the starting point is that particular citizen's expectation of a site where the security "can be trusted". The interaction with the TVA would then go something like this:

1. The Citizen enters their expectations of a trustworthy site. For example "*privacy is high and data storage is very good*"[1].
2. The Citizen identifies a relevant agency. For example "*Five Hills District Council*".
3. The TVA will attempt to infer the extent to which the agency's provisions meet or exceed the expectations and provide an evaluation. For example "*Five Hills District Council meets your privacy expectation but not your data storage expectation*".
4. The Citizen might then drill down into the reasons for the conclusion. For example "*Explain privacy*".
5. The TVA explains the basis for this. For example "*Privacy is high needs (1) server access restriction to be high, (2) data access controls to be high, and (3) workstation access to be high*".
6. etc.

If the citizen drills deep enough they will reach the Five Hills District Council's technical audit statements that support TVA evaluation. For example "*Staff access to the computer room is restricted to designated card holders*".

The technology to achieve such an interaction is well established within the expert systems area. For each risk or threat identified by the user the capability of the agency can be determined by backward chaining through production rules like:

IF *firewall-architecture* IS *demilitarised-zone* THEN *vulnerability-to-hacking* IS *low*

IF *archive-strategy* IS *weekly* AND *archive-location* IS *off-site* THEN *data-protection* IS *very-good*

This model of reasoning dates right back to the early artificial intelligence experiments with systems like MYCIN (Shortliffe, 1976). However, in order to handle the uncertainty of set membership in the presence of linguistic variables like "High" and "Low" the system needs to employ a fuzzy rather than crisp set based evaluation model. Such models, derived from the work of Zadeh (1973), are now standard components like the

[1] It is not intended that the TVA will use natural language as typed here but that terminology and meaning will be equivalent to these statements.

Fuzzy Logic Toolbox (MathWorks, 2006) in MATLAB®. The desired explanatory behaviour (Goguen 1983) is also a well established procedure that simply traverses the production rule tree articulating the structure and values at each of the nodes (Hasling 1984).

The technical challenge in building the TVA is not in devising relevant technology but in developing the rule base and the design of an appropriate user interface.

9 SUMMARY

The aim of this project will not be to develop a new trust building model between government and citizens through the implementation and use of e-government, but will rather present one way in which communication between citizens and government in the e-government environment is transparent enough to ensure that citizens are able to make informed decisions for engagement, based on the degree of security to that is implemented.

To achieve such an artefact depends on the acquisition and structuring of the relevant knowledge base, rather than any need to develop new algorithmic models of reasoning. Established expert systems technology will suffice. The project will make a key contribution to knowledge with its understanding of the relationship between security as perceived by the lay citizen and formal security models and audits used within the IT profession.

Acknowledgement

The collaboration and planning to develop this project proposal was undertaken within the Network for *e*Government Integration and Systems Evaluation (*e*GISE). This is a research network funded by the Engineering and Physical Sciences Research Council in the UK (grant GR/T27020/01)

References

Anonymous. 2003.. “E-gov initiatives making strides”. *Information Management Journal* , 37 (6):14.

Carter L.. Belanger F. 2005.. “The utilization of e-government services: citizen trust, innovation and acceptance factors”. *Information Systems Journal*, 15 (1):5-25.

Chen S.C. and Dhillon G.S. 2003.. Interpreting Dimensions of Consumer Trust in E-Commerce. *Information Technology and Management*, 4: 303-318.

Clark E. 2003. “Managing the transformation to e-government: An Australian Perspective” *Thunderbird International Business Review* , 45(4):377-397.

Davis F.D. 1989. “ Perceived usefulness, perceived ease of use, and user acceptance of information technology”. *MIS Quarterly*, 13 (3):319-339.

Deloitte Research. 2000. ‘At the Dawn of E-government’. *Global Public Study by Deloitte Consulting and Deloitte & Touche.* http://www.egov.vic.gov.au/pdfs/e-government.pdf Accessed July 2005

Earl M. 2000. ‘Evolving the E-business’. Business Strategy Review 11(2):33-8.

eEurope Benchmarking Report 2002. http://www.nwnode.org.uk/documents/b/benchmarkin_en.pdf accessed July 2005.

Egger F.N. Towards a Model of Trust for E-Commerce System Design. http://www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html accessed December 2005

Finger M Pecoud G. 2003. ‘From e-Government to e-Governance? Towards a model of e-Governance’. *Electronic Journal of e-Government* , 1(1):1-10. www.ejeg.com

Gilbert D. Balestrini P. Littleboy D. 2004. “Barriers and benefits in the adoption of e-government”. *The International Journal of Public Sector Management*,17 (4):286-301.

Grant G. Chau D. 2005. ‘Developing a Generic Framework for e-government’. *Journal of Global Information Management*, 13(1): 1-30

Hasling, D. W., Clancey, W. J. and Rennels, G, 1984. "Strategic Explanations for a Diagnostic Consultation System." *International Journal of Man Machine Studies* 20(1): 3-19.

Horst M. Kuttschreuter M. Gutteling J.M. 2006. Perceived usefulness personal experiences risk perception and trust as determinants of adoption of egovernment services in the Netherlands. *Computers in Human Behaviour* in press available online

Hung S. Chang C. Yu T. 2006. Determinants of user acceptance of the e-government services: the case of online tax filing and payment system. *Government Information Quarterly* in press available online

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

Ke W. Wei K.K. 2004. 'Successful e-government in Singapore'. *Communications of the ACM*, 47(6):95-99.

Lauer T.W. 2004. "The Risk of E-voting". *Electronic Journal of E-government*, 2 (3):177-186.

Lewicki R.J. Bunker B.B. 1996. Developing and maintaining trust in work relationships, Trust in *Organisations: Frontiers of Theory and Research*. Sage Publications, Thousand Oaks, CA pp 114-139.

Marchionini G. Samet H. Brandt L. 2003.. "Digital Government". *Communications of the ACM*, 46 (1):25-27.

MathWorks, 2006. "Building a Fuzzy Inference System", MathWorks Inc. Product Documentation, http://www.mathworks.com/products/fuzzylogic/description3.html accessed 21 June 2006

McKnight D.H. Choudhury V. Kacmar C. 2002. "The Impact of Initial Consumer Trust on Intentions to Transact with Web Sites: A Trust Building Mode"l. *Journal of Strategic Information Systems*, 11: 297 – 323.

Mercuri R.T. 2005. "Trusting in Transparency". *Communications of the ACM*, 48, (5):15-19

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

MoormanC. Deshpande R. Zaltman G. 1993. "Factors affecting trust in market research relationships". *Journal of Marketing*, 57(1): 81-101.

Moynihan D.P. 2004. "Building Secure Elections: E-voting, Security, and Systems Theory". *Public Administration Review*, 64 (5):515-528.

Norris D.F. Moon M.J. 2005. "Advancing e-government at the grassroots: Tortoise or Hare?". *Public Administration Review* , 65(1):64-75.

OECD 2003. "The e in e-government". Organisations for Economic Co-operation and Development. *The OECD Observer*, Sep 2003 .239 pp.45.

O'Hara C. 2000. "Commerce embraces e-gov". *Federal Computer Week*, 14, (4):41.

Parent M. Vandebeek C.A. Gemino A.C. 2005. "Building citizen trust through e-government". *Government information Quarterly* 22: 720-736

Rand Europe 2003. *Benchmarking Security and Trust in the Information Society in Europe and the US*. Information Society Technologies. http://www.enisa.eu.int/doc/pdf/studies/esecurity_in_eu.pdf accessed May 2006.

Ratnasingham P. 1998. "Trust in web-based electronic commerce security". *Information Management and Computer Security*, 6 (4):162-166.

Riedl R. 2004. "Rethinking trust and confidence in European e-government" *IEEE Proceedings* http://www.ifi.unizh.ch/egov/Trust_v1.0.pdf accessed May 2006.

Rohleder S.J. Jupp V. 2004. "eGovernment Leadership:High Performance, Maximum Value". *Accenture Report The Government Executive Series.* http://www.accenture.com/xdoc/en/industries/government/gove_egov_value.pdf accessed July 2005.

Shackleton P. Fisher J Dawson L 2004. 'Internal and external factors impacting on e-government maturity: a local government case study'. *Journal of Information Technology Cases and Applications*, 6(4):36-50

Shapiro S.P. Shepherd B.H. Cheraskin L. 1992. Business on a handshake. *The Negotiation Journal*, 1(4): 365-378

Shetty A.V. 2003."Why most e-government projects fail". *Businessline International Edition,* November 15, 2003. http://www.blonnet.com/2003/11/15/stories/2003111500050800.htm accessed July 2005.

Shortliffe, E. H. 1976. Computer-Based Medical Consultations: MYCIN, Elsever, AI Series 2.

Skok W. Ryder G. 2004. "An evaluation of conventional wisdom of the factors underlying the digital divide: a case study of the Isle of Man". *Strategic Change*, 13(8):.423-428.

StamoulisD. Gouscos D. Georgiadis P. Martakos D. 2001. "Revisiting Public information management for effective e-government services". *Information Management and Computer Security* , 9(4):146-153.

Swartz N. 2004.. "E-government Around the World". *Information Management Journal*,38(1):12.

Tan C.W. Pan S.L. 2003. 'Managing e-transformation in the public sector; an e-government study of the Inland Revenue Authority of Singapore'. *European Journal of Information Systems,* 12(4):269-281.

TassabehjiR. 2003. *Applying E-commerce to Business*. Sage Publications, New York.

Tassabehji R. 2005. "Principles for Managing Information Security". *Encyclopedia of Multimedia Technology and Networking,* Pagani, M. Ed.pp.842-848. Idea Group Reference.

Thomas C.W. 1998. "Maintaining and restoring public trust in government agencies and their employees". *Administration and Society,* 30(2):166-193

Vriens D. Achterbergh J. 2004. "Planning Local E-government". *Information Systems Management,* 21(1):45-57

Watson R.T. Mundy B. 2001. "A strategic perspective of electronic democracy". C*ommunications of the ACM,*.44(1): 27-30.

West D.M. 2004. "E-government and the transformation of service delivery and citizen attitudes". *Public Administration Review,* 64(1):15-27.

Zadeh, L. 1973. "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes." *I.E.E.E. Transactions on Systems, Man and Cybernetics* SMC-3(1): 28-44