American Journal of Applied Sciences 3 (11): 2122-2130, 2006
ISSN 1546-9239

Building an e-Government e-Trust Infrastructure

Hussein Al-Omari and Ahmed Al-Omari
Computer Science Department, Applied Science University, Amman, Jordan

Abstract: This paper presents a Trust Model for e-Government implementation. In the first part of the paper, the trust definition from different points of view (psychology, philosophy, linguistic, sociology, and mathematics) was presented. Most people think that to build trust between the government and its customers or citizens, one must start by implementing IT Security and some kinds of Customer Relationship Management (CRM) systems and that will lead to a full customer trust. However, this was not always true; most citizens or customers do not have positive attitudes toward their governments for political reasons, social reasons, and other reasons. The second part of the paper shows the main elements of trust with some examples. The last part discusses the proposed e-Government trust model and shows that trust was a multidimensional issue. Each part was fully integrated with the others in a certain relationship that formulates trust. The main building blocks of trust are: IT security, process automation, policies and procedures, social and culture practices, and legislation. This model represents a suitable guideline for any government who wishes to build or rebuild trust with its customers. It is necessary to use modern technologies to complete the trust architecture.

Key words: e-Government, trust model, e-trust, e-model, Jordan

INTRODUCTION

According to the main classifications of e-Government sectors, four main categories have been identified: Government to citizens (G2C), government to business (G2B), government to government (G2G), and government to employees (G2E) [1]. These categories are the main customers of e-Government, and we will use the term customers to indicate any or all of these categories.

Trust is the foundation of relationship between customers and organizations. Trust decreases feelings of insecurity, binds people together, and enables confidence [2]. Trust grows over time as organizations show accountability and responsibility, which leads to more customers, cost reduction, and time saving for both parties in the relationship. The level of trust will continue to grow with each successful positive online interaction. It can even become a competitive advantage. However, trust is not earned over night. The establishment of trust between a customer and an organization needs to evolve over time [3]. In principle, without confidence and trust in the notion of Secure Government and a framework of trust, very little can be offered over what is expected in the development of e-Government services.

The availability of multiple delivery channels, conventional Internet access, digital television, mobile access, smartcards, biometrics and other new technologies, present their own challenges involving support for trusted services, authentication and confidentiality. With multiple agencies frequently involved in the development of e-Government projects, the information security infrastructure is invariably the element most open to compromise and the one that frequently presents the greatest risk to e-Government projects.

To adopt e-Government processes, citizens must have the intention to "engage in e-Government", which encompasses the intentions to receive information, to provide information, and to request e-Government services. Will citizens exchange information electronically given the choice between an online process and a traditional method? [4] Without customers' confidence and trust in the government portals, processes, procedures, and other aspects of government, the vision of fully electronic service delivery will remain a challenging target. Most customers eventually have no choice than to "talk" to government. So, there is a strong incentive to ensure that the trust model is robust, reliable, and enjoys a high confidence level.

Trust between online electronic transaction parties is a key to the success of a business relation [5, 6]. Trust building is a complicated issue in e-Business or e-Government relations, where the parties on the two ends of the exchange conduct online electronic transactions without having any previous experience with each other or without having detailed information about one another [7].

Corresponding Author: Dr. Hussein Al-Omari, Computer Science Department, Applied Science University, Amman, Jordan

Trust overview

Trust definition: We use trust frequently in our daily life activities. We get up in the morning and go to our work trusting that we still have our jobs [3], we go to eat from restaurants trusting that we eat healthy food, we pay our invoices trusting that our balance will be stalled down, we interact with our governments trusting that we are dealing with accountable agencies, and too many other activities with similar trust. We are performing those activities under a trusting certainty factor.

Trust does not have one specific definition; most definitions come from linguistics, psychology, philosophy, sociology, and mathematical representations.

From linguistic point of view, the Webster's New Collegiate Dictionary [29] defines trust as:

- Noun: 'assured reliance on the character, ability, strength, or truth of someone or something'.
- Verb: have trust in - 'to place confidence: DEPEND', 'to be confident: HOPE', 'to commit or place in one's care or keeping: ENTRUST', 'to permit to stay or go or do something without fear of misgiving', 'to rely on the truthfulness or accuracy of: BELEIVE', 'place confidence in: rely on'.
- Morton Deutsch defines trust from psychology point of view as confidence that one will find what is desired from another rather than what is feared [8].
- Niklas Luhmann's defines trust from sociology point of view; he talked about the relationship between humans and the society. "Luhmann argues that the concept of trust is a means of reducing complexity in society; every time we face a complex or even simple decision-making situation, we have to make some assumptions taking into account the particular situation and the particular environment and then make some trusting choice. The importance of trust goes beyond the boundary of complexity in society and it plays a significant role in our interactions with society" [8].

Gambetta Diego presents a unique definition of trust, based on mathematics as follows:

Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently or his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly, when we say that someone is untrustworthy, we imply that the probability is low enough for us to refrain from doing so [9].

The importance of Gambetta's definition has several directions; Firstly, trust is modeled mathematically and hence becomes more concrete than abstract compared to other definitions. Secondly, this definition makes trust somehow quantifiable; it has a range from 0 to 1, where 0 represents complete distrust and 1 represents complete trust. Blind trust is an example of complete trust where one agent has complete trust in another no matter what. Finally, it emphasizes that, our actions are dependent on the probability and this excludes those instances where trust in someone has no influence on our decisions. This definition recognizes the fact that trust is relevant only when there is a possibility of distrust, betrayal, exit, or defection. This can be expanded by saying that when someone is trusted (but not completely; otherwise, his probability would be 1), there is a chance that the action he performs may be non-beneficial to us [9].

The need for trust: In the past, organizations, customers, and others choose to implement business process transactions based on different forms of trust such as personal relationships, using ID cards, using trust certificates, or using any other valid form of identification.

In the modern economy and the wide spread of using the Internet in most daily life activities, old means of trust techniques are not convenient; hence, a new trust model based on new technologies which is able to preserve trust among communicating parties is highly demanded. Nowadays, trust plays an important role and became the backbone of modern business transactions. One can assume that we do not need to interact with other people face to face that much. This is only partially true. The true part is that we do not need to interact with other people face to face that much, but the importance of trust still exists; if not between people then definitely between the electronic devices we use to interact with each other [3].

The most important concern in the Internet world (i.e. e-Business and e-Government) is how to trust that we are buying from the right shop, we are paying the right person, we are dealing with the right entity, the items will arrive after we have paid for them, our privacy is preserved, our personal files and records are kept securely, our business process transactions are treated professionally, and that there is nobody monitoring our credit card details or our login credentials. These are the issues the networking environment has to resolve before we put our faith in the Internet transactions system.

The widespread of electronic linking of individuals and organizations has created a new economic environment in which time and space are much less limiting factors, information is more important and accessible, traditional intermediaries are being replaced

and the customer holds increasing amount of power. Internet brings new challenges and opportunities to organizations. On one hand, the Internet can increase the amount of transactions and operations from local to worldwide, improve internal efficiency and productivity, enhance customer service and increase communication between different parties, reduce cost, provides transparency, accountability, more customer access and participating in actions, and many others. On the other hand, Internet brings many challenges and threats, like transaction security and privacy, rapid changing technology, difficulty of integrating existence systems (legacy systems) with e-Government software, shortage of skilled technical employees, funding, culture concerns, political concerns, and many others [10].

The Internet is a public network that consists of thousands of private computer networks connected together. This means that a private computer network system is exposed to potential threats from anywhere on the public network. Protection against these threats requires organizations to have stringent security measures in place. Additionally, organizations must protect against the unknown. Also it is important to protect the organization's relationships with its customers. Many Internet users perceive that there is a large risk to their privacy and security when they submit their personal information or conduct some business process [10].

In order to achieve the main goals and objectives of launching e-Government initiatives [11], it is critical for governments to gain a competitive advantage, establish formal privacy policies, proactively monitor their actual practices, and build a strong trust model, before a privacy breach occurs. By acting early, organizations can build their credibility and earn customers confidence [2].

By offering services on the Web, governments can gain unique benefits such as:

- New customers: Anyone with an Internet connection is a potential customer to government.
- Cost-effective delivery channel: Many services can be provided to customers via web and email, enhancing customer experience, and increasing profitability by eliminating the transportation and overhead costs associated with services fulfillment.
- Streamlined enrollment: Paper-based enrollment workflows are fraught with delays. Applications for services can be held up in the mail and once received, application information must be entered into computer systems manually, a labor-intensive process that can introduce errors. By accepting applications via a secure Web site, businesses can speedup application processing, reduce processing costs, and improve customer service.
- Widespread of services through better customer knowledge: Services announcement on the Web can result in more customers asking for the service. This can maximize government revenue such as the case with tax payers.

Before entering the competitive e-Government arena, organization must carefully assess and address the accompanying risks and concerns.

Trust concerns: Trust is a central defining aspect of many economic and social interactions [1]. "Building trust is a core requirement for establishing new relationships concerning security, confidentiality, integrity, non-repudiation, trust, etc, especially in an online virtual environment. Equating online trust solely with underlying security requirements is a mistake. These security requirements include authenticating users or Web sites and ensuring the confidentiality and validity of online interactions. Those requirements form an essential foundation, but business trust also encompasses the non-technical issues surrounding online transactions between online partners. Those issues must be satisfied; in other words, sufficient trust must be established, for any relationship to deliver the desired business value" [12].

The main key enablers of trust are customers and organizations. In order to build a trusted relationship and a partnership between both parties, you need to build a concise trust model, which is strong enough to break the ice and gain a mutual trust. Doing so requires the trust model to address and resolve the concerns related to each party. Some of the main concerns raised by each party are listed below:

- Organizations Concerns:
  * Will I get paid according to the services?
  * Can I depend on the customer to honor the transaction?
  * Will the customer deny his service request?
  * Will the customer's behavior enhance my reputation and performs the transactions in a good way?
- Customers Concerns:
  * Will the organization deliver service on time?
  * Will the service quality meets my expectations in terms of time, delivery, money, legality, and security?
  * Will the organization be responsive and accountable to changes I have in requested services or schedules?
  * Will the organization preserve privacy and confidentiality?
  * Will my payments be secured and acceptable?
  * Will the organization address any fulfillment problems that arise and follow up procedures?
- Concerns for Both Parties:
  * Confidentiality and privacy.
  * Is there a non-disputable and auditable record of the transaction?

* Can we develop a long-term relationship?
* Enhanced performance.
* Accountability and responsibility.

The National Electronic Commerce Coordinating Council (NECCC), in an e-Government White Paper of various federal, state and local government agencies, indicates that the future of e-Government includes conducting all varieties of transactions over the Internet. (For more information about NECCC, visit www.e3c.org.) In Advancing Electronic Commerce in the 21st Century report 1, the NECCC named security, authentication, and privacy as the major barriers to making e-Government a reality. Various federal Agencies and state and local governments have addressed this topic [13].

Rephrasing the above concerns from IT Security point of view we can summarize the concerns as follows [1]:

- Confidentiality: to assure no one is prying on my data.
- Privacy: to assure my data is going to be treated only for the purpose it was asked for and no one else is going to use it other than the recipient. Clearly, the issues of privacy and security in e-Government are vital to maintain the public trust. The issue of what is done with private information is becoming more of a concern as e-Government becomes more of a reality.
- Authentication: to verify the identities of both communicating parties.

Authenticating documents is an issue in government applications. How can documents like purchase orders that must be signed before they are legally transferred over the Internet? State and local governments need to address this issue individually. In some governments digital signature has been approved as a mean of identification for electronic transactions. For example, US in early 1999, an executive order was signed authorizing the use of digital signatures in the federal government. The government of Jordan has approved the Electronic Transaction Law (ETL); a temporary law No. 85 for the year 2001. Digital signatures are a safe and secure way to authenticate individuals and to authorize documents for all business transactions.

Conducting secure business transactions, whether through integrated applications on an intranet or with partners, associates, or citizens over the Internet, requires the establishment of trust and identity between parties. This type of trust and identity is now available in many industry applications like the mySAP.com family [14]. Those industry solutions provide government's customers strong security for e-Government transactions based on digital certificate encryption, and provide user authentication and single sign-on convenience. They also provide smooth migration from password-based authentication on an intranet to certificate-based authentication on the Internet. In addition, the solution can be extended for use with partner solutions, such as smartcard and biometrics solutions [13].

Trust elements: The degree of trust, processes, procedures, and actions that are required to build a partnership and relationship between a government and its customers vary according to the relationship strategic significance or risk. Cultural fit and process alignment between partners are critical trust elements in strategic partnerships and require significant staff involvement to evaluate properly. However, trust can be established in less strategic relationships with less human effort [12].

Zucker [4] suggests that; there are three basic modes by which trust takes place in an economic environment. These include institution-based trust, characteristic-based trust, and process-based trust.

In fact, many others factors are involved in building trust. In the following sections, the most important trust elements that play significant roles in building trust in the Internet arena, mainly in e-Government, will be presented:

Information technology security: In e-Commerce or e-Government, much security seems to focus on trusting the other part in the exchange. From a security perspective, trust is the result of applying a combination of IT controls [15]; those controls are:

- The organization knows that the customer is who he says he is.
- The customer has the authority to send the message.
- The message did not change between the receiver and the sender.
- The message came only from the sender.

The goals and objectives of the IT controls are to assure user authentication and data confidentiality [3]. The different components of those controls are focused on:

- Availability: Assures that the system works properly and the services are available to authorized users for intended use only. This objective defends against intentional or accidental attempts to either perform unauthorized deletion of data or cause denial of service, as well as against any attempts to use a system or data for unauthorized purpose.
- Integrity of Data and System: Means that the data is free from unauthorized manipulation, either in storage, during processing, or during transmission. System integrity means that the system has not been manipulated or accessed in an unauthorized manner.
- Confidentiality of Data and System: Means only the intended user receives the information and that information is not disclosed to any unauthorized individual. The confidentiality principle applies to data in storage, processing and in transmission.

- Accountability: Is a requirement that actions of an entity must be traced uniquely to that entity; it becomes significant for issues like non-repudiation, fault isolation, intrusion detection and prevention, after-action recovery, and legal action.
- Assurance: Is required to show that the security measures have been properly implemented and they work as intended.

Implementing the Public Key Infrastructure PKI would be the best choice to address those controls. PKI is a set of software tools, network services, and management techniques that provide trust.

Any organization, no matter how large, will have a difficult time trying to foster trust among suspicious customers. According to the Gartner Group survey, "During the past few years, many Financial Service Providers (especially credit card companies) and technology vendors, have launched campaigns to convert the distrustful to online shoppers by installing new applications (e.g., disposable credit cards) that they believed would encourage non-shoppers to change their ways. However, the survey found that even more security on the Internet would not convince non-shoppers to shop. It should be no surprise that past efforts by credit card companies to offer security features in the hope of converting non-shoppers have failed" [16].

Information security, no matter how strong it is, seems to be no more than an enabler of the e-Government business model; also the open nature of the Internet provides an ever-growing list of security vulnerabilities that every organization needs to address. Information security seems to be one of the most important trust elements, but it is not the only factor; some other factors play a significant role in building the trust.

Process automation: Using new technologies represent new possibilities and challenges at the same time for businesses. Some organizations block the use of new technologies because the risks are too high. But the risk of not using new technologies could mean an organization is outdated [17] and no customers are willing to deal with it. The impact of using new technologies might positively affect the organization from trust point of view; customers would feel they are cared of by the organizations; this results in good reputation and more trust.

It is not enough to automate organization business processes and use high technologies [18]; any business should create a revolutionary business environment (i.e. a comprehensive Business Process Re-Engineering "BPR") [Tomas H. Davenport et al, 1990]. The bottleneck here is the process flow itself, where it is recommended to streamline the business process by reinventing the business process again, in order to facilitate the process application. To achieve process improvement [18], the current process efficiency has to be reevaluated based on some common criteria from different perspectives, i.e. customers oriented and organization oriented.

As with many technology-driven systems, the adoption of online services should be predicted by the Technology Acceptance Model (TAM). A Web interface that is perceived to facilitate the interaction process while being easy to operate is likely to increase citizen's intentions to use it [4]. Organizations that focus on using new technologies without enhancing internal business processes will face hard times, and technology will be an extra overhead. On the other hand, using technology in the right time and place will result in more customer trust and loyalty.

Policies and procedures: Policies and Procedures followed by e-Government are very important to strengthen trust between exchange parties. They include internal policies and procedures concerning business process implementation, accountability, responsibility, transparency, preserving privacy, compliance investigations and expose punishments and precautions taken to keep personal information safe and secure [1].

Privacy policy is one of the most important factors, to bridge the privacy gap; organizations are required to start early to formally address the need of managing privacy. The organization should have transparent statements and procedures shown to all customers in a way that reflects organization accountability and responsibility [2]. This includes but not limited to:

- Privacy Policy: Design privacy policies to meet customer and business need requirements.
- Compliance Programs: Develop internal frameworks and programs to monitor and investigate ongoing compliance.
- Operational Procedures: Develop or reviewing operational procedures to ensure detailed procedural support for organization compliance and business process.
- Readiness Reviews: Build a team work to review regulatory or legislative requirements and perform self-assessments, consulting services, and gap analyses.
- Privacy Audit: Implement a comprehensive privacy assurance services.
- Training and Awareness: Conduct training and awareness programs to employees with privacy-sensitive activities and implement industry codes of practice and legislation.

As trust is the foundation of a sustainable relationship between a government and its customers, violating this trust makes it difficult and costly to reestablish. Therefore, it is critical for organizations to establish formal privacy policies and proactively monitor actual practices to help avoid privacy breaches. Only by building and maintaining the trust of their customers can organizations truly maximize the opportunities afforded by the e-initiatives.

Social and cultural practices: System trust is based on the effectiveness of social structures in reducing uncertainty and providing foundations for secure feelings about the future [19-21]. For example, Zucker (1986) points out that much of the personal-based trust of the 1700s and early 1800s in the United States was displaced in the late 1800s because the populace became much more heterogeneous through immigration. Hence, it became necessary for system trust to fill in for the absence of personal trust. System trust means the trust in institutions, like banks, courts, regulations, professional associations, and governmental departments.

People beliefs, internal government, social and cultural practices, and accompanying security may provide a foundation basis of trust. People usually try to simplify complex and uncertain issues by organizing these issues into categories so they can use an "equivalent response to all instances of a category" [22]. In a new relationship, a person may initiate three types of trust-related categorization mechanisms. Each of these mechanisms supports trusting beliefs:

- Unit grouping: Means that one person, because of the new relationship, now perceives the other person in a new grouping that places the pair into a natural cohesive partnership. Unit grouping is likely to produce feelings of security that the beliefs of one party about the trustworthiness of the second party are valid [22].
- Reputation categorization: This is based on one party's reputation, as known by the other party [22].
- Stereotyping: This is related to more general biases (stereotypes) about the other person. Stereotyping may be done at the broadest level, such as gender, or at more specific levels, such as prejudices against specific small groups. These prejudices may cause immediate distrust between majority and minority groups. Johnson & Johnson point out that such impression "takes place even before direct contact begins" [23].

Culture has two folds: organizational and customers' culture. A resilient organization culture is built on principles of organizational empowerment, purpose, trust, accountability, and strong sense of trust between employees, management, and customers. Customers assume responsibility without question; they commit to action and do what has to be done, regardless of rank, title, or job description [24].

Fairness conducting of transactions will improve practices of customers with government regardless of gender, kin, origin, and nationality.

Previous experience of customers with government is a very important factor in composing the trust image, where trust is usually based on prior experience. Governments can create trust this way by convincing their customers that the same rigorous controls, which make government handling of traditional transactions trustworthy, also apply to online transactions.

Trust is beyond the short-term control of any government; it will take time to convince customers to believe that better results will occur if one trusts others. Government cannot readily manipulate these beliefs; it can take advantage of opportunities afforded by different cultural segments in the population and gain trust while doing so.

A culture behavior is likely to contribute to the adoption or resistance to online services. Hofstede (1997) identifies five cultural factors that affect how people interact. He mentioned the power distance, which is a measure of how much people at the lower level (lower power distance) of society differ from those at the top (greater power distance). Citizens in societies with greater power distance are more likely to adopt available e-Government services. The other culture factor Hofstede mentioned is uncertainty avoidance. The greater the cultural tendency to avoid uncertainty, hence risk, the greater the impact of trust on e-Government adoption. Higher uncertainty avoidance will reinforce the positive effect of citizen trust on intentions to engage in e-Government [4].

Organizational culture in building trust requires a big shift. It requires rethinking and reinventing what government is for us. Using advanced technology and organizational innovation, redesigning of work processes, reducing bureaucracy, and increasing collaboration between differing experiences, to improve government services are essential things in establishing e-Government. It also requires a shift in culture so that through the use of the latest technology, employees put customers first [25].

Building this new social and culture system is more difficult than creating the technological system to run it. To create a new social system, many considerations bear in mind, like political, financial, and legal issues. Building the new social system is not like creating an IT infrastructure; we are creating a process of interactive and collaborative partners. The challenge is to get the leadership and technology experts working together to create this new system. As a result, creating e-Government culture requires doing many things simultaneously. Technologists or leaderships can not create e-Government alone; collaboration and working toward a mutual vision and shared goals are highly required to reinvent the new government culture [25].

Legislations and legal cover: The foundation stone in building e-Government initiative goes beyond organizational, governance and leadership, customer, competency, policies and procedures, and technology issues [1]. It involves the canonical form of the government performance which is the legal part of e-Government, where new procedures and other government activities have to be formally regulated by issuing laws, bylaws, directives, and rules [26].

e-Commerce and e-Government are natural consequence of the Internet evolution. If the Internet should be free from legal implications - as it has often been stated - then the same should apply to e-Commerce and e-Government. The same argument holds for electronic transactions and the traditional common business manual transactions. When the Internet was restricted to military and academic applications, it was indeed free of legal issues, but after the Internet evolution in the late 1980's; some legal questions arose. After more than a decade of Internet practice it is obvious that common regulation sometimes fails in cyberspace. The question arises though is deciding which is faster: the Internet or its legislation.

Although e-Commerce and e-Government are closely related, e-Commerce was first, then came e-Government, and by now we are literally approaching a certain stage of e-Xistance (i.e. e-learning, e-banking, e-voting, e-democracy and so on) [27]. The question arises again: are traditional legal systems prepared to deal with fast spread of electronic developments? The answer is definitely no and the gap between electronic and legal development keeps increasing. Since e-Commerce has longer experience in the market; can we apply e-Commerce legislation and transferring its legal criteria to e-Government: whereas e-Commerce is subject to the parties agreements public administration is strictly bound to legal determination?

A fundamental question raised here regarding conducting electronic transactions from everywhere in the globe is deciding which jurisdiction's law to govern the transaction, including such matters as the proper venue for breach of contract actions, what evidentiary rules to apply, what rules apply to interpreting the language of the contract (in case of G2B for instance) and many other issues [28].

e-Governance mostly focuses on:

- Rewriting laws whose applicability is challenged in cyberspace,
- Formulating new rules to address new business models, new consumer's risks, and new ways of delivering government services,
- Ensuring the infrastructure survivability and competitiveness.
- Developing infrastructure, education, and seed funding for start-ups at the society level and in less-advanced digital societies.

The need for legal cover: e-Governance in the department's context will focus on ensuring that existing strategies and policies are updated to address new kinds of internal and external relationships and to exploit new delivery channels. In particular, the various structures within an e-Governance framework structure must expect to address the following specific challenges which are likely to arise:

- Increasing computer and Internet use in schools and libraries, combating the digital divide, and placing computers in low income neighborhoods.
- Providing a framework for the use of digital signatures and including provisions that authorize email as a legal form of communication.
- Promoting the creation of a national information infrastructure or a national legal framework for conducting online businesses. This implies having tough controls on Internet security to increase IT usages.
- Establishing essential acts to protect the privacy and confidentiality of customers.
- Establishing broad government laws to solve the globalization concerns, where the current government laws and legal enforcement mechanisms are rooted in physical geography. However, the Internet is a global facility.
- Issuing new legislations to manage the Internet and assign accountability and responsibility on official servers.

All governments face the need to devise regulatory and enforcement tools that are vastly different from what has been used in the past. Not just different in degree or geographic reach, but entirely different in character. Law enforcement in cyberspace is going to look very different from law enforcement on the sidewalks of countries and cities [29].

Legal cover and trust relationship: In the cyberspace, the issue of verifying and binding the sender's identity to what has been sent when conducting electronic transactions becomes problematic. One of the main concerns related to both government and its customers is responsibility and accountability among others. The only way to preserve rights and build trust between both communicating parties is to legalize the process by setting the legal framework for electronic transactions and its consequences. Once the canonical form has been identified, the trust can be solely built. The foundation stone in implementing e-Government is trust, and the foundation stone in trust is the legal framework. For this reason, it is important to design a concise trust model capable to handle and support the e-Initiative as a whole, in professional and legal way.

The trust model: For a trust model to be practical and acceptable, it should address the most common concerns in a reliable manner that proofs the truth of the model. As an expected consequence, both parties will appreciate and may work to adopt the model, which helps in building a mutual trust.

Trust is a multi-dimensional discipline; each dimension is integrated to a certain degree with the other dimensions; at the end, the trust model can be carefully formulated from the different trust elements. The basic building blocks of the trust model as shown in Fig. 1 are:

- Information Technology Security (ITS): Although this is very expensive, it is not enough to provide trust without integration of IT Security with the other trust elements.
- Process Automation (PA): This is the last step toward building full e-Government trust. Technology and automation are means to e-Government; they can only speed up the process and find new delivery channels of services. Technology integration with policies and procedures will encourage customers to adopt electronic transactions.
- Trust: the objective we are struggling to achieve.

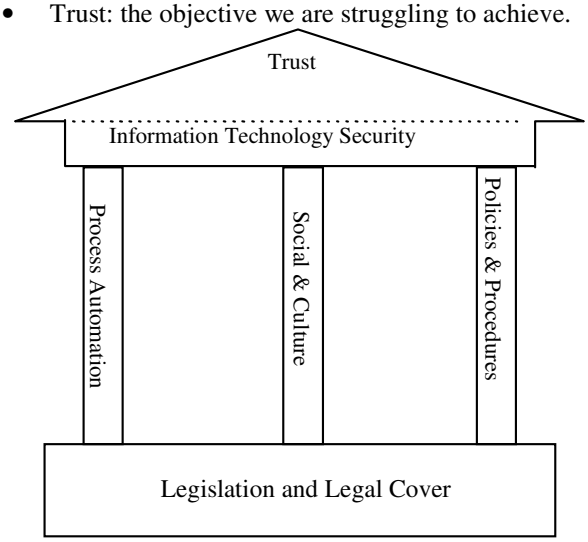

Fig. 1: The Proposed Trust Model

- Policies and Procedures (PP): This represents strong support of legal issues. When transparency exists, clear policies and procedures are posted to everyone, and those procedures are open to inspection by public, and the trust will be open.
- Social and Cultural Practices (SCP): Previous experience with governments has a major role in building trust. Once the government treats all people fairly and lawfully, and shows responsibility and accountability, people suspicion about the government will be dissolved; as time goes by, a solid trust will be formalized slowly but robustly.
- Legislations and Legal Cover (LLC): This represents the basic building block that all trust elements need as a solid foundation stone to start from. It also provides the legal cover for both customers and government authorities.

CONCLUSION

Trust doesn't belong to one specific discipline; lots of definitions from different areas such as psychology, Sociology and Science points of view were viewed in order to understand the different factors of trust. In this changing world, especially because of the Internet evolution and the globalization terms, new forms of relationships start to formulate. The old trust practices become unsuitable in the Internet world. To get around this problem, once needs to reconstruct trust based on the new elements. Those elements were identified in this study as: IT Security, Process Automation, Policies and Procedures, Social and Culture Practices, and Legislations and Legal Cover. They construct the basic building blocks of e-Government trust and should interact in a multi-dimensional relationship to produce trust.

By building this proposed e-Government trust model, each government who wishes to implement an e-Government initiative can use this model as a guideline to build its trust and strengthen relationship with its customers.

REFERENCES

1. Ahmed Al-Omari and Hussein Al-Omari, 2004. A framework model for assessment of e-Government readiness. IMTC 2004 - Information Technology Conference Amman, Jordan.
2. Watchfire, 2002. The Privacy Gap: Managing Website Privacy.
3. Lamsal, P., 2001. Understanding trust and security. Department of Computer Science, University of Helsinki, Finland.
4. Warkentin, M., D. Gefen, P.A. Pavlou and G.M. Rose, 2002. Encouraging citizen adoption of e-Government by building trust. Electronic Markets, 12: 157-162.
5. Mayer, R.C., J.H. Davis and F.D. Schoorman, 1995. An integrative model of organizational trust. Acad. Manag. Rev., 20: 709-734.
6. Special Issue on Trust in Organizations. Acad. Manag. Rev., 20: 3.
7. McKnight, D.H. and N.L. Chervany, 2002. What trust means in e-commerce customer relationships. Intl. J. Elect. Comm., 6: 35-53.
8. Marsh, S., 1994. Formalizing trust as a computational concept. Ph.D. Thesis, University of Stirling.
9. Gambetta, D., 2000. Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford.
10. Albert, H.N., P.J. Judd, O.N. Rivers, S.W. Wagner, 2001. Creating A Winning e-Business. Thomson Learning.
11. The Jordanian Ministry of Information & Communication Technology (MoICT), Launching e-Government in Jordan: A proposed Approach, Final Report, 2000.
12. Reilly, G. and C. Rozwell, 2001. B2B resiliency is built on trust. Gartner Group Research Center.
13. SAP Public Services Inc., 2001. e-Government for the congressional internet cacus advisory committee, e-Government Task Force.

14. SAP AG, mySAPTM Public Sector e-Government, SAP White Paper, 2001.
15. Witty, R., 2001. Information security policies. Gartner Group Research Center.
16. Litan, A., 2001. Online Trust: Earning it big time means big-time earnings. Gartner Group Research Center.
17. Gartner Group Report, 2002. Gartner Group Report to the Jordanian Ministry of Information and Communication Technology (MoICT).
18. Cooper, R. and M.L. Markus, 1995. Human reengineering. Sloan Management Review.
19. Luhmann, N., 1991. Trust and Power. Ann Arbor, MI: University Microfilms International.
20. Lewis, J.D. and A.J. Weigert, 1985. Trust as a social reality. Social Forces, 63: 967-985.
21. Shapiro, S.P., 1987. Policing Trust. In C.D. Shearing & P.C. Stenning (Eds.), Private Policing, pp: 194-220. Newbury Park, CA: Sage.
22. Shetzer, L., 1993. A social information processing model of employee participation. Organization Sci., 4: 252-268.
23. Johnson, D.W. and R.T. Johnson, 1989. Cooperation and Competition: Theory and Research. Edina. MN: Interaction Book Company.
24. Bell, M., 2001. The five principles of organizational resilience. Gartner Group Research Center.
25. Browne, M. and R. Margolies, 2001. Denver: Creating leadership and the culture for e-Government. NATOA J. Municipal Telecommunications Policy, pp: 14-16.
26. Deloitte and Touche Report, 2002. Deloitte and Touche Report to the Jordanian Ministry of Information and Communication Technology (MoICT).
27. Zankl, V.W., 2002. Legal circumstances on the way from e-commerce to e-Government and e-xistance.
28. Renée Dejewski Legal Barriers to e-Government, 2001.
29. State of the Internet 2000, International Technology and Trade Associates - ITTA, 2000.
30. Merriam-Webster®, Webster's New Collegiate Dictionary.