

Building an e-Commerce Infrastructure in Jordan: Challenges and Requirements

[doi:10.3991/ijim.v4i4.1425](https://doi.org/10.3991/ijim.v4i4.1425)

Dr. Muhannad Al-Shboul¹, Dr. Izzat Alsmadi²

¹The University of Jordan, Amman, Jordan

²Yarmouk University, Irbid, Jordan

Abstract—Many countries around the world are trying to build and enhance their internet infrastructure and utilize services related to the Internet such as e-Commerce, information connectivity, accessibility, etc. However, studies indicated that network and hardware requirements are not always the major barrier for progressing in these goals. In some cases, cultural, legal or environmental factor may dominate the type of barriers for the expansion of internet related service in many countries around the world. This paper presents challenges and requirements for the enhancement of e-Commerce services in particular for Jordan.

Index Terms—e-Commerce, Network Security, Digital Certificates, Certification Authority, e-Business, PKI, and Digital Signature.

I. INTRODUCTION

The revolution of the Internet has played significant role in commerce and business in the whole world, which connects millions of people as well as millions of computers. Nevertheless, these types of communication are increasing day after day, and it is used in many sectors, especially in conducting business on the Internet, because internet reduces cost of process, accomplishes and achieves more work without any increasing of costs, and it improves the quality of services, but this does not mean every online business can be success, because on the other hand Internet and the new technology encourage and help hackers and online criminals to attack any kind of business and disrupt it, so this leads to emerge security issue, also hackers might access and steal customer personal and financial information, as a result this will lead to emerge privacy issue. In addition because the Internet gives people the ability to access any Website in everywhere, people can search for better products or services, accordingly this increases the competition among companies.

e-Commerce websites allow financial transactions to be executed over the internet. This completes the full cycle of buying or selling an item (i.e. shopping, selecting, paying, shipping, and receiving). e-Commerce websites can work as virtual stores only or can augment physical retail operations. e-Commerce websites can also be built to sell services or items that does not required shipping such as tickets, calling cards, stock trading, subscriptions, and memberships.

The ability for e-Commerce websites to complete the transaction online is very important. The ability to complete this transaction in a secured manner is more important to raise the customers' level of confidence on online shopping as a competing alternative for regular ones. A secure e-Commerce website can provide businesses with

powerful user's motivated advantages, including increased online retail sales, as well as streamlined application processes for products such as insurance or credit cards.

Digital identification is increasingly evolving in use and importance as a method to safely identify humans or entities especially through online business transactions. Through history, several techniques are used to uniquely identify individuals. Up to date, writing signatures are significant and required to verify that the person filling an application for example, is the same person he or she claims to be. Biometric signatures such as finger prints, iris patterns of the eyes, retina scans, DNA, voice prints, facial features, etc. are important and are able to uniquely identify an individual. However, none of those signatures can be conveniently implementing online to complete a transaction in a short time with a reasonable cost.

Public Key Infrastructure (PKI) is a set of technologies and security policies used to issue, revoke, and manage digital certificates and key pairs [1].

In digital certificates, users are identified by the information embedded on their machines, and verified by mutually trusted third party entities called Certification Authorities (CA) (such as Thawte or Verisign), that guarantee that the website operating is who it claims to be [2].

CA issues and manages digital certificates. They are third party trusted entities to authenticate sellers to buyers, banks to customers, email servers to email users, etc. In general, users are not supposed to expose any personal or financial information in any website that does not have a valid certification.

There are some requirements for any company or entity that wish to become a certificate authority who issues certificates to clients. As a hardware requirement, digital certificates are usually created by certificate servers such as Cisco IOS, Microsoft certificate server, EverLink, etc. CA's should make sure that their certificate database is secured from being accessed or hacked by invaders.

There are several forms of digital certificates. In this first type of certificates, software companies send their keys (public keys) to their customers. Customers will return back a certificate that combines the software company's public key with their private key (which includes specific information taken from their computers to include unique identifiers that distinguish a computer from all other computers). This information may include MAC addresses, IP address, CPU and hard drive unique identifiers, etc. The digital certificate will be encrypted so that its information will not be readable if retrieved by unauthenticated users. It can be understood only by those who is-

sued it. Figure 1 shows a sample of a digital certificate retrieved from a computer.

In a second type, users can also gain self or individual certificates if they wish to uniquely identify themselves through online transactions. There are some companies who can provide such individual certificates for free.

The third type of digital certificates, which is our focus here, is those digital certificates that are gained by websites who want to allow users to enter personal or financial information online. They want their users to trust them and feel secure entering their personal or financial information. Examples of such websites include: banks, hotels, e-businesses (such as Amazon, ebay, etc.), and email servers (such as Yahoo and Gmail).

There are different models for CA's. In the traditional model or infrastructure for the Public Key Infrastructure (PKI), a company or entity will submit their information and request to a certificate authority. The CA will review the submitted information and decided whether to issue a certificate or not. The certificate will be issued for a specific limited time. The same process is repeated whenever the certificate is renewed. This type of certification is not dynamic or real time. This means that the CA does not check the validity of the CA upon requests. The entity will possess the certification for the specified amount.

In another model, the certificate are requested and authorized, or declined upon request. This process is expected to be more secure, but more complex than the earlier one. In different flavors of the models, the transaction content will, or will not be sent with the authorization request. As such, some entities will be authenticated in general, while others will be authenticated to do specific transactions.

Digital certificates are trusted identifications in electronic formats that bind a public encryption key to an identity to achieve public trust in that identity. They are a major factor in giving users confidence in websites and their legitimacy.

Some digital certificates can be transferred from one machine to another. Others generate the individual private key using some of the machine information such as the MAC address, computer name, etc. This means that those certificates can not be used on other machines – without being reinitialized by the CA or the company who issued it.

Typically, two things distinguish a certified website: the letter "s" after http, and the certificate header in the right side of the address bar (Figure 2 and 3). The "s" in "https" means that you are logging onto a Secure Socket Layer (SSL) site.

If you view the certificate from the web browser, it will display three main information: issued to, issued by, and the validity period.

II. CERTIFICATE AUTHORITIES IN MIDDLE EAST

Some companies such as Comtrust [3] offer digital certificates in United Arab Emirates (UAE). They provide PKI technologies and authorize digital certificates for servers, companies, and individuals. Nevertheless, they still require individuals to come in person to verify their identity. In Egypt, digital certificates are issues through some companies such as: ITIDA (Root-CA, Trento Egypt and Gateway, LINKdotNET, etc... Egypt experienced research and proposals e-Government services to allow

citizens to process some papers online. In Saudi Arabia, the Government is in the progress of authorizing certificates, secure emails and several other e-Government and e-Business solutions. Some companies or agencies who are working toward this goal are: SAMA and Entrust partnership. Israel has several CA companies that issue certificates such as: ComSign, IUCC, StarCom, etc.

Jordan started early in studying the possibilities of implementing online security. In 2002, a joint effort by Middle East Communications Corporation (MEC) and WISE-key Switzerland is initiated to allow MEC issuing digital certificates in Jordan [4]. It was expected to be in use by the year 2004.

```

This digital certificate contains CREN's public key. Content-Description: filename="cren.txt"
Content-Disposition: inline; filename="cren.txt"
Content-Type: text/plain; name="cren.txt" Certificate:
Data: Version: 1 (0x0)
Serial Number:
04:60:00:00:02
Signature Algorithm: md2WithRSAEncryption
Issuer: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
Validity
Not Before: Nov 17 00:00:00 2006GMT
Not After: Nov 17 00:00:00 2007 GMT
Subject: C=US, O=CREN/Corp for Research and Educational
Networking, OU=Education and Research Client CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:96:f8:eaa:aa:de:bc:33:74:ce:02:54:ef
82:da:95:87:35:f8:2a:9a:75:1f:de:34:3d:27:0c:
6c:39
Exponent: 65537 (0x10001)
Signature Algorithm: md2WithRSAEncryption
1e:50:cf:82:d0:27:fa:2:86:f1:c6:dd:b2:d1:f2:56:dc:9e:
90:5f:ea:74:4c:97:5a:82:33:84:20:51:70:04:bd:65:ae:97:
8f:f8:c0:fa:91:08:07:e1:e:c2:fd:9:bc:7:cf:3:3a:02:ca:27:
56:ec:67:22
-----BEGIN CERTIFICATE-----
MIIDYDCCAkgCBQRgAAACMAOQCsqGSIb3DQOEBgUAMHQxCzAJBgNVBAYTAiVTMToV
OAYDVQQKEzFDUKVLOlNvcnAgZm9yYjFjc2VhcmNoIGF1ZCBFZHVjYXRpb25hcCBO
ZXR3b3JraW5nMScwJwYDVQQLEyBFZHVjYXRpb24gYXNjaW5kZm91b3VhcmNoIENsaWVv
dCBDOQAeFw05OTExMTcwMDAwMDBaFw0wMzExMTcwMDAwMDBaMHQxCzAJBgNVBAYT
AIVTMTowOAYDVQQKEzFDUKVLOlNvcnAgZm9yYjFjc2VhcmNoIGF1ZCBFZHVjYXRp
b25hcCBOZXR3b3JraW5nMScwJwYXZ0eXN1NkEKAFAZUw3XTUxSiEMYSN867tL/
reWzWCVdQJvtPlx58xU/0ae7h2hqC3DDGVRGhNFxKdpzeZk0JWnw3Qo1txuWNMg5
Usv6phbEpg+YUS9Ekf/qdEyxWolzCBBRCAS9Za6Xj/jA+peIB+HsL9m8fPM6AsonVuxnlg==
-----END CERTIFICATE-----
    
```

Figure 1. A digital certificate example.

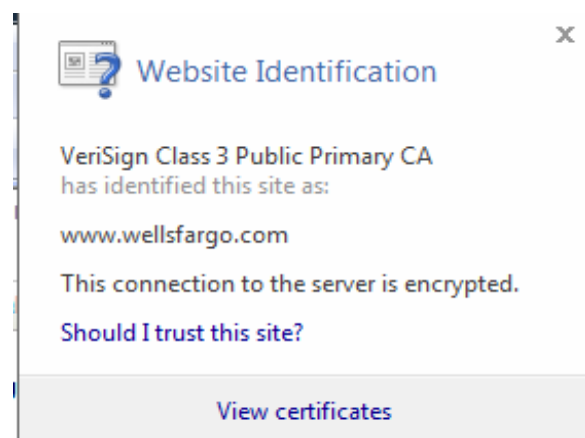


Figure 2. A typical certified website user interface.



Figure 3. A URL address of a certified website.

In 2003, Jordanian ESKADENIA Software Solutions worked in a project to be a local dealer for UAE Comtrust to market e-business services in Jordan [5]. However, neither one of those projects apparently reached a deliverable goal.

In an article published in June 14th 2006 by the Ministry of Information and Communications Technology (MoICT) [5], the document envisions a plan for an e-Government through a plan over the period of 2006-2009. Several laws and regulations were issued to regulate online services. The article concluded by the assessment for critical success factors and risks. Table1 shows the critical success factors and Table2 shows the risk elements.

Tables1 and 2 summarize some of the obstacles and barriers for implementing e-Government including offering online identities, digital certificates, and several other online related services.

Ahmed and Hussein Al-Omari (2006) [7] similarly listed some of obstacles and challenges such as organizations, government, and customers' readiness.

TABLE I.
CRITICAL SUCCESS FACTORS.

Critical Success Factor	Requirement
Availability of resources (HR)	Commitment by Gov of Jordan
Availability of local skills to implement and use e-Government	Develop courses locally School/College/ University to re-skill people
Availability of local skills to implement and use e-Government	Incentives to e-Government stakeholders to strengthen e-Gov related skills
Availability of Laws and regulations that support the implementation of e-Government	Active coordination among concerned agencies to develop and enforce coherent and effective legal framework
Cooperation and harmony among Government entities in decision making for e-Government initiatives	Appoint and activate the National e-Government Steering Committee (eGSC)
Ability and willingness of Government entities to document and share their business requirements, processes, services, data and strategies	Active coordination among Government entities to document and share information necessary for e-Government initiatives
Political commitment to ensure "buy in" by Government entities across government	Appoint and activate the National e-Government Steering Committee (eGSC)
Internet channel penetration	Telecom sector development, regulatory framework to promote competition
Private sector capacity to participate in/support e-Government	ICT sector development
Sustainability of e-Government implementation despite political changes and reshuffle of Government officials	Appoint and activate the National e-Government Steering Committee (eGSC)
	Passage of e-Gov regulations and other actions to secure endorsement at top levels of Government
	Development of "champions" at key ministries / entities; development of administrative will for e-Government initiatives
	Recognition of e-Government as a priority in National Agenda

However, it is fair to say that some of those obstacles are not exclusively related to Jordan or any third world country. This field is quickly evolving in a way that presents a difficulty for public or government entities to keep up with. Governments are not expected to take the major role in such field. The Governments will be responsible in making sure that there is an infrastructure for handling all related activities.

Laws and regulations should be established to control online business and activities. The government should promote using digital certificates and online business through cooperation and acceptance. Internal or external investors should be invited and helped in building an infrastructure for establishing such environment. There is no much difference between this field and the wireless and cell phones communications fields. They both require large investment to build a reliable infrastructure. As a result, investments need to see a commitment from the Government for cooperation. Using digital certificates can be a one important step to facilitate e-Business. Jordan does not lack technical problems in the telecommunication and industry fields. On contrary, Jordan is a pioneer country in the Middle East in those fields. It also provides several other countries in the region with the personnel support and experience.

TABLE II.
E-GOVERNMENT RISKS.

Risk	Mitigation/Contingency
Cost of e-Government is too high for the GOJ	Realistic, well-sequenced phases for e-Government rollout
	Develop pilot projects that can be scaled later based on demand and biz CA's
	Encourage use of innovative commercial arrangements (PPPs) attractive to private sector for investment in e-Government
	Encourage strategic partnerships with specialized international vendors to invest in e-Government
Conflicting decisions among government departments	Use of inter-agency working groups with clear authority to supervise and enforce e-Government policies and standards
Resources within GOJ do not have the skills to implement e-Gov Strategy	<ol style="list-style-type: none"> Support to government entities for IT training and other necessary Skills Recruit staff with relevant skills Incentives for Government entities to invest in developing ICT expertise internally Outsourcing certain functions when business CA's supports it Create links with local universities to give on-the-job-training to students Promote retention of skilled professionals in cooperation with other programs (e.g., Reach)
Resistance to change	Increase awareness among stakeholders, raise accountability, and enhance change management
Speed of change does not satisfy political agenda	Re-align e-Government Strategy with political priorities and changes
Expectations are overly high	Increase awareness of e-Government Strategy among stakeholders and manage expectations

III. JORDAN E-GOVERNMENT: CHALLENGES AND PROGRESSES.

Currently, Jordan offers several e-services to its citizens. They can inquire about several related information such as [8]: Greater Amman Municipality (vehicles ticketing and complaints), driver and vehicle licenses department (vehicle license expiration date), Jordan custom (Inquiry about vehicle custom, guarantee orders, etc), Amman (Water Bills), Income and sales tax department (income balance for individuals), and housing and urban development corporation.

However, user can inquire – and not have to pay for example – for those services. There is not any usage of digital certificates (not even the e-Government websites themselves). According to the income and sales tax department’s website (<http://www.incometax.gov.jo/IncomeTax/Home/Login.aspx>), users can inquire and pay their taxes on line. The website states that it is certified, however, it does not seem to be using digital certificates. The website does not allow users to create their user name and password which indicate that they may need to register in person first.

Doing a survey for Jordanian banks, very few banks, such as the Arab bank, Arab Jordan investment bank, the housing bank, etc. are using digital certificates and securing online transactions – verified by VeriSign CA, a widely known international certificate authority-, others do not have on line access at all, and the third category offers online services without secure transactions which may cause customers’ information to be compromised. As an online user, before entering personal or financial information online, the user should check the certificate, to verify the identity of the website he or she is entering his or her information into. Without such information, user could be giving his or her information to unknown individuals that may reuse it without prior knowledge. However, similar to e-Businesses, banks are the second major category that will benefit from digital certificates.

Figure 4 shows the certificate market share for CA’s in Jordan [9]. The international certificate authority, VeriSign, is taking the majority of the market share in Jordan. Table 3 shows the number of certified websites in selected countries as of 2006 [9]. Jordan has only 26 websites (mainly banks), which is relatively a very small number of websites if it will be compared to the readiness of Jordan (in resources and infrastructure). In most studies to evaluate e-Government worldwide [10, 11, 12, 13, 14, 15], Jordan scores relatively low in terms of citizens’ participation. Jordanian citizens will be encouraged to visit e-Government websites if they can provide them with alternative services to check their taxes and pay them, check their electric, water, and phone bills and pay them, or check the status of any info or service they are requesting from a governmental entity. All those services may not be possible without digital certificates.

As described earlier, there have been several unsuccessful trials by local companies to establish certificate authorities in Jordan. They maybe have problems getting the right authentication and trust from Government and private sectors. As an alternative, Jordanian Government, represented by any entity or ministry such as Ministry of Information and Communications Technology (MOICT) can be a certificate authority that will authenticate certificates for all those who are requesting to have them.

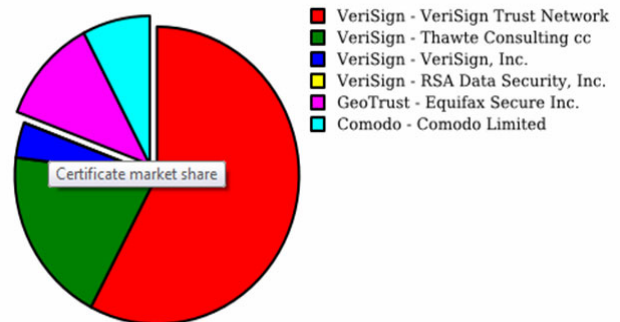


Figure 4. Certificate market share for CA’s in Jordan [9].

TABLE III. NUMBER OF CERTIFIED WEBSITES IN JORDAN AND SOME SELECTED COUNTRIES [9].

Country	No. of servers certified	Country	No. of servers certified
USA	250558	Lebanon	38
UK	31870	Iran	26
Turkey	1528	Jordan	26
Israel	1221	Morocco	24
UAE	222		
KSA	90	Qatar	17
Kuwait	83	Tunisia	16
Egypt	46	Oman	8
Bahrain	44	Algeria	4

IV. GOALS AND APPROACHES

A successful e-Commerce or e-Business infrastructure in Jordan will help several public and private sectors benefit from it. For example, electric power, water and telephone companies may utilize the e-Commerce infrastructure to allow their customers check their accounts online for their current amount of usage and will also allow them to pay online. This may help both service providers and customers. Providers will have less effort and their employees can perform accounts checking and billing and will reduce the overhead of customer services tasks. For customers, it will be more convenient as they can track their account status and pay on their convenient time without the need to go to local, usually busy, agencies. Banks and hotels have also large piece of the steak of interest of having a successful e-Commerce infrastructure. For hotels, customers can shop their websites and book online without the need for mediators or agencies who usually charge for being the middle man. e-Banking is convenient to both banks customers and employees. It will reduce the amount of customer service calls from customers who usually enquire about their account details or transactions that they can check online.

Requirements for a successful e-Commerce infrastructure in Jordan are divided into three categories: legal, software and hardware perspectives. The followings are the typical requirements for each category, along with what is missing and needed.

A. *Legal perspectives: e-Commerce laws and regulations*

In European Union countries, e-Commerce refers to the carrying out of business using electronic means. This generally means over the internet. However, from a legal per-

spective, the term is often used to include remote selling by telephone and email, as well as online. It is also frequently used to refer to legal issues generally relating to the Internet and online trading.

There are several types of contracts which are required to exist when a business becomes involved in e-Commerce transactions. As a result, laws should regulate each section of those contracts to ensure that online customers transactions will go smoothly and that a judge can have clear regulations to rule with once an online dispute occurs. These include:

Website development: content and hosting agreements. When a business wishes to set up a website, it needs to ensure that the design and content of the website do not infringe or violate any third party rights.

For example, laws should regulate who is in charge of website content, the owner or the design company. Other related issues may arise from sites performance and security specially once a website start having heavy online transactions.

Internet service provider agreements: Companies who are responsible for developing the e-Commerce website can be the same companies who provide the hosting service or they can be separate. Similar to the web design companies, web hosting companies should have clear responsibilities regarding their duties and responsibilities. This may include laws about privacy, copyrights, etc. It also needs to be sure that their websites are properly hosted and will not suffer from excessive down time. These issues can be dealt with by website development, content, and hosting agreements. Disputes may occur between companies who provide the e-services and the company who support them or provide the hosting or the related tasks. Laws should regulate when a support company is liable for performance, reliability, or security problems. In general, supporting companies should provide explicit agreements of things they are liable to provide or control and will be compared to their rivals once their clients claim that they did not perform their expected duties.

Website usage and privacy policies: This may include the privacy of both owners and customers. Web site design and hosting companies are not supposed to expose their clients' information to their rivals. They should have implicit or explicit agreements with their clients of who is in charge of contents protection. In some cases, hackers may access an e-Commerce website to vandalize it. Clear boundaries should be drawn of what is considered as "reasonable" protection from the web design or hosting companies for their clients' information. This is usually compared to the security and protection that competitor companies provide.

Website and telephone sales terms and conditions: In some countries, online or telephone sales are governed by the Consumer Protection (Distance Selling) Regulations 2000 and the Electronic Commerce Regulations 2002. Such sales are generally conducted in a manner where there will be no scope for negotiating terms. Accordingly, any business hoping to trade in this way will require standard terms and conditions of sale. There are special rules which cover most sales to customers (subject to some exceptions), and give them more rights than they would have in a face-to-face purchase. These include:

A: A right to receive certain information as to the products and the identity of the seller. This will ensure protection from scammers or fake e-Commerce companies.

B: A right to cancel goods without any penalty or fees. This can be for up to certain amount of days after delivery if the necessary information has been provided to the customers and the right for customers to return their products without any charge, if sold products were not as prescribed. Return policies can be cumbersome for both clients and sellers in initial stages. On the one hand, sellers need to respect their buyers' right to undo a sale that they are not happy with, within certain amount of time. On the other hand, buyers need to learn that despite the fact that they have the right to return a product within certain time, and they should not do this without a logical convincing reason. As mentioned earlier, this can be initially complex and require time and cultural change.

C: A duty imposed on the seller to deliver goods within 30 days of the order (subject to an ability to extend or cancel)

Because the relevant regulations are laid down by European law, these rights apply to all customers located in any European Union country.

B. Software perspective: How to build an infrastructure for a trusted e-Commerce websites

This section will focus on the software and websites requirements to implement e-services or business.

In most e-Commerce infrastructures, to secure access to e-Commerce websites, it should be including two basic components in order to allow users to securely perform online transactions:

A: Digital certificates for web servers, providing guarantees of authentication, privacy and data integrity through encryption. Digital certificates can be issued by mediators called Certificate Authorities (CAs) to authenticate the seller to the buyer and vice versa. They can be generated through special programs or tools. They contain unique information about the user identity or machine to uniquely identify them from others. Digital certificates are also used to protect software products from piracy. Two users of particular software will have problem using it once they both go online as the owner of the software will discover that the key that was given for a particular client is used by more than one user.

Encryption is used to secure the information embedded in digital certificates. Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. Encryption uses mathematical formulas called cryptographic algorithms, or ciphers, and numbers called keys, to encrypt or decrypt information.

B: Secure e-payment system and management, to allow e-commerce sites to secure and automatically accept, manage and process online payments. This can be usually organized with owners' banks. Websites will be securely connected to the buyers' bank accounts. Once an online transaction is secured executed, the money should be directly transferred from the seller to the buyer account. This process should be performed in a fast, reliable, and secure way. Those three elements (i.e. reliability, performance, and security) are vital to the success of any e-Commerce website.

Laws should regulate any dispute on online transactions. Users may deny that they actually perform such transaction. They may claim that their cards were stolen. They may also claim that they have been double charged, or charged extra amounts. In some cases, insurance companies may provide services to cover such expenses.

C. Network and hardware perspective: Internet readiness

A closely related requirement to the software and websites' requirements is the existence of a network or hardware infrastructure. This may include the routers, fiber optics, or wireless communication channels, firewalls, etc.

Since both (software and hardware perspectives) may include hardware and software elements, they will be distinguished through the location. This perspective represents any requirements outside the user machine.

Generally speaking, Jordan has a relatively good network and internet infrastructure relative to most Middle East countries. Internet services exist in different forms in Jordan. They are also accessible to most citizens with a reasonable cost. Internet service is currently provided by several companies. It is also provided in different speeds such as dial-up, ADSL, and wireless. Users can access the internet from their desktops, laptops, and PDAs.

D. Extra requirements for a successful e-Commerce business

Another major player in the e-Commerce world is the shipping companies. In order to compete with normal shops and businesses, shipping should be also quick, reliable, and secure. Laws should regulate the terms for shipping, such as costs, types, and who is in charge in case of products defects. Products defects may due to buyers or shipping issues.

Despite the fact that an e-Business culture should exist in any country to allow such business to exist, however, laws and regulations should always assume the worst and be able to handle dispute cases.

V. CONCLUSION AND FUTURE WORK

In order to build an e-Commerce infrastructure in any company, the technical, network, and hardware requirements are not always the only barriers. The readiness for such technologies or services may require also improving or enhancing society, cultural, or legal regulations and perspectives to the new technologies.

Customers need to learn how to communicate online. They need to learn how to shop, sincerely post items online, committed to pay and ship on time. Businesses also need to be opened toward some necessary ethical e-Business manners such as giving their buyers certain period of time for returning the items or changing them.

Jordan Internet infrastructure is strong and capable of handling the construction of a trusted network. The private sector should take the lead in PKI and digital identity infrastructure. Once such infrastructure is established, many of those related and dependent industries can exist and provide an important economical input to the national revenue.

In future, the researchers will follow up with two research projects. They will create surveys to evaluate strengths and weaknesses in e-Government implementation in Jordan. Then they will try to distribute the survey

among those who can provide the right useful information for the purpose of the study.

The second track will use web metrics to evaluate the traffic and usage of e-Government websites in Jordan. This stage is expected to give the researchers a better image about the actual usage of those websites. It may indicate weaknesses or strengths in particular websites. In order to do that, the researchers may need the assistant and the cooperation of e-Government websites administrators to get websites log or to add scripts to monitor those websites.

REFERENCES

- [1] Secure computing corporation. Digital certificates. http://www.securecomputing.com/gateway/digital_certificates.cfm. 2008.
- [2] Conjecture corporation. What are digital certificates. <http://www.wisegeek.com/what-are-digital-certificates.htm>. 2008.
- [3] Comtrust. <http://www.comtrust.co.ae/docs/contactus.htm>. 2008.
- [4] WISEkey. <http://www.wisekey.com/press/-jordan32002.htm>. 2002. 2008.
- [5] Jordan e-government program, e-Government strategy. http://www.moict.gov.jo/moict/e_gov_strategy/e-Government%20Strategy.pdf. 2006. 2008.
- [6] Comtrust ties up Jordanian company ESKADENIA. AME Info. <<http://www.ameinfo.com/26458.html>>. 2003. 2008.
- [7] Ahmed Al-Omari and Hussein Al-Omari. E-Government Readiness Assessment Model. J. Computer Sci., 2 (11): Pages: 841-845, 2006. <<http://www.scipub.org/fulltext/jcs/jcs211841-845.pdf>>.
- [8] Zain - Jordan Mobile Telephone Services. <<http://www.jo.zain.com-/English/Business/BusinessServices/Pages/E-Government.aspx>>. 2008.
- [9] Netcraft, Certificate services. <<http://news.netcraft.com/SSL-Survey-CMatch/certs>>. 2006. 2008.
- [10] Holzer, Mark, and Seang-Tae Kim. DIGITAL GOVERNANCE IN MUNICIPALITIES WORLDWIDE, An Assessment of Municipal Web Sites Throughout the World. The E-Governance Institute/ National Center for Public Productivity Rutgers, the State University of New Jersey, Campus at Newark. 2003.
- [11] Holzer, Maroc, and Aroon Manoharan. Global Trends in Municipal E-Government: An Online Assessment of Worldwide Municipal Web Portals.
- [12] Holzer, Mark, and Seang-Tae Kim. DIGITAL GOVERNANCE IN MUNICIPALITIES WORLDWIDE (2007), A Longitudinal Assessment of Municipal Web Sites Throughout the World. The E-Governance Institute/ National Center for Public Productivity Rutgers, the State University of New Jersey, Campus at Newark. 2007.
- [13] West, Darrel. Global e-government. <http://www.insidepolitics.org/egovtdata.html>. 2005.
- [14] West, Darrel. Global e-government. <http://www.insidepolitics.org/egovtdata.html>. 2006.
- [15] West, Darrel. Global e-government. <http://www.insidepolitics.org/egovtdata.html>. 2007.
- [16] e-business infrastructure, W.H. Inmon, http://www.business.aau.dk/oekestyr/file/e-business_infrastructu_re.pdf. Billinmon.com 2000, 2010.
- [17] Thein, N.; Naing, T.T., Grid Security Framework for Managing the Certificate, Web Intelligence, 2006. WI 2006. IEEE/WIC/ACM International Conference on Volume , Issue , Dec. 2006 Page(s):166 – 169.
- [18] Dawn Jutla, Peter Bodorik and Yie Wang, Developing internet e-commerce benchmarks, Information Systems, Volume 24, Issue 6, September 1999, Pages 475-493. doi:10.1016/S0306-4379(99)00028-9
- [19] Brian Cusack, Assessing Business Value of IT and IS Risk: Security Issues, 20th Australasian Conference on Information Systems, 2009.

AUTHORS

Dr. Muhannad Al-Shboul is a member of the Researchers' Association and with the Computer Center, The University of Jordan, Amman, CO 11942 Jordan (e-mail: malshboul@ju.edu.jo).

Dr. Izzat Alsmadi is with the Department of Computer Information Systems, Yarmouk University, Irbid, CO 21163 Jordan (e-mail: ialsmadi@yu.edu.jo).

Submitted, August 11, 2010. Published as resubmitted by the authors on September 27, 2010.