

**ECONOMIC AND SOCIAL
COUNCIL**

Distr.
LIMITED
E/ESCWA/ICTD/2010/WG.5/Report
2 September 2010
ENGLISH
ORIGINAL: ARABIC

Economic and Social Commission for Western Asia (ESCWA)

REPORT**WORKSHOP ON BUILDING TRUST AND CONFIDENCE
IN ARABIC E-SERVICES
BEIRUT, 25-27 MAY 2010****Summary**

As part of its activities to build trust in electronic services in the region, the Economic and Social Commission for Western Asia (ESCWA) held a workshop on Building Trust and Confidence in Arabic e-Services from 25 to 27 May 2010 at United Nations House, Beirut. With the preparation of a study on building trust in e-services in the ESCWA Region, the Commission began its activities in this field in 2009, and continues its efforts as a crucial step for developing the information society in the Arab region.

The workshop aimed at building capacity in the field of trust in e-services, providing a platform for dialogue, debate and exchange of successful experiences, and getting acquainted with progress made in this regard in ESCWA member countries. It highlighted the importance of developing national plans to enhance the protection of infrastructure and information systems, and to raise the level of trust in e-services.

In addressing the importance of developing national strategies and frameworks to build trust and confidence in e-services, two consecutive sessions were dedicated thereto. The workshop also included two sessions on the importance of developing and harmonizing legal frameworks in the Arab region to enhance trust in e-services. The workshop included sessions to share experiences and discuss best practice, and highlighted requirements for improving trust in e-services, including the protection of networks and applications within institutions and the protection of critical infrastructure in different countries. Two sessions were devoted to presenting the main achievements in the Lebanese banking sector and American health sector, in relation to improving trust in e-services provided by these sectors. In light of these discussions, the workshop concluded with a set of recommendations for building trust in e-services in the Arab region, including the need to formulate national strategies/action plans to build trust and security through e-services, develop organizational structures and implement the necessary mechanisms to develop cyberlegislation, train judges and lawyers on such applications, and launch awareness programmes targeting the public sector, business owners, individuals, households and children, centered on the mechanisms for protecting the digital environment and methods of safe and ethical interaction with digital environments.

The workshop on Building Trust and Confidence in Arabic e-Services was attended by participants from 14 countries, including representatives from agencies and governmental departments concerned with e-services in the public and private sectors, and experts from the banking and health sectors.

CONTENTS

	<i>Paragraphs</i>	<i>Page</i>
Introduction.....	1-3	3
<i>Chapter</i>		
I. RECOMMENDATIONS	4-10	3
II. TOPICS FOR DISCUSSION	11-38	5
A. National strategies and frameworks for building trust in e-services.....	11-14	5
B. Legislative framework for building trust in e-services	15-17	6
C. Experiences from the United States in building trust in e-health and e-services	18-19	6
D. Best practice in building trust in e-services	20-25	7
E. Building trust in the e-banking sector, Lebanese experience.....	26-27	8
F. Experiences from the ESCWA region	28-34	8
G. Discussion	35-37	9
H. Recommendations and closing session	38	10
III. ORGANIZATION OF WORK	39-45	10
A. Date and venue.....	39	10
B. Opening.....	40-42	10
C. Participants.....	43	11
D. Agenda	44	11
E. Documents	45	11
ANNEXES		
I. List of participants		12
II. List of documents		15

Introduction

1. The spread of information and communications technology (ICT) and the development of e-services vary between different ESCWA member countries. Studies indicate that investment in e-services in their various forms, including e-Government, is still at its rudimentary stages in most of these countries. The unwillingness of Governments and the private sector to provide such services is due to weak trust in the digital environment and e-services. Trust in e-services and transparent interactions with individuals are the key factors that encourage individuals to use cyberspace and its applications as an alternative to traditional services. Although e-service developers allocate significant funding for infrastructure and developing necessary applications, the level of interest in transparent interaction with users is still weak and needs to be strengthened and developed, whether at the level of interaction mechanisms with citizens or at the level of cyberlegislation that legally preserves the rights of users. Personnel supervising the management of information systems also need to be trained, while overseeing the confidentiality of information exchanged via e-services, especially since the human element is deemed the weakest link in the system for maintaining confidentiality and providing confidence.
2. The workshop on Building Trust and Confidence in Arabic e-Services held by ESCWA from 25 to 27 May 2010 at the United Nations House in Beirut falls within the framework of the Information and Communication Technology Division (ICTD) activities aimed at enhancing trust in e-services. Work in this field began in 2009, when ESCWA prepared a study on building trust in e-services in the ESCWA region. The workshop was conducted because of the importance of the topic in enhancing investment in ICT and the dissemination of e-services. It aimed at building capacity in the field of trust in e-services, providing a platform for dialogue, discussion, exchanging successful experiences between countries, and ensuring better insight on progress made in ESCWA member countries in this regard. The workshop highlighted the importance of developing national plans to improve protection of the infrastructure and information systems, and enhance trust in all types of e-services.
3. The workshop was attended by participants from 13 Arab countries and the United States of America, representing Government agencies and departments concerned with e-services in both public and private sectors, ministries of telecommunication and information technology, as well as experts from banking and health sectors. Key findings of the workshop included a set of recommendations on the main tools to build trust in e-services in the Arab region. Recommendations covered all areas related to building trust in cyberspace and its services, taking into account the challenges and constraints in the region.

I. RECOMMENDATIONS

4. Discussions held during the workshop covered a number of topics closely related to building trust in the use of e-services in the ESCWA region, and led to a set of recommendations related to the topics of the workshop.
5. Recommendations concerning a national framework for building trust in e-services are as follows:
 - (a) To develop a national strategy/plan of action to build trust and confidence in e-services, and to identify key issues and priorities that Governments should address at a national level to build trust in e-services, and identify bodies responsible for each issue;
 - (b) To establish the national regulatory structures necessary to implement that strategy/plan of action, such as national teams/centres to respond to computer-related emergencies, set into action the work of these organizational structures, and delegate to them the necessary authority for their work.
6. Recommendations for a legislative framework to protect cyberspace security are as follows:
 - (a) To develop comprehensive cyberlegislation to cover all topics related to cyberspace, in line with the needs of the cyberenvironment and its applications, in particular those related to cybercrimes and maintain the privacy and confidentiality of personal information;

- (b) To train judges and lawyers on the application of cyberlegislation in the field;
 - (c) To promote homogeneity among cyberlegislation in force in Arab countries to facilitate e-transaction and build an Arab information society, and emphasize the importance of the ESCWA initiative for regional harmonization of cyberlegislation;
 - (d) To get acquainted with international and regional treaties and conventions in the field of cyberlegislation, to develop and adopt local cyberlegislation, if appropriate.
7. Recommendations for raising awareness to build confidence in e-services are as follows:
- (a) To launch awareness programmes targeting decision makers on the importance of protecting cyberspace and building trust in e-services;
 - (b) To launch awareness programmes targeting workers in the public sector, business owners, individuals, households and children on protection mechanisms in the digital environment and safe, secure and ethical interaction;
 - (c) To use all communication and media means to raise awareness on the protection and security of cyberspace.
8. Recommendations for the development of secure and reliable e-services are as follows:
- (a) To prepare a clear definition of trust, development of a manual and guidelines on how to develop safe and strengthened e-services and applications resilient to external risks and threats, and propose investment and technical standards in this regard;
 - (b) To adopt novel and innovative methodologies for the development of reliable e-services, and develop necessary mechanisms to maintain the privacy and confidentiality of personal information;
 - (c) To involve the end-user in the design of e-services, determination of their characteristics and conditions of operation, and to provide citizen-centric services presenting more added value;
 - (d) To focus on the specificity of the Arab region, reflected in the use of the Arabic language, and develop digital Arabic content.
9. Recommendations for the development of educational programmes and research and development programmes are as follows:
- (a) To update educational programmes and include a number of specialized topics related to the protection and security of cyberspace, encourage universities to train experts in the field of safety and protection of cyberspace and develop secure and reliable ICT applications;
 - (b) To launch specialized training programmes for workers in the public and private sectors, particularly those supervising the operation of information technology systems on the security of such systems; and on the importance of maintaining the confidentiality of information in order to gain the confidence of users;
 - (c) To encourage research and development in the field of ICT protection and security in national universities and research centers;
 - (d) To include cyberlegislation issues in ICT curricula and majors, and to include special programmes for the use of ICT in law school curricula at ESCWA member country universities.

10. Recommendations for national, regional and international cooperation for building trust in e-services are as follows:

(a) To share information on the risks and threats of information technology between governmental bodies and private sector companies at a national level, and establish partnerships and enhance cooperation between the private and public sectors in order to build trust in e-services;

(b) To exchange successful experiences in the field of reliable e-services, work on disseminating such experiences in the region, exchange expertise and experience on ways to confront current threats, and seek to link national computer emergency response teams/centres (CERTs) at regional and international levels;

(c) To continue organizing regional workshops and meetings to exchange expertise and experience in the field of building trust in e-services.

II. TOPICS FOR DISCUSSION

A. NATIONAL STRATEGIES AND FRAMEWORKS FOR BUILDING TRUST IN E-SERVICES

11. Following the opening, the first session of the workshop was held to address national strategies and frameworks for building trust in e-services. Mr. Belhassen Zouari, Director General of the National Agency for Computer Security at the Ministry of Communication Technologies in Tunisia, made a presentation on developing a strategy for cybersecurity and establishing a team that would assume the role of an operational tool to respond to computer emergencies. Mr. Zouari reviewed the main components of the national strategy for cybersecurity, namely defining the appropriate legal framework for the protection of cyberspace, training and awareness-raising to build trust in e-services, and finding appropriate mechanisms for practical implementation of national strategy measures. The presentation highlighted the importance of establishing units to respond to computer emergencies (CERTs), to secure cyberspace at a national level, in view of their key role in the prompt and efficient response to Internet incidents and in preparing institutions and individuals to face the risks of cyberspace, through awareness programmes and training. In addition, Mr. Zouari presented the Tunisian strategy in the field of cyberspace, in detail, as a case study.

12. At the second session on strategies, Ms. Nibal Idlebi, chief of the Information and Communication Technology Applications Section at ESCWA, made a presentation on international and regional efforts to build trust in e-services. The presentation started with defining the main problems facing the use of a digital environment and e-services, it then pointed to the global dimension regarding issues of protection and trust in the digital environment, and reviewed efforts made by a number of international and regional organizations in this field. Ms. Idlebi specifically highlighted the efforts of the International Telecommunication Union in the protection and security of cyberspace, the efforts of the European Union aimed at building trust in cyberspace and its services, relevant efforts made by the Organization for Economic Co-operation and Development, and efforts of the United Nations General Assembly. Ms. Idlebi then reviewed activities carried out by ICTD in the field of building trust in e-services in the ESCWA region, and focused on national strategies/plans of action in this field.

13. Mr. Sherif Nour El-Din, consultant in the field of protection of information systems at the Information Technology Industry Development Agency in Egypt, presented best practice in ensuring the security of e-services in Egypt. He pointed to the main security measures designed to ensure the provision of sound e-services, as well as to a number of necessary actions for the facilitation of providing such services on the Internet in Egypt. Mr. Nour El-Din stressed the importance of special legislation in e-services and adequate infrastructure for e-signatures. He presented, in detail, the structure of work for providing e-signatures, and the relationship between different stakeholders, particularly the relationship of the Information Technology Industry Development Agency at the Ministry of Communications and Information and Technology and the competent authority for digital authentication.

14. Mr. Nasser Khalaf, Director General at the National Information Center in Jordan, presented a lecture on the security and protection of information in his country. He gave an overview of Internet penetration in the public sector and the information security policy in Jordan. He explained that the Government issued a policy on information security and protection and circulated it to all institutions. The circulated document defines security requirements for each unit or department and the security solutions. It also outlines resources that must be protected, and the extent to which they must be respected by concerned parties in order to provide the necessary protection. Mr. Khalaf pointed to the completion of necessary studies for the establishment of the national center for the management of information technology security incidents in Jordan.

B. LEGISLATIVE FRAMEWORK FOR BUILDING TRUST IN E-SERVICES

15. Mr. Younes Arab, Chairman of the Arab Law Group in Jordan, opened this session with a general assessment of cyberlegislation in the Arab region. He highlighted vulnerabilities in the majority of Arab countries, whether in terms of a slow issuance of laws related to cyberspace and the use of e-services that protects the user and secures their rights, or in terms of the absence of necessary procedural measures to implement these laws, if any. He stressed the need to consolidate efforts to develop an action plan in the field of cyberlegislation in the Arab region to ensure mechanisms aimed at revising existing texts in certain countries and reconsidering them if needed, or issuing new laws in other countries to build trust in e-services. Mr. Arab affirmed the importance of efforts exerted by ESCWA in this field, particularly with regard to the preparation of cyberlegislation models and the project on harmonization of such legislation in the Arab region.

16. Mr. Belhassen Zouari reviewed the most important legal aspects needed to address ICT issues. He started with defining a number of legal concepts related to cyberspace, such as electronic crime and evidence in digital space. He stressed the need for an integrated legislative and legal framework as a first step towards ensuring cybersecurity and building trust in e-services. Mr. Zouari gave a presentation on the Tunisian experience in this field, and pointed to the Tunisian Cybersecurity Legal Framework, as he reviewed a number of laws issued in recent years for ensuring the protection of cybersecurity, such as the Computer Crime Law 1999, the Electronic Certification Act, Intellectual Property Laws 2000 and 2001, the Computer Security Act and Privacy Protection Act 2004, as well as the Act on Cyber Terrorism 2003.

17. Ms. Mima El-Hajj Barbar, Information Technology Officer in the ICT Policies Section at ESCWA, gave a detailed presentation on the results of ESCWA efforts to improve the cyberspace legislative framework in the region. She reviewed the most important accomplishments of the ICT Division in this field since 2007. In addition, she presented the ESCWA initiative for the regional harmonization of cyberlegislation to promote the knowledge society in the Arab world, launched in 2009. The main objectives of the initiative are to develop cyberspace guidelines and model laws similar to the European laws and guidelines, to be adopted in Arab countries; contribute to building capacity for the development of such legislation; and enhance the use of ICT applications in the public sector as well as in economic, cultural and social activities.

C. EXPERIENCES FROM THE UNITED STATES IN BUILDING TRUST IN E-HEALTH AND E-SERVICES

18. This session was dedicated to a number of experiences from the United States in the field of building trust in e-services. It included two presentations, where dialogue with the lecturers was made available through videoconference. Mr. Eric Danker, expert in ICT affairs, opened the session with a presentation on certain general concepts related to protection and trust in the internet. He reviewed building trust through the supervision and protection of data and issuance of adequate policies that encourage citizens to use e-services. In addition, Mr. Danker noted the importance of communication channels in the process of building trust, especially to exchange opinions and reactions, thus enhancing transparency in transactions and increasing the trust of citizens in the use of e-services.

19. The second presentation was made by Ms. Lucy Drury, expert in ICT, on the United States experience in building trust in e-health services. Ms. Drury explained that the last twenty years were a slow transitional period that marked the beginning of the transfer of e-health services from medical records to e-medical records. She clarified that this transition is not yet complete, due to several reasons, mainly the reluctance of many health service providers to stop using paper records, the cost of such a transition, and the lack of trust in e-records. Ms. Drury then pointed to the Health Insurance Portability and Accountability Act for the health care sector, and its impact on the use of e-records. The Act covers the unification of administrative practice, procedures for bill calculation, and the standardization of electronic transmission to citizens, privacy of medical information and the protection and limitation of access to such information to authorized persons.

D. BEST PRACTICE IN BUILDING TRUST IN E-SERVICES

20. Two sessions of the workshop were dedicated to this issue. The second day started with a presentation by Mr. Fadi Moubarak, Director General of Cisco in the Arab Mashreq, on eServices Technologies: Enablers or Barriers. Mr. Moubarak stressed the importance of technological infrastructure in e-commerce websites, and of innovation in the design of these sites. He reviewed the results of an evaluation study prepared by Cisco in 2009 comprising a large number of e-commerce sites. The study results showed that while foundational capacities are strong across most of the sites, it is their innovative capabilities that raise the “top 12” sites above the rest. Innovation is reflected in the inclusion of new technologies in e-commerce, such as the use of social networks and mobile technologies. Mr. Moubarak stressed the necessity of interaction and ease of use, security and speed of access to information, in addition to providing special services in order to enhance the trust of customers in e-services.

21. Mr. Saleem Zoughbi, ESCWA Regional Advisor on ICT, made a presentation on Extending e-Governance to data security and privacy. He pointed out that e-Governance is an opportunity for Arab Governments to get closer to the citizen and to build partnership with diverse communities of interest, practice and expertise, and thus to gain the confidence of citizens in e-services. Hence, building trust in e-services starts with trusting electronic goods governance and democracy, which require a radical change in decision-making, provision of services and the use of technology in Governments. Mr. Zoughbi stressed the importance of providing added value in e-services to encourage citizens to use them.

22. Regarding e-health, Mr. Moutasem Shafa’amry, Professor at the International University for Science and Technology, highlighted the lack of e-health services in the Syrian Arab Republic. He pointed, however, to the preparations for such a step in a number of health institutions, as most hospitals are using ICT in management, in addition to initiatives taken to interlink emergency points. Mr. Shafa’amry pointed out that in April 2010, the Ministry of Health declared the launch of a process to identify necessary criteria for the establishment of an electronic file for the patient.

23. Mr. Zouari gave a presentation on the importance of raising awareness to create a culture of cybersecurity, which would increase safe practice and reduce the risks of cyberspace. Mr. Zouari presented the Tunisian experience in this field, as he pointed to the most important outreach programmes provided by the Center for Computer Emergencies, targeting all community groups, including children, youth, parents, teachers, staff and managers as well as other stakeholders in the civil sector. He explained the strategy developed by Tunisia for cybersecurity awareness and mechanisms used for successful implementation.

24. Mr. Abdulrahman Alfriah, General Manager of the Computer Emergency Response Team (CERT), presented the functions of CERT in Saudi Arabia, namely to boost the National Information Security awareness level, to coordinate national efforts towards promoting IT security best practice, and creating trust within the cybercommunity, and to help in managing information security attacks and incidents. Mr. Alfriah indicated that CERT plays an important role in Saudi Arabia, being the reference point of information security for the cybercommunity, in building human capacity in the field and helping to build a trusted

environment for e-transactions. In addition, Mr. Alfriah presented the structure of the centre as well as the mission and role of each unit.

25. Mr. Ahmad Kamal, Projects Manager at the Ministry of State for Administrative Development in Egypt, presented the role of his ministry in the process of building trust in e-services. He explained the main initiatives in this field, including the provision of free Internet and establishment of ICT clubs, which would increase the number of Internet users in Egypt. In addition, Mr. Kamal reviewed the project of building an e-Government that would provide its services through the Egyptian e-Government website. He highlighted Government initiatives, including the blog on the Egyptian Government Services Portal launched in October 2009, which facilitates interaction with beneficiaries, discussion of new ideas for service delivery and evaluation of e-services.

E. BUILDING TRUST IN THE E-BANKING SECTOR, LEBANESE EXPERIENCE

26. Mr. Jean-Michel Kaoukabani, Head of the Information Security Department in Byblos Bank Group, gave a presentation on data privacy in the banking sector. He stressed the need to integrate information security in the overall process of management. He explained the importance of data, information assets and their value, which makes them vulnerable to internal intended and unintended threats, in addition to external threats stemming from the exploitation of security vulnerabilities and the disruption of services. Mr. Kaoukabani presented the Open Web Application Security Project, which is an open network dedicated to enabling institutions to buy, develop and protect their applications. The project also allows free access to tools and standards that ensure the security of applications, as well as to books on security and protection, and to take advantage of open libraries and relevant research and conventions.

27. Ms. Zeina Aoun, Head of Security Division at the IT Department in Banque du Liban (BDL), highlighted the progress of the Lebanese banking sector in the field of e-services. This has enabled Lebanon to assume a leading role in the Middle East as a provider of e-services, including e-commerce, e-banking, and e-financial services. It has also made the country a haven for secure payment among banks, markets and Governments within and across borders. Ms. Aoun explained the most important solutions adopted by BDL to ensure the security of its services, such as the Secure Electronic Banking and Information for Lebanon (SEBIL) project that includes electronic payment and reporting systems, a treasury management system and asset management. She also reviewed the infrastructure developed by BDL to build trust in e-banking services.

F. EXPERIENCES FROM THE ESCWA REGION

28. Mr. Maher Suleiman, Director General of the National Agency for Network Services (NANS) at the Ministry of Communications and Technology in the Syrian Arab Republic, made a two-folded presentation. The first part dealt with the law on electronic signature which was issued in 2009, whereas the second part explained the functions of NANS established under that law. Mr. Suleiman indicated that the law on electronic signature legitimated the use and adoption of e-signature and granted it the same authenticity as written evidence (such as the common signature, stamp and others). He also introduced basic rules for dealing with e-signature and digital certificates. Mr. Suleiman pointed out that NANS began its work at the beginning of March 2010, is a public governing body that has a legal personality, financial and administrative independence, and is linked to the Minister of Communications and Technology. Its core mission is to develop e-signature systems and controls, monitor their implementation, and grant licenses to provide e-signature services and management of Syrian top-level domain names (.sy and سورية).

29. Ms. Cheema Anzi, Advisor at the Ministry of Electricity and Water in Kuwait, presented a document on the legal reading of recent trends for the settlement of emerging disputes on e-commerce. Ms. Anzi explained the means for settling emerging disputes related to e-transaction, particularly in the light of difficulties arising on the competence of ordinary courts, applicable law and implementation of provisions of judicial authorities and foreign arbitrators. She reviewed the role of regular courts in this field, as well as

such alternative means for settling disputes arising from e-transactions, as negotiation, conciliation, mediation and arbitration.

30. Mr. Adel Al-Faqih Hassan, member of the National Committee for Digital Certification in the Sudan, gave a presentation on legislation supporting e-Government. He started by reviewing e-Government work in the Sudan, as well the main projects to be implemented in this framework, such as building a single portal, developing and building workflow systems, document management, service provision and the establishment of a secure governmental network. Mr. Hassan subsequently overviewed the Electronic Transactions Act and Cybercrime Act, issued in 2007, as he explained the content of these laws and their means of implementation. He presented the main projects within the five-year plan for the period 2007-2011, such as the completion of legislation on electronic financial transactions, the digital laboratory for media studies, as well a number of other projects.

31. Ms. Heyam Hazeem, Assistant Director at the Service Delivery Department at the e-Government Authority, presented the Bahrain e-Government Programme. She referred to the e-Government vision 2030 centered on improving e-services and making them available to everyone. She reviewed a number of services provided by the Bahrain e-Government and its main initiatives, such as the mobile e-Government project, which so far comprises 49 services. In addition, Ms. Hazeem outlined some strategic projects aimed at achieving an integrated e-Government, including the Bahraini identification card and electronic gates at airports.

32. Mr. Ahmad Al-Tayyar, General Manager of Networks and Computers at the National Information Center in Yemen, presented the status of e-services in Yemen as well as the constraints faced by this sector. He focused on efforts exerted by the Yemeni Government for the dissemination of these services in several such areas as banking, bill settlement, e-training and education, and e-commerce. He explained the obstacles faced by the dissemination and development of these services in Yemen, mainly the rate of Internet penetration and computer networks, lack of awareness about the use of information technologies in the field of services, lack of trust in e-services, legislative aspects and cultural and educational barriers. He explained that the Government works hard to improve the status quo, and has implemented a number of projects, including the information national network, and the issuance of e-transaction and information acts.

33. Ms. Samira Salem, IT Undersecretary at the Ministry of Telecommunications and Information Technology in Yemen, and Director General of the National Programme for Information Technology, focused, in her presentation, on building trust in e-services in Yemen, the efforts of the Ministry in supporting e-services and its cooperation with stakeholders within Yemen and from the international community and its organizations. She presented a document on the strategic vision for the role of ICT in supporting comprehensive development plans in Yemen in the period 2001-2025. Plans include an overview of the role of ICT in the economic, social, scientific, cultural and political sectors.

34. Mr. Mohammed Al-Muqadem, Senior Manager of the legal affairs unit at the Telecommunications Regulatory Authority in Oman, outlined the role of the Authority in managing and supervising the Information and e-services sector. The Authority assists in granting licenses to bodies entrusted with the provision of e-services and oversees their delivery. He affirmed the importance of royal decrees and laws regarding the organization of information and e-transactions in this field and ministerial decisions that impose the obligation of protecting individuals, in order to enhance the trust of citizens in using e-services.

G. DISCUSSION

35. Ms. Nibal Idlebi opened the discussion with a presentation on challenges faced in the process of building trust in e-services in the region, through a number of issues related to national strategies, cyberlegislation, the role of protection centres, the use of technologies and safety and protection applications, the design of reliable applications, the raising of awareness, and international and regional cooperation. Then, discussion about these issues began, as participants defined priorities and challenges according to the

specificities of each country. Participants pointed to the need for legislation that would protect the rights of the citizen and enhance trust in using e-services. They stressed the necessity of involving citizens in service selection and method of provision. They also considered the facilitation of service use and the provision of transparency to build trust between the Government and the citizen.

36. Participants noted the need to manage change and urged managers and officials in Government agencies to commit to the shift towards e-services and enhancing trust in such services. They also discussed the allocation of sufficient resources to ensure the sustainability and security of provided applications and e-services. In addition, participants stressed the need to organize awareness campaigns to build the culture of cyberspace protection and the safe and secure use of e-services. They stressed the importance of these campaigns targeting all categories of society, including decision makers, officials and Government employees, as well as the private sector and end-users.

37. Discussions reaffirmed the importance of investment in the ICT sector, including e-services, and the necessity of a clear vision on services and how to provide them in a secure way. Participants thus defined priorities in this field, mainly developing a comprehensive national plan of action for the development of reliable e-services; cooperation between the private and public sectors for the development and provision of services; cooperation between Arab countries to build trust in e-services; provision of successful examples of services offered by Arab Governments; organization of workshops in this field; and setting standards in the provision of reliable e-services.

H. RECOMMENDATIONS AND CLOSING SESSION

38. Mr. Yousef Nusseir, Director of ICTD at ESCWA concluded the workshop on the third day in a session dedicated to recommendations and concluding observations. Ms. Nibal Idlebi and Ms. Mirna El-Hajj Barbar presented a set of recommendations drawn from discussions. Participants agreed to the initial version of the recommendations, and ESCWA indicated that it would send recommendations electronically to all participants in order to include their observations before issuing the final version.

III. ORGANIZATION OF WORK

A. DATE AND VENUE

39. The ICT Division at ESCWA held a workshop on Building Trust and Confidence in Arabic e-Services, from 25 to 27 May 2010 at United Nations House in Beirut.

B. OPENING

40. Mr. Yussef Nusseir, Director of ICTD opened the workshop by welcoming the attendees. He focused on the importance of e-services in building an information society, advancing the development process, increasing transparency and bridging the digital divide between the ESCWA region and other regions. He stressed the importance of trust in and transparency of e-services as the two main factors that would encourage individuals to use cyberspace and its applications as an alternative to traditional services. Mr. Nusseir declared that in spite of important funding being allocated to infrastructure and development of applications, the interest of service developers in transparency in their interaction with users is still weak and needs to be enhanced and developed whether at the level of interaction mechanisms with citizens or of cyberlegislation that guarantees the legal rights of users. In addition, Mr. Nusseir stressed the need to train human resources to supervise information systems in order to ensure the confidentiality of information exchanged through e-services, especially as the human element is considered to be the weakest link in the system designed to preserve confidentiality and confidence. He pointed to the responsibility of Governments in building this trust through laws that protect users, and to the important role of service providers in building the desired confidence. Mr. Nusseir pointed to the study launched by ESCWA last year on building trust in e-services and presented its five themes, namely:

1. National strategic framework to enhance trust in e-services.
2. Legislative framework.
3. Protection and security in cyberspace.
4. Education and training.
5. Development of reliable e-services.

41. At the end of his statement, Mr. Nusseir expressed his hopes that participants come out with recommendations that benefit decision makers in the field, and contribute to achieving the desired objectives of the workshop.

42. Ms. Nibal Idlebi presented the workshop agenda, and noted that it would include discussion and deliberation sessions, as well as the planned presentations.

C. PARTICIPANTS

43. The workshop brought together around thirty participants from thirteen Arab countries, namely Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Saudi Arabia, The Sudan, The Syrian Arab Republic, Tunisia, and Yemen. Participants mainly included representatives of ministries and governmental bodies providing e-services in public and private sectors, as well as experts from the banking and health sectors.

D. AGENDA

44. The agenda of the workshop is as follows:

1. Opening.
2. Two Sessions on National Strategies and Frameworks for Building Trust in e-Services.
3. Session on the Legal Framework for Building Trust in e-Services.
4. Session on Experiences from the United States in Building Trust in e-Health and e-Services.
5. Two Sessions on Best Practice in Building Trust in e-Services.
6. Session on Building Trust in the e-Banking Sector.
7. Two Sessions on Experiences from the ESCWA Region.
8. Panel for Discussion.
9. Recommendations and Closing Remarks.

E. DOCUMENTS

45. A list of documents submitted at the workshop is included in annex II to this report. Documents can be accessed on ESCWA website: <http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=1246E>.

Annex I*

LIST OF PARTICIPANTS

Bahrain

Ms. Heyam Hazeem
Assistant Director
e-Government Authority
E-mail: hhazeem@ega.gov.bh

Ms. Buthaina Khalil
Health Licensure Specialist
Ministry of Health
E-mail: bwahab@health.gov.bh

Egypt

Mr. Sherif Nour El-Din
Senior Cybersecurity Consultant and Head of the
Root CA
ITIDA
E-mail: snoureldin@itida.gov.eg

Mr. Ahmed Raafat
Senior Infrastructure Engineer
Ministry of State for Administrative Development
E-mail: araafat@ad.gov.eg

Mr. Ahmed Shaaban
Senior Projects Manager
Ministry of State for Administrative Development
E-mail: Akamal@ad.gov.eg

Iraq

Ms. Tayseer Hameed
Manager of Training and Research Department
Ministry of Communications
E-mail: tayseer@moc.gov.iq

Jordan

Mr. Khaled Lahham
Acting General Secretary
Ministry of Information and Communications
Technology
E-mail: Khaled.l@moict.gov.jo

Mr. Nasser Khalaf
Director General
National Information Technology Center
E-mail: nasser.k@nitc.gov.jo

Dr. Younis Arab
Chairman
Arab Law Group
E-mail: lawoffc@nets.jo

Kuwait

Ms. Shimah Alenezi
Counsellor
Ministry of Electricity and Water
E-mail: maasi50@hotmail.com

Lebanon

Mr. Fadi Moubarak
General Manager
Cisco (Levant)
E-mail: fmoubara@cisco.com

Ms. Leila Serhan
General Manager
Microsoft (Levant)
E-mail: leila.serhan@microsoft.com

Mr. Mark Chaban
MEA Security and Privacy Director
Microsoft (Dubai)
E-mail: mark.chaban@microsoft.com

Mr. Jean-Michel Kaoukabani
Head of Information Security
Byblos Bank
E-mail: jmkaoukabani@byblosbank.com.lb

Ms. Tania Zaroubi
Senior ICT Project Manager
Office of the Minister of State for Administrative
Reform
E-mail: TZaroubi@omsar.gov.lb

* Issued as submitted.

Lebanon (continued)

Ms. Zeina Aoun
IT Security Manager
Banque Du Liban
E-mail: zaoun@bdl.gov.lb

Oman

Mr. Mohamed Al Muqadam
Senior Manager
Telecommunications Regulatory Authority
E-mail: almuqadam@tra.gov.om

Palestine

Mr. Riyad Hamarsha
Legal Assistant
Ministry of Telecommunication and Information
Technology
E-mail: Hamarsheh00@yahoo.com

Saudi Arabia

Mr. Abdulrahman Al Friah
General Manager
CERT-SA
E-mail: afriah@citc.gov.sa

The Sudan

Dr. Adil Alfaki Hassan
Member
National Digital Certification Committee
E-mail: adilalfaki@hotmail.com

Ms. Alawia Alhamadabi
Manager of International Relations
National Information Center
E-mail: ahamadabi@hotmail.com

Syrian Arab Republic

Dr. Ahmad Bassel Alkhchi
Deputy Minister
Ministry of Communications and Technology
E-mail: balkheshi@moct.gov.sy

Dr. Maher Suleiman
General Director
National Agency for Network Services
E-mail: director@nans.gov.sy

Dr. Moutasem Shafa'amry
Head of Computer Science Department
International University for Science and
Technology
E-mail: moutasem@scs-net.org

Tunisia

Mr. Belhassen Zouari
CEO
National Agency for Computer Security
E-mail: b.zouari@ansi.tn

United States of America

Mr. Eric Danker
Expert in ICT
E-mail: danker@gmail.com

Ms. Lucy Drury
Expert in IT
E-mail: lhd0240@charter.net

Yemen

Mr. Ahmed Al-Tayar
Director General of Networks and Computer
National Information Center
E-mail: altiar@y.net.ye

Ms. Samira Salem
Assitant Deputy Minister
Ministry of Telecommunication and Information
Technology
E-mail: samirasptc@yahoo.com

Economic and Social Commission for
Western Asia (ESCWA)

Mr. Yousef Nusseir
Director
ICT Division
E-mail: nusseir@un.org

Mr. Mansour Farah
Chief, ICT Policies Section
ICT Division
E-mail: farah14@un.org

Ms. Nibal Idlebi
Chief, ICT Applications Section
ICT Division
E-mail: idlebi@un.org

Economic and Social Commission for
Western Asia (ESCWA) (continued)

Mr. Saleem Zoughbi
Regional Advisor on ICT
ICT Division
E-mail: zoughbi@un.org

Ms. Mirna Barbar
IT Officer
ICT Division
E-mail: barbarm@un.org

Mr. Matthew Perkins
IT Officer
ICT Division
E-mail: perkinsm@un.org

Mr. Marc Khayat
Research Assistant
ICT Division
E-mail: khayat@un.org

Annex II

LIST OF DOCUMENTS

Title	
1.	Documents
	<ul style="list-style-type: none">- Agenda- Preliminary information note
2.	Presentations
	<p>During the two sessions on National Strategies and Frameworks for Building Trust in e-Services:</p> <ul style="list-style-type: none">◦ Establishing a cybersecurity strategy and setting up a CERT as an implementation tool;◦ International and regional initiatives for building trust in e-services;◦ Egyptian best practices: securing e-services;◦ Jordanian strategy: data security and procedures. <p>During the session on the Legal Framework for Building Trust in e-Services:</p> <ul style="list-style-type: none">◦ Plan of action in the field of cyberlegislation to build trust in Arab e-services;◦ What legal aspects are needed to address specific ICT-related issues?◦ Harmonization of cyberlegislation in the Arab region. <p>During the session on Experiences from the US in Building Trust in e-Health and e-Services:</p> <ul style="list-style-type: none">◦ Building trust in a connected world;◦ Building trust in e-health services: the US experience. <p>During the two sessions on Best Practice in Building Trust in e-Services in the region:</p> <ul style="list-style-type: none">◦ E-services technologies: enablers or barriers? (Cisco presentation);◦ Extending e-governance for data security and privacy;◦ Security requirements and techniques for building trust in e-health services;◦ Raising Awareness to create a culture of cybersecurity;◦ Safe delivery to the customer and commerce (cloud computing) (Microsoft presentation);◦ Measures for secure national e-transactions (in Saudi Arabia);◦ Building trust in e-services (Egypt case). <p>During the session on Building Trust in the e-Banking Sector, Lebanon experience:</p> <ul style="list-style-type: none">◦ Data privacy and emerging threats (Byblos Bank);◦ IT security in Banque du Liban. <p>During the two sessions on Experiences from the ESCWA Region:</p> <ul style="list-style-type: none">◦ The e-signature law and the national agency for network services in the Syrian Arab Republic;◦ Conflict resolution in e-transactions: the role of cyberlegislation (Kuwait);◦ E-Government legislations in the Sudan;◦ Bahrain e-Government programme;◦ Building trust in e-services: the case of Yemen;◦ Organization structure of the Telecommunications Regulatory Authority in Oman.