



July 2006

Background Paper On Radio Frequency Identification (RFID) And The Public Policy Implications

BACKGROUND

Radio frequency identification is a subset of a group of technologies, often referred to as automatic identification technologies, that are used to help machines identify objects, and which include bar codes and smart cards. RFID refers to the subset of automatic identification that uses radio waves to identify an object. An RFID system typically will include a chip attached to the object that contains a number identifying the object (and perhaps other information) and which is connected to an antenna, forming an RFID transponder or RFID tag. The antenna enables the chip to communicate via radio waves to a reader which converts the radio waves from the chip into a form that can be passed on to computers that store information about the object to which the tag is attached.

The simplest tags are "passive"—without their own power supply, receiving power from the electromagnetic waves emitted by the reader which induce a current in the tag which allows the transmission of the information stored on the tag. Other tags are "active" containing some form of power supply to broadcast the information to the reader. Active tags transmit over a much longer range than passive tags—100 feet or more, for instance, compared to under ten feet for passive tags. Tags can be "dumb" without any capability of processing data on-board or "smart" with such capacity including the ability to use encryption or authentication systems. Tags can also be linked with sensors for measuring conditions such as pressure or heat. Tags can have chips that can be read-write, where information can be added to the tag, read-only tags or electrically erasable programmable read-only memory where data can be overwritten using an electronic process.

All the possible differences are reflected in the cost of the chips. Active chips, smart chips, and read/write chips are all more expensive than their passive, dumb, and/or read only counterparts. RFID has, until recently, been used only to track expensive items because of the cost of the chips which, in many cases, has exceeded several dollars a chip.

The two other critical elements of the system are the readers which interrogate the chips and receive the identification and other data and the network for the transmission and storage of information about the objects. Readers vary in the frequencies that they use to read tags; low frequency readers and tags are cheaper

than ultra high frequency readers and tags, use less power, and penetrate non-metallic substances better. On the other hand, ultra high frequency tags provide greater range for the readers and can transfer data faster than their lower frequency counterparts. Both higher and lower frequency systems have certain advantages over bar code systems in that they can read objects within their range without line of sight access; they can also read multiple objects at the same time, unlike the one by one scanning of objects carrying bar codes. Readers presently cost approximately \$500-\$1000 each and, until recently, have generally been able to use only one frequency to read tags.

A network is required to transmit the data from the readers to databases where information about the identified object is stored.

These elements are combined into RFID systems which can have very different capabilities and characteristics, depending on the applications for which they are used. Because RFID is an infrastructural technology, these applications are virtually unlimited. Different applications will have different technological and economic requirements; some applications, for example, will require longer read ranges while others depend on the tags being only inches away from the readers. Some systems require highly secure communications between readers and tags while other systems that use much less sensitive information have lower security requirements.

ABOUT WITSA

WITSA is a consortium of over 60 information technology (IT) industry associations from economies around the world. WITSA members represent over 90 percent of the world IT market. As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information.

RECENT DEVELOPMENTS

Several developments have increased the potential for the pervasive use of RFID and the creation of what has been called an "Internet for things".

The most important development is that it has become possible to dramatically reduce the cost of the chips—something of critical importance if billions and even trillions of chips need to be attached to objects. While technology advances allow greater functionality to be achieved on the same size chip, it also allows the same functionality to be achieved on progressively smaller chips. Tags now being produced are roughly the size of a grain of rice and cost, it is estimated, between 5 and 10 cents each when produced in volume; even smaller tags are being developed and with new printing and antenna technologies it is estimated that prices could fall to a penny a tag or less. At the same time, the costs for readers, and network transmission and storage are all declining, following the trends common to information technology products. These price declines, and increases in the capabilities of RFID system components have provided an exciting environment for RFID development.

Recognizing these possibilities, and under the leadership of the Auto ID Center at MIT, (sponsored by a number of manufacturers, retailers, and service providers from around the world), an RFID system was developed as a "next generation" bar code system to be used for inventory management and the tracking of goods. Based on the Electronic Product Code (EPC), this system established open standards for very small, inexpensive passive chips which would include unique identifiers that could be attached to all packaged goods—from a soft drink can to a razor to a computer printer. At the same time the Center developed a system similar to the Internet's Domain Name System, which would allow EPC participants to locate where data about a particular tagged item are stored. Thus rather than having to add memory or processing to the tag itself—thereby increasing the cost of the tag dramatically--the amount of information available about the tagged item would be limited only by the costs of adding information to a database on the network.

The Center also created a "physical mark-up language" based on XML to describe the physical attributes of objects and oversaw the development of an agreement about a code for the EPC chips themselves which went beyond the information now included on bar codes but and included a unique identifier for *every* object; the present code space on an EPC chip would allow for a unique identifier, for example, for every molecule in the universe.

The EPC system's open standards allowed the competitive supply of small, inexpensive tags the development of "agile" readers that can utilize more than one frequency, and middleware that can ease the flow of billions of transactions generated by reading tags and connecting to databases. When the research phase of the project was complete, MIT's Auto ID Center turned over the implementation of the EPC system to EPCglobal, a joint venture of the Uniform Code Council and EAN which have overseen the bar code system around the world.

Overall, the EPC system was designed to make the supply chain much more visible, from manufacturer through distributor to the retail outlet at various points along the way. Each object could be tracked, and its attributes recorded, with additional details that might prove useful such as expiry dates, chemical composition of the packaging etc. Each participant in the supply chain could have access to that information that it requires such as when the item was shipped, received, where it was stored etc. Each participant could automate processes using the machine-readable data replacing today's manual handling as appropriate. The wide spread deployment of such a system would allow better inventory management, eliminating excess production and shipping, reducing inventory on hand, and increasing a retailer's ability to make sure that the right items are on the right shelf in the right amount to meet customer demand. It is estimated that inventories could be reduced 10-30%, sales increased up to 2% due to reduced out of stock situations, and costs of monitoring shipping and receiving slashed all along the supply chain. Manufacturers and retailers both see the potential for use of the system to reduce theft of goods. And beyond improved access to goods, consumers should eventually have the benefit of lower prices due to lower costs, faster checkouts, and new information services linked to the identification of products they select. EPC supporters also foresee improved processes for returned goods and warranties, better protection against counterfeited goods and more efficient product recalls.

The potential benefits in the supply chain have led a number of major companies and governmental organizations to begin requiring the use of EPC systems by their

leading suppliers; within the U.S., Wal-Mart and the Department of Defense have taken the lead. Implementation of EPC systems at the pallet and case level has begun, based primarily on the advantages over the present bar code system—including the ability to read all tags within the reader's range (including tags on cases within pallets) rather than requiring line-of-sight access to bar codes, and the ability to read multiple tags at once as opposed to the bar code's one-at-a-time requirement. Standards for a more capable next generation chip have been agreed to and major steps have been taken to ensure compatibility between EPC standards and those of international standards organizations.

While considerable progress has been made in developing and implementing this supply chain oriented system, it is still expensive, complex, and time consuming to develop the necessary infrastructure and re-engineer existing systems to take advantage of new capabilities. To gain the maximum benefit all items will need to be tagged and systems of readers established throughout the supply chain. Even as prices decline, tags are still far more expensive than bar codes and the technology is not mature; improvements in accuracy and reliability are necessary to deal with real world situations where it will be necessary to read tags in the presence of liquids and metals, where there are likely to be collisions between multiple tags being read at the same time, and where multiple readers simultaneously obtain data from the same tag.

Three other applications have also heightened interest in RFID.

Faced with increased concern about the diversion of drugs such as oxycontin from, and the introduction of counterfeit drugs into, the pharmaceutical supply chain, the U.S. Food and Drug Administration is exploring the possibility of utilizing RFID systems for the purposes of tracking and tracing drugs. A number of states have already required new systems to provide the "pedigree" for pharmaceutical products and it possible that the FDA will require RFID labeling for track and trace purposes which would bring RFID systems directly into the pharmacy.

In another major development, financial institutions in the U.S. have begun to issue "contactless" payment cards. Rather than swiping a card's magnetic stripe through a reader, the card is held close to a reader with which it communicates by radio waves. This speeds customers through the check out process. The security measures taken in these systems reflect the sensitivity of the financial information involved. The tags embedded in the contactless cards are more expensive and capable chips allowing for encryption and authentication; the read ranges in the system are much shorter (1-3 inches) than those used in the EPC systems for inventory control.

A last development worth noting is the growth in the use of RFID in identification documents. While a number of private sector employers have utilized RFID enabled identification documents for access control purposes, it was the decision of the U.S. government to issue RFID enabled passports and other RFID enabled identification documents that has increased the focus on policy related issues. Unlike supply chain systems that are designed to track objects, RFID identification documents would potentially be used to track people; unlike commercial uses of RFID which, due to commercial competition provide consumers with some ability to make choices about their use of RFID, governmental uses of RFID technology in identification documents would be mandatory. The initial U.S. RFID passport proposal was severely criticized but a series of changes by the U.S. government has led to substantially improved privacy and security protection.

POLICY ISSUES

Overall, RFID systems are used for four general purposes: 1) to track objects such as the EPC supply chain management system; 2) to track people such as prisoners, hospital patients, or even school children; 3) to provide services such as automated toll-taking systems on highways; and 4) as internal components of other systems such as in car keys where the RFID system is used to authorize the use of the specific key to start a specific car. Systems used for these various purposes differ considerably in, among other things, the cost and sophistication of the components, the levels and sources of power, the communications protocols and the read ranges between tags and readers.

A number of important policy issues have been raised by the increasing, and potentially pervasive deployments of various RFID systems involving, among others, privacy, security, access to radio frequency spectrum, possible health effects, and labor practices. Any sophisticated analysis of the public policy implications of an RFID system will need to look at its specific uses and system characteristics because systems differ as described above and, most importantly, in the sensitivity of the information they generate. The principle characteristic that all systems share is the use of radio frequencies to communicate between tags and readers; these communications may be subject to unauthorized interception and use including the reading of tags by unauthorized readers.

Privacy. RFID technology raises privacy concerns when its use enables parties to obtain information about particular individuals that they otherwise would be unable or unauthorized to access. Privacy issues are greatest when information generated by the RFID system is linked with personally identifiable information (PII), such as linking an individual's PII with the purchase of a tagged item. In the retail context, for example, this issue is largely the same as that raised by the linking of customer purchases with PII through the use of payment cards or customer loyalty cards; the principal difference is that EPC data would allow PII to be linked to the purchase of a particular item (this can of soda as opposed to a can of this soda.) In dealing with these issues, companies can draw upon the policies they have adopted regarding the use of loyalty card and payment card data. It should be noted that the linking of PII with data collected through such systems is governed in Europe by the European Commission's Privacy Directive requiring notice of the collection, consumer choice about whether it will be allowed, and rules governing retention, protection, and access to the linked information. Rules in various countries differ and companies will have to decide whether to adopt the strictest rules and follow one set of policies and practices globally or follow different rules in different countries.

The second major privacy issue is the potential use of RFID systems for the purpose of tracking or targeting individuals. Many devices such as cell phones, GPS receivers, even credit cards now generate location data; if RFID tags can be associated with an individual could they similarly provide data useful for tracking or targeting or developing a detailed profile of that individual? Would it be possible to learn that an individual, whose identity may even be unknown, is carrying a product that he or she does not want others to know about—a controversial product or a product which the bearer might not want to divulge?

The tracking and targeting issues have already been raised by critics and depend on the RFID tags being readable, for example, after a customer purchases a tagged item and leaves the retail establishment. Consumers, if they have notice that a tag is present, could choose not to purchase the item, or could discard or destroy the tag (in most cases the tag will be on the packaging). The EPC standards even provide for a "kill" command that would allow for the deactivation of the tag although there are technical and operational issues that must be resolved if this is to be cost effective.. Technical research is continuing on other means to address the tracking and targeting issues including the use of blocker tags to prevent unauthorized reading, encrypting the tags or providing randomized data if the tag is read, requiring some form of authorization to read the tag, shortening the antenna to reduce the read range, or ultimately allowing the tags to be turned on or off. Such means however are likely to raise the costs of the tags. Moreover, some of the most interesting potential benefits of pervasive tagging, from consumer-oriented uses such as the facilitation of returns and warranties, to societally desirable uses such as reducing counterfeited goods, increasing the efficiency of recycling by allowing for automatic sorting of recyclable goods, tracking toxic materials, or facilitating home health care monitoring of the elderly depend on the tags remaining readable.

The tracking and targeting issues are certainly present in the case of government issued identity documents with embedded RFID tags. Because their use is mandatory nature and because they are likely to include PII, government issuers should engage in the most careful planning and execution. It is not surprising that legislative activity at the state level in the U.S. is increasingly targeted at RFID systems in this area.

Security. There are a number of different aspects of security with respect to RFID systems. Unauthorized users must not be able to obtain sensitive information or to track individuals either from interception of the radio communications between tags and readers, through unauthorized reading of the tags, or via unauthorized access to the network or the database. In addition, the tags must be secure in that they can not be easily killed or changed without authorization, spoofed or counterfeited; the data generated and stored must also be protected from unauthorized amendment.

Individuals are not the only parties interested in the security of the RFID systems and control over access to information. If manufacturers, distributors, and retailers, for example, are to rely on the EPC system to enable them to operate a global supply chain management system, they must be able to rely on the system's integrity. Moreover competing manufacturers, distributors, and retailers won't be satisfied unless they can be sure that their competitors do not have access to information about their practices and processes that is competitively important. Even those parties that are not direct competitors are sensitive to this issue; a manufacturer would not want different retailers that are its customers to be able to use EPC data to track the manufacturer's activities with a competing retailer.

The security issues, other than those related to the radio transmissions between the tags and the readers and the unauthorized reading of tags, are the same as for any other networked database systems. Recently the Federal Trade Commission has begun to hold companies liable for failure to provide information security appropriate to the amount and sensitivity of the information they have accumulated and stored. In an environment marked by major instances of data leakage and increasing legislative activity at the state level regarding information security, it will be

important for companies to address foreseeable risks to the security, confidentiality, and integrity of personal information that they gather. Minimization of the information stored on the tag would help reduce security risks from the unauthorized interception of tag to reader transmissions and unauthorized tag reading.

In conclusion, security is a sensitive issue especially with reference to some critical applications such as electronic contactless payment or identification documents.

Radio Frequency Spectrum. There are several related policy issues involving access to spectrum.

Presently, RFID operates in unlicensed bands which provide considerable flexibility but which inhibit the creation of protocols within the band to reduce tag and reader collisions.

If the use of RFID systems expands as predicted it is possible that additional spectrum will be needed to prevent undesirable levels of interference within the frequency bands that are utilized.

At the present time, different frequency bands are used in different geographic regions for RFID; if [b1] RFID systems such as the global EPC system are to work seamlessly in a world of global commerce, it will be important that the same bands be used or that the bands be located close enough together with compatible operational rules so that there are no problems with interoperability or that system costs are not raised unduly.

Health effects. The EPC standards and others governing RFID systems, including their limits on emissions, are in conformance with present standards on exposure to radio frequency energy. The controversy over the health effects of RF exposure to cell phones, however valid or invalid, suggests that there is a considerable concern in the general public about these issues that should be addressed in connection with pervasive EPC deployment, or intensive use of RFID stand alone or networked systems in a particular environment.

Labor practices. In many countries local or regional laws govern labor practices. In certain European countries, for example, the introduction of a technology capable of measuring labor productivity is a legally required subject of negotiation between labor and management. Companies that utilize EPC systems will need to examine the impact of local labor and contract law on their deployment.

Recommendations

It would be highly desirable for RFID systems to operate under a single set of rules governing the collection, retention, protection, and utilization of information involving the linkage of personally identifiable information and information generated by the use of RFID. A great deal of work has been done in this area involving the development of best practices which should inform the development of company policies in this area, including the OECD's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. To that end the following set of principles should apply:

- Individuals should be given notice that RFID technology is being employed in a commercial or public environment. Products or packaging bearing tags should be identified by the use of a recognizable logo or identifier on the product or packaging. A guiding principle is that there should be no hidden tags.
- Customers should be given, and informed of, their choice to remove and/or discard, destroy, or deactivate RFID tags from the products that they have purchased.
- The public should be able to obtain accurate information about RFID systems and their applications. In order to create a more informed environment for the deployment of RFID systems, companies and government should engage in consumer education about RFID; in particular, companies should provide consumers with information about post sale applications of RFID so that consumers can make informed choices about discarding, destroying, or deactivating the tags.
- Companies should disclose their policies regarding any linkage between personally identifiable information and information generated by the use of RFID. Such policies should provide for consumer choice about collection of such information and should cover issues of minimization of collection, as well as retention, protection, and access to such information.
- Companies should implement measures to address privacy, security, and access to information issues as they design new RFID applications. Making privacy and security part of the design process is much preferable to having to retrofit RFID systems.
- Companies should establish and maintain information security appropriate to the amount and sensitivity of the information stored on their systems. Such a security program should be designed to address foreseeable risks to the security, confidentiality, and integrity of personal information, and addresses those risks.
- Companies should continue to support the development of technical means that will offer a greater range of choices for customers regarding RFID systems.
- Companies should take steps consistent with the sensitivity of the information to protect the radio transmissions between radios and tags from unauthorized interception and use of information and from unauthorized reading of the tags. In furtherance of this objective, companies could minimize the information stored on the tags.
- Cooperation with appropriate rules governing operations will be important to ensure access to sufficient spectrum in appropriate radio frequency bands worldwide. Such cooperation will make it far easier to ensure the efficient worldwide deployment of RFID systems with an optimum use of the radiofrequency spectrum.

Acknowledgement

WITSA acknowledges the substantive contributions of **Elliot E. Maxwell** in the preparations of this briefing paper on RFIDs. He is a Fellow of the Center for the Study of American Government at Johns Hopkins University, Distinguished Research Fellow at the eBusiness Research Center of the Pennsylvania State University, and chair of the International Policy Advisory Council of MIT's Auto-ID Center.

The World Information Technology and Services Alliance (WITSA)

Algeria	Algerian Information Technology Association (AITA); msaidi17@gmail.com
Argentina	Cámara de Empresas de Software y Servicios Informáticos (CESSI) URL: http://www.cessi.org.ar/ E-mail: camara@cessi.org.ar
Armenia	Armenian Union of Information Technology Enterprises (UITE) URL: http://www.uite.org/ E-mail: uite@arminco.com
Australia	Australian Information Industry Association (AIIA) URL: http://www.aiia.com.au/ E-mail: aiia@aiia.com.au
Bangladesh	Bangladesh Computer Samity (BCS) URL: http://www.bcs-bd.org/ E-mail: samity@dhaka.agni.com
Benin	AP.TIC Benin – The Professionals of Information and Communication Technology Association URL: http://www.apticbenin.org E-mail: contact@apticbenin.org
Bermuda	Business Technology Division of the Bermuda Chamber of Commerce URL: http://www.bermudacommerce.com/divisions/business-technology.html ; info@bcc.bm
Bulgaria	Bulgarian Association of Information Technologies (BAIT) URL: http://www.bait.bg/ E-mail: bait@spnet.net
Canada	Information Technology Association of Canada (ITAC) URL: http://www.itac.ca/ E-mail: info@itac.ca
Chinese Taipei	Information Service Industry Association of Chinese Taipei (CISA) URL: http://www.cisanet.org.tw/ E-mail: cisa@mail.cisanet.org.tw
Colombia	Colombian Software Industry Federation (FEDESOFIT) URL: www.fedesoft.org E-mail: proyectos@cati.org.co
Costa Rica	Costa Rican Chamber of Information and Communication Technologies (Camtic) URL: http://www.camtic.org/ E-mail: fcartin@camtic.org
Ecuador	Association Ecuatoriana de Tecnología de Información y Servicios (AETIS) URL: http://www.aetis.org.ec E-mail: aetis@usa.net
Egypt	Egyptian Information Technology, Electronics and Software Alliance (EITESAL) URL: http://www.eitesal.org E-mail: moh.fouad@eitesal.com
Finland	Federation of the Finnish Information Industries (TIETOALAT) URL: http://www.finnishinformationindustries.net E-mail: info@tietoalojenliitto.fi
France	Syntec Informatique URL: http://www.syntec-informatique.fr/ E-mail: ljego@syntec-informatique.fr
Greece	Federation of Hellenic Information Technology and Communications Enterprises (SEPE) URL: http://www.sepe.gr/ E-mail: sepe@compulink.gr
Guatemala	Software Commission of Guatemala (SOFEX)

Hong Kong	Hong Kong Information Technology Federation (HKITF) URL: http://www.hkitf.org.hk/ E-mail: mok@hknet.com
Hungary	Hungarian Association of IT Companies (IVSZ) URL: http://www.ivsz.net/ E-mail: szekfu@ivsz.hu
India	National Association of Software and Service Companies (NASSCOM) URL: http://www.nasscom.org/ E-mail: nasscom@nasscom.org
Indonesia	ASPILUKI - Indonesian Telematic Software Association URL: http://www.aspiluki.or.id/ E-mail: g_rianto@link.net.id
Israel	Israeli Association of Software Houses (IASH) URL: http://www.iash.org.il/ E-mail: software@industry.org.il
Japan	Japan Information Technology Services Industry Association (JISA) URL: http://www.jisa.or.jp/ E-mail: info@jisa.or.jp
Jordan	Information Technology Association - Jordan (int@j) URL: http://www.intaj.net/ E-mail: info@intaj.net
Kenya	Computer Society of Kenya (CSK) URL: http://www.cskonline.org/ ; E-mail: csk@nbi.ispkenya.com
Laos	Lao ICT Commerce Association (LICA)
Lebanon	Professional Computer Association of Lebanon (PCA) URL: http://www.pca.org.lb/ E-mail: Info@pca.org.lb
Lithuania	Association of the information technology, telecommunications and office equipment companies of Lithuania (INFOBALT) http://www.infobalt.lt/ E-mail: office@infobalt.lt
Malaysia	Association of the Computer And Multimedia Industry Malaysia (PIKOM) URL: http://www.pikom.org.my E-mail: info@pikom.org.my
Mexico	Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) URL: http://www.amiti.org.mx/ E-mail: amiti@amiti.org.mx
Mongolia	Mongolian National Information Technology Association; badarch@magicnet.mn
Morocco	l'Association des Professionnels des Technologies de l'Information (APEBI); http://www.apebi.org.ma/ E-mail: apebi@apebi.org.ma
Nepal	Computer Association of Nepal (CAN) http://www.can.org.np/ info@can.mos.com.np
Netherlands	ICT~Office URL: http://www.ictoffice.nl/ E-mail: info@ictoffice.nl
Netherlands Antilles	Curacao Information & Communication Association (CICA) URL: http://www.cica.an/ ; E-mail: info@cica.an
New Zealand	Information Technology Association of New Zealand (ITANZ) URL: http://www.itanz.org.nz/ E-mail: info@itanz.org.nz
Norway	ICT Norway (IKT Norge) / http://www.ikt-norge.no/ E-mail: bt@ikt-norge.no
Palestine	Palestinian IT Association (PITA) URL: http://www.pita-palestine.org/ E-mail: info@pita-palestine.org

Panama	Asociación Panameña de Software (APS) http://www.aps.org.pa/ / aps@arango.com
Philippines	Information Technology Association of the Philippines (ITAP) URL: http://www.itaphil.org/ E-mail: cvparlade@pablaw.com.ph
Poland	Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji - PIIT) / http://www.piit.org.pl/ Email: biuro@piit.org.pl
Republic of Korea	Federation of Korean Information Industries (FKII) URL: http://www.fkii.or.kr/ E-mail: grant@fkii.org
Republic of Macedonia	Macedonian Association of Information Technology (MASIT) URL: http://www.masit.org.mk E-mail: contact@masit.org.mk
Romania	Association for Information Technology and Communications of Romania (ATIC) URL: http://www.atic.org.ro E-mail: atic@softnet.ro
Russia	Russian Information & Computer Technologies Industry Association (APKIT) URL: http://www.apkit.ru/ E-mail: info@apkit.ru
Rwanda	Rwanda ICT Association (RICTA); arugege@artel.rw
Senegal	Senegalese Information Technology Association (SIT' SA) www.sitsa.sn / sitsa@sitsa.sn
Singapore	Singapore infocomm Technology Federation (SiTF) http://www.sitf.org.sg/ / sitf@sitf.org.sg
South Africa	Information Industry South Africa (IISA) URL: http://www.informationindustry.org.za/ info@informationindustry.org.za
Spain	Spanish Association of Electronics, Information Technology and Telecommunications Companies (AETIC) URL: http://www.aetic.es/ E-mail: aetic@aetic.es
Sri Lanka	Sri Lanka Information and Communications Technology Association (SLICTA) E-mail: sg@searcc.org ; http://www.slicta.lk/
Syria	Syrian Computer Society (SCS) URL: www.scs.org.sy , E-mail: sec@scs-net.org
Tanzania	Tanzania Information and Communication Technologies Association (TICTA)
Thailand	The Association of Thai Computer Industry (ATCI) URL: http://www.atci.or.th/ E-mail: Info@ATCI.or.th
Trinidad & Tobago	The Information Technology Professional Society of Trinidad and Tobago (ITPS); URL: http://www.itps.org/ ; E-mail: itps@itps.org
Tunisia	Tunisian IT Chamber (National Chamber of Information Technology Engineering and Services Companies – CNS-SSII); URL: http://www.ssii.org.tn/ ; E-mail: info@ssii.org.tn
Turkey	Turkish IT Services Association (TUBISAD) URL: http://www.tubisad.org.tr E-mail: tubisad@tubisad.org.tr
Uganda	The Private-Sector ICT Association of Uganda (PICTA) URL: http://www.picta.or.ug/ E-mail: info@picta.or.ug

Ukraine	Association "Information Technologies of Ukraine" (IT Ukraine); URL: http://www.itukraine.org ; E-mail: alex@itukraine.org.ua
United Kingdom	The Information Technology, Telecommunications and Electronics Association (Intellect) URL: http://www.intellectuk.org E-mail: info@intellectuk.org
United States	Information Technology Association of America (ITAA) URL: http://www.ita.org/ E-mail: jmcwilliams@ita.org
Uruguay	Uruguayan Chamber of Information Technology (CUTI) URL: http://www.cuti.org.uy/ E-mail: info@cuti.org.uy
Venezuela	CAVEDATOS - Venezuelan Chamber of IT Companies URL: http://www.cavedatos.org.ve/ E-mail: cavedato@telcel.net.ve
Vietnam	VINASA - Vietnam Software Association URL: http://www.vinasa.org.vn/ E-mail: office@vinasa.org
Zimbabwe	Computer Suppliers' Association of Zimbabwe (COMSA) http://www.comsa.org.zw/ / comsa@csz.icon.co.zw