THE SUN, THE WORLD, AND RFID

Valerie Sinclair

THE TECHNOLOGY BEHIND E-PASSPORTS PROMISES TO DRAMATICALLY STREAMLINE THE GLOBAL MOVEMENT OF GOODS AND PEOPLE.

BY EMILY SOPENSKY

Perhaps it is an exaggeration to say that radio frequency identification is a broad, all-encompassing technology that has the capacity for influencing our daily lives around the word, much as the sun does now. But it is only a slight overstatement.

First used in World War II to identify airplanes, RFID has quietly expanded over the past 60 years to several important applications we now take for granted, such as remote keyless entry to our cars. Last year, it was spiced up and moved to the front burner when two giants in the logistics industry — the U.S. Department of Defense and Wal-Mart — mandated its use in their operations.

Today RFID tags are already used to speed transactions at the point of sale, track livestock and pets, increase highway throughput, label shipping containers and gain entrance to buildings, to name just a few applications. Pharmaceutical companies are beginning to adopt the technology to prevent counterfeiting of drugs. With the introduction of biometric passports, the State Department, too, is beginning to use RFID.

Understanding how the technology works is important to Foreign Service officers as well as to the general public (see "How It Works," p. 32). Adoption and implementation of the new e-passports, or "electronic passports," though important in its own right, presage debates and projects to come, where technology breakthroughs will both challenge and facilitate the delicate balance between individual privacy and state security.

The Biometric Passport

U.S. passports are a valuable commodity to many around the world. Deputy Secretary for Consular Affairs Frank Moss testified on June 22 that 8.8 million applications were processed in the last fiscal year — up 22 percent from the year before. He stated that his office expects 10 million to be processed by the end of FY 2005.

To provide enhanced security in the post-9/11 era, the U.S. passport has been undergoing changes. To prevent fraud, new artwork is visible only under ultraviolet light. Additionally, this next generation of the U.S. passport includes biometric technology that will further support border security goals.

Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the Department of State issued that passport. The biographic data page, which includes the bearer's digitized photo, has been moved to an interior page, and the data is replicated in a contactless chip implanted in the back cover. The data in the integrated circuit is checked by an inspector with an RFID reader. If the data page and the chip data are not the same, the individual bearing the passport is subjected to further ID checks.

Traditionally, facial recognition has been used to differentiate among humans. Other human physiological or behavioral characteristics that scientists and technologists have been studying include the unique pattern of the iris, the retina, ear, voice, gait, palm and finger tip. In the first generation of the e-passport, which Congress ordered to be fully implemented by October 2006, the biometric data is limited to the bearer's photo. It is quite likely that second-generation U.S. e-passports will add iris scans (but not fingerprints, primarily because the iris scans have a higher accuracy rate and require less storage space).

The specifications for the new U.S. e-passports are governed to some extent by the Enhanced Border Security and Visa Entry Reform Act of 2002, which requires border entry documents to be machine-readable "containing biometric identifiers" and to be in compliance with the International Civil Aeronautics Organization standards. ICAO determined in 2002 that facial features, fingerprints and iris recognition are all applicable to machine-readable travel documents. The European-based agency designated facial recognition as the preferred biometric, and characterized the latter two as additional options. ICAO also selected contactless integrated circuits as the best means of implementing the biometrics data standard.

Pilot Testing

Tests began in mid-2005 on the first generation of biometric passports. Partnering with Department of Homeland Security border officials, the State Department conducted a field test with Australia and New Zealand, issuing approximately 250 of the new U.S. passports to a few airline crews (United Airlines, Qantas and Air New Zealand). The test compared the e-passports of all three countries. In January 2006, Singapore plans to test one thousand of its e-passports issued to Singapore Airlines crews at U.S. borders and in Changi Airport. In the next step of the pilot program, beginning in early 2006, diplomatic and government employee passports will receive the chips.

Both the midpoint report during the first phase of the trinational test and the final report at its conclusion found

Emily Sopensky was the 2004 Institute for Electrical and Electronics Engineers-USA Fellow to the U.S. State Department, where she worked with the Office of eDiplomacy in the Bureau of Information Resource Management and with the SMART project. She is a business consultant, specializing in technology.

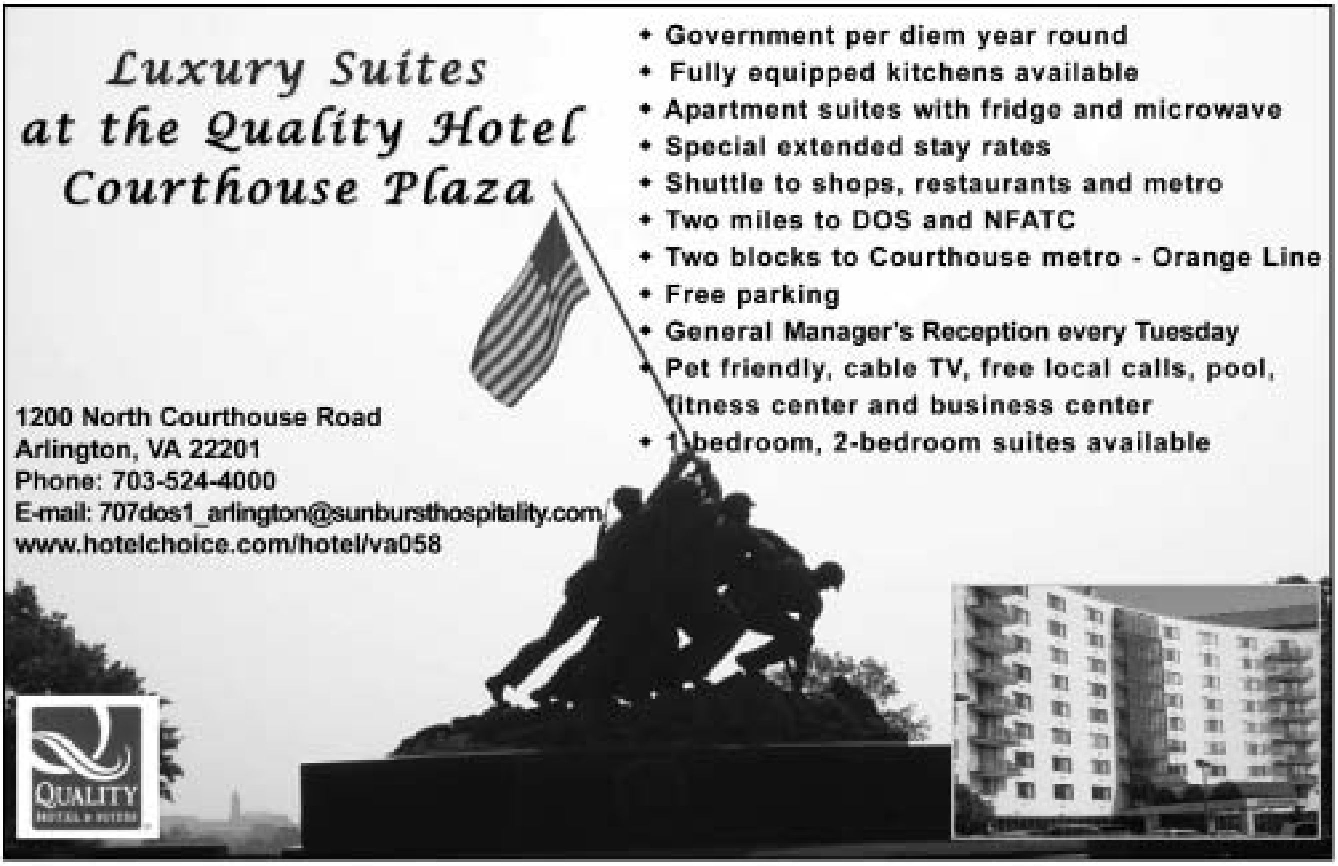
that improvements are needed in the technology, that human factors must be thoroughly analyzed and that focused training must be implemented.

In keeping with requirements adopted by ICAO and directives from the Department of Homeland Security, the new passports are to be issued domestically to all applicants by the end of FY 2006. All 27 nations in the Visa Waiver Program must begin issuing e-passports by Oct. 26, 2006, in order for their citizens to be able to continue to enter the U.S. without first obtaining a visa.

According to final regulations issued by the State Department this past Oct. 25, the chips in the new e-passports will have enough memory to accommodate additional biometric information. Moss says that Consular Affairs is already investigating adding additional biometrics (e.g., iris scans). Among the general parameters specified by ICAO to determine the standard for biometric passports, were the requirements that the technology had to support 32 kilobytes of storage, and that stored data needed to be easily accessible and transmitted quickly.

Because RFID allows data to be collected inconspicuously and at a distance, privacy and security advocates are wary of its use in many applications, including e-passports. In response to such concerns, the State Department's Oct. 25 ruling mandates that the new e-passports be equipped with "anti-skimming" technology. The department is testing the feasibility of sandwiching a metallic mesh within the front cover and spine to prevent RF reads until the e-passport is opened and read at close range by an official. In June 22 congressional testimony, Deputy Secretary Moss made clear that the e-passports would not be rolled out until security issues were fully dealt with: "The bottom line is that we will not issue biometric passports to the general public until we have successfully addressed these concerns."

Although very challenging technological hurdles have already been overcome in the development of the e-passport, there are still a few other issues. Not the least of these is that the technologies incorporated in the new



How It Works

RFID is a generic term for technologies that use radio waves to automatically identify people or objects. Radio frequency identification technology uses the same electromagnetic radiation spectrum that radios use to transmit.

A Brief Primer on the RF Spectrum

To make radio waves, an alternating current is sent to an antenna, creating an electromagnetic field.

The portion of the electromagnetic radiation spectrum used for wireless broadcasting and communications is from nine kilohertz to thousands of gigahertz. Still higher frequencies make infrared, visible light, ultraviolet, X-rays and gamma rays possible.

To see the full-spread spectrum-usage allocation for the U.S., the National Telecommunications and Information Administration (U.S. Department of Commerce) has a nifty chart at http://www.sss-mag.com/pdf/freqchrt.pdf.

Other countries allocate the use of spread spectrum differently. For the ultra-high-frequency RFID tags being used for supply chain applications, the U.S. uses 915 megahertz. Japan prohibits the use of this frequency. Europe prefers 868 MHz. Consequently, the chance of reading these tags from one port to the next is not quite as easy as RFID advocates in the supply chain business would like. This is one reason why RFID is still considered an emerging technology.

China, as with many issues in today's commerce, holds the trump card. With so many products coming from China, RFID tags must be applied that will meet frequency allocation regulations there and elsewhere around the world.

Biometric passports do not encounter this problem as they are subject to standards set by an international organization, the International Civil Aeronautics Organization.

The basic RFID system comprises a transponder, a reader and an antenna. Data are stored in a transponder device called a tag. Current tags, depending on application, can hold up to two kilobits of data. Tags can be read-only or read/write.

A radio frequency signal is transmitted from the reader to a transponder that passes within range of the reader's antenna.

Unlike the ubiquitous bar code or the magnetic strip on a credit card, the RFID tag does not need a clear line of sight in order to be read. Instead, data in the tag is communicated via a radio signal. The signal is stimulated by a reader, which triggers the data in the tag to "ride" the radio wave back to the reader, where the data is captured and authenticated by a backend computer system. This tag is called a "passive" tag as the data is plucked by an external force. By contrast, an "active" tag relies on its own internal battery to supply energy and send the data to the reader. Active tags are more expensive than passive tags. The Department of Defense is planning on incorporating global positioning technology with active transponders to be able to track in real-time where shipping containers of supplies are around the world.

The type of RFID tag helps determine the read range, or how far away the data on the tag can be read. The source of power is another factor. Antenna size, too, is part of this determination, but the size and type of antenna are mostly functions of the operating frequency used.

Frequency range	Frequency type	Read range	Memory	Comments
2.45 GHz	Microwave	2 meters max	Less than 1 kilobit	Silicon technology is in its infancy for this frequency.
300 MHz to 3 GHz (typically **866 to 960 MHz**)	UHF or more Ultra High Frequency	Can be 6 meters	1 kilobit	Sends faster and further than lower frequencies. Spectrum use varies by country. (Europe uses 868 MHz for UHF; the U.S. uses 915 MHz. Japan prohibits the use of UHF spectrum for RFID, but may open the 960MHz portion.)
3 to 30 MHz (usually **13.56 MHz**)	HF High Frequency	1.5 meters at best for high-end readers	256 bits but additional data memory available today	Used for smart cards. Sometimes called "proximity" cards.
30 kHz to 300 kHz	LF Low Frequency	1 meter at best	64 bits to 1,360 bits; larger possible.	Globally available frequency. Low frequency allows tags to be read through watery substances — the only technology that allows for this.

passports do not come cheap. Initial U.S. yearly cost estimates range between $1.6 billion and $2.4 billion.

Further, as the new passports are only in a limited trial, reliability has yet to be proven. And, transmission times have been too long. In the midway report on the trials with Australia, New Zealand and the U.S., the average time to read the chip varied from a low of 1.7 seconds with a New Zealand passport to a high of 6.3 seconds with a U.S. passport.

It remains to be seen whether the planned implementation schedule can be maintained. Given the complex nature of the technology, and the amount of training that will go into a full rollout of the new passports, Congress should be prepared to extend the October 2006 deadline, itself an extension of the original October 2004 deadline.

The Logistics of Globalization

Independently, the U.S. Department of Defense and Wal-Mart, the world's largest retailer, are now requiring their primary suppliers to tag each of their products with RFID tags. It's hard to say no to such behemoths. For many suppliers, no matter how large or small, these mandates will change the way they do business.

Both DoD and Wal-Mart are interested in maintaining a flow of goods and products from and to points around the globe. For Wal-Mart and other corporations invested in assembling and moving goods globally, being able to guarantee genuine parts manufactured in China, assembled in Japan, shipped through Europe, and distributed in the United States adds value to the finished product. Being able to track assets throughout the manufacturing and distribution process — the supply chain — is also a counterbalance to counterfeit and theft. At the beginning of 2005, Wal-Mart started holding trials with its top suppliers.

The key to why RFID is so seductive to those in the business of moving products around the world is the fact that digital data remains in its native digital format. Once encoded into the tag, identifying information such as serial number, manufacturer's code and product line is

transferred electronically. Having to manually re-enter the data upon shipping, on the manifest and bill of lading, at the customs house, in the retailer's warehouse, in the stockroom and at the checkout can be eliminated in a complete end-to-end distribution system supported by an RFID infrastructure.

A GLOBAL IMPACT: OTHER APPLICATIONS

Airline baggage. Some airlines, like British Airways, have been studying the use of RFID in baggage tagging, hoping to decrease operational costs. Misdirected or lost baggage can cost as much as $200 per bag on average, some analysts estimate. In 2004, the International Air Transport Association conducted a pilot study of RFID technology. They concluded that: 1) RFID must be concurrently integrated with bar-code technology; 2) only a systemic, integrated approach will be successful in the long run; and 3) tag costs are still too high. Eventually though, U.S. domestic airlines may be forced to adopt RFID luggage tracking for security reasons.

Shipping containers. Shipping is another area where RFID tagging has a future. Some analysts estimate that of the 18-20 million shipping containers moving around the world on any given day, less than 400,000 are ever inspected. To address this, containers that range in length from 20 to 45 feet are being retrofitted with external seals that include RFID technology. Sophisticated harbors, like Singapore, are already equipped to handle RFID-tagged containers.

Livestock. One longtime practical and successful application of RFID tagging has been to identify and track livestock. By encoding the type of breed, diet and breeder's information into a tag implanted under the skin of a pig, for example, the entire hog industry has much more control over its market and consumers benefit from increased quality control.

Already used to track valuable migratory wildlife and fish whose geographical boundaries rarely respect political boundaries, RFID tagging could also be used as a tool to aid in containing dangerous, life-threatening contagions and viruses that jump from livestock to humans, such as avian influenza, SARS and mad cow disease.

Airplane parts. The U.S. Federal Aviation Administration recently decided to authorize using RFID tagging on airplane parts. Once the supporting system is in place, airplane manufacturers and airlines can incorporate into routine maintenance practices a scan of the airplane's parts. The tags will store data on each part's age and service record, for example, thereby expediting maintenance and improving overall quality control.

Pharmaceuticals. The Food and Drug Administration expects that counterfeiting drugs will be "extremely difficult or unprofitable" with reliable RFID in place. By the end of 2005, one of the first pharmaceutical companies to ship with RFID tagging to thwart counterfeiting is Pfizer. The drug giant is expected to begin shipping packages of Viagra, one of the most counterfeited drugs, with RFID chips.

In addition, each item can have its own unique identifier, thereby permitting each item to be tracked and traced. Tracking product usage, returns and even recalls gives nearly complete control over product distribution and development, making the detection of counterfeiting and thefts much easier and quicker.

But, as with any technology that is mouthwatering to some, the issues surrounding its development and application warrant a clear-eyed look.

Disruptive, Discordant Technology

The infrastructure to support RFID technology is not yet in place globally. Issues range from interoperability of systems to the lack of globally recognized standards, testing and reliability. Four challenges, however, stand out.

First, the real-time nature of RFID data creates concerns for privacy and security experts. Eliminating paperwork and removing the human element may speed goods through the supply chain, but those advances also threaten traditional laws, regulations and procedures established to maintain the flow of goods and people across borders. The biggest challenges of RFID arise from the proliferation of data, the sharing of the data and databases, and from the possibility of snooping via radio.

With few standards or common patterns of behavior yet established on a global basis, RFID watchdogs suggest that the following information practices must be accepted in order for the technology to thrive:

- Users must be provided notice that the technology is in use with the intent of collecting personal data limited to the purposes for which it is collected.
- Collected data is accurate, complete and timely.
- Personal data are protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.
- Users can view all information collected about them.
- Compliance with these guidelines is mandated and a system is maintained to implement compliance.

Second, there are no laws yet to provide warranty protection on systems, readers and antenna RFID products.

There is little recourse for malfunctioning RFID equipment.

Third, and equally important, is the fact that there is no certification or registry recognizing approved system integrators, RFID consultants and trainers. Some companies do train on their own equipment, but a vendor-neutral solution to certifying providers is not yet available. Especially because RFID technology is remotely readable, invisible and capturing data in real time, trust that the data are being captured and transmitted safely and securely is essential for its spread.

Finally, there is the challenge of misinformation and confusion about RFID that is more pervasive than the technology's advocates want to believe. Education is key to defusing misinformation. RFID is a generic technology with many possible applications, each of which has its own benefits and limitations. Currently, however, each industry using RFID has mounted its own informational campaign, and the resulting consumer confusion is echoed in the press, thus confounding any inherent misunderstandings about the technology. Establishment of recognized, certified courses in its fundamentals is still a work in progress.

Acceptance of any disruptive technology — and RFID is one — takes time. We take bar-code technology for granted now, but it took at least 20 years for it to be incorporated as a mainstay of commerce. RFID technology presents a similar challenge to the way we live and work around the world.

Thanks to G. Matthew Ezovski, a senior engineering student at Rensselaer Polytechnic Institute in Troy, N.Y., and a 2005 Washington Internships for Students of Engineering (WISE) intern, whose paper summarizing the e-passport policy, "Biometric Passports: Policy for International and Domestic Deployment" (Journal of Engineering and Public Policy, *Vol. 9, 2005), was helpful in preparing this article. It is available at http://www.wiseintern.org.* ■