



December 2009

Uses of RFID Technology in U.S. Identification Documents

Project Leads

Monica Nogueira, PhD, University of North Carolina at Chapel Hill

Noel Greis, PhD, University of North Carolina at Chapel Hill

Statement of Problem

The investigations following the attacks of September 11, 2001, showed that our ability to verify a person's identity is crucial to our national security. As pointed out by *The 9/11 Commission Report* (National Commission on Terrorists Attacks Upon the United States, 2004), travel documents are as important as weapons for terrorists. To carry out an attack on American soil, foreign terrorists must cross our borders—which requires passing an identification screening. A valid passport also allows a terrorist to obtain other valid documents (e.g., driver's license, credit cards, health insurance card) that are important to performing normal life activities while maintaining a low profile and avoiding detection.

Four projects, currently in different stages of implementation, use Radio Frequency Identification (RFID) or Machine-Readable Zones (MRZ) technologies for verification and validation of identity in the United States. These programs are (1) e-Passport, (2) PASS Card, (3) Real ID, and (4) Enhanced Driver's License. The use of RFID enables data to be stored electronically in chips embedded in identification documents and shared quickly in digital format by law enforcement personnel. Documents with RFID chips and a secure networking environment to exchange data are deemed more secure and less prone to counterfeiting than conventional, non-electronic documents. However, there is still debate about how to best

balance the security benefits from RFID-enabled identification documents with concerns about privacy.

Background

In response to potential security threats after 9/11, the U.S. Congress passed the Enhanced Border Security and Visa Entry Reform Act of 2002, establishing new requirements for visa operations in the United States that allow travelers from the 27 countries then participating in the Visa Waiver Program (VWP)¹ to enter the United States for business or pleasure for up to 90 days without attaining a visa—provided they have a machine-readable passport that uses biometric identifiers (U.S. Department of State, n.d., *Enhanced border security*). This act is considered one of the major factors that spurred the adoption of RFID chips for national identification in the United States and worldwide.

The international standards for travel documents with MRZ and RFID that are used by most countries have been developed by the International Civil Aviation Organization (ICAO), an international organization run by the United Nations. Electronic documents that feature machine-readable zones can be read by physical contact with optical scanners. The U.S. Department of State (DoS) has been issuing machine-readable passports since 1981. Machine-readable passports contain two lines of 44 characters on the data page with the bearer's name, country, and passport number. The Enhanced Border Security and Visa Entry Reform Act of 2002 set a new standard by establishing interoperability standards, along with integrated entry and exit data systems and requirements for tamper-resistant, machine-readable documents that contain ICAO-compliant biometric identifiers such as a digital photograph.

The recent addition of RFID chips to machine-readable documents balances the need for electronic data storage on the e-document with automated document control, since the RFID chip can be quickly read from a distance (i.e., “contactless”) rather than by contact with an optical scanner. RFID chips and contactless smart cards use radio frequencies for communicating data over the distance between the chip and reader. Both contact-based and contactless smart cards contain a small microprocessor that provides more memory and stronger security capacities, while (passive) RFID tags typically contain a chip with less memory and limited functionality. For the purposes of this brief, we do not distinguish between RFID-enabled cards and contactless smart cards.

¹ Today, VWP serves 35 countries.

American E-Document Programs

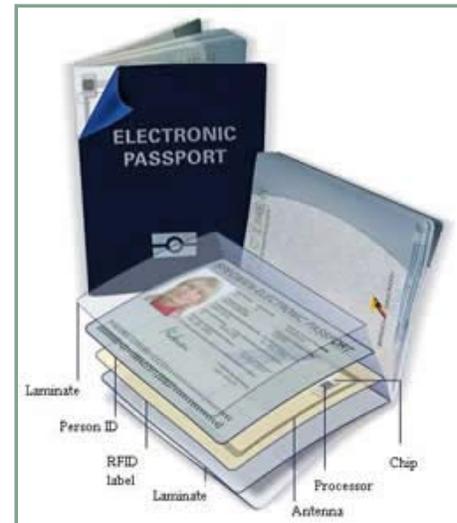
e-Passport. Following 9/11, the United States accelerated plans for the adoption of a new electronic passport standard that would increase the security of travel documents and protect against unauthorized entry by terrorists (U.S. Department of State, n.d., The U.S. electronic passport). Shortly thereafter, in May 2003, ICAO formulated standards for a new e-Passport with an integrated circuit RFID chip that would securely house personal

identification information about the bearer. The ICAO standard specified that all e-Passports were to contain a digital photo of the traveler, as well as additional identifying biometric data such as fingerprints and iris images. As shown in Figure 1, the same data elements from the front page of the passport are stored on a chip embedded in the back cover of the passport. U.S. legislators have adopted the term "biometric passport" to denote a machine readable e-Passport in which a digital photograph has been electronically printed to the data page rather than pasted onto the page. The use of RFID technology to store digital photographs enables biometric comparison through the use of facial recognition technology, which allows for faster and automated identity verification at international borders and ports of entry. It is important to note that the data in

e-Passports cannot be changed or amended. Anyone seeking a data alteration must apply for a new e-Passport. The DoS began issuing e-Passports in August 2006. Since August 2007, the U.S. has been issuing only e-Passports, but a previously issued passport can still be used for travel as long as it is valid. The RFID chip is protected by a Faraday cage—a metallic shield that interrupts the transmission of electromagnetic energy or electrostatic discharge across it—to prevent skimming and implements the Basic Access Control (BAC), allowing encryption of transmissions between the passport's radio frequency (RF) chip and the RF reader. The adoption of a Faraday cage limits the reading of the RFID chip data to the times when the bearer physically opens the passport.

PASS Card. In October 2006 the Department of Homeland Security (DHS) expanded the use of RFID to the PASS (People, Access Security Service) System (shown in Figure 2). This system, a joint DoS and DHS initiative, was designed to meet the requirements of the Western Hemisphere Travel Initiative (WHTI) for U.S. citizens entering the United States by land and sea (U.S. Department of Homeland Security and U.S. Department of State, 2008). Devised as a less expensive, smaller, and more convenient alternative to the e-Passport, the new electronic passport card, or PASS Card as it is called, is intended for use by Americans

Figure 1: Parts of the e-Passport



invited comments on how states would incorporate other WHTI-compliant technologies, such as RFID-enabled vicinity technology, in addition to the Real ID PDF417 barcode requirement. The Act mandated that states, prior to issuing or renewing a new ID, must verify the citizenship or immigration status of applicants—including verifying the validity of the Social Security number (SSN) and the authenticity of all submitted source documents. In addition, states would be required to capture and store digital images of the source documents for extended periods of time—7 years for paper copies or 10 years for digital images. The Act mandated the creation of state databases to be accessible to all other states, in effect creating a network of national identification databases. It also mandated the use of the Systematic Alien Verification for Entitlements (SAVE) system to verify the legal presence status of any foreigners applying for a U.S. driver’s license or identification card. Criticized for its high costs, short implementation timeframe, lack of privacy protections, and widespread perception as creating a *de facto* national identification card, the law was greeted with strong opposition (“Controversial Real ID,” 2005; Garson, 2006; Rotenberg, 2006; “Real ID deadline”, 2007; National Veterans Committee on Constitutional Affairs, 2007). A coalition of at least 38 states was formed to informally oppose it (Ferguson, 2007)—a reaction that probably accelerated the approval of The REAL ID Repeal and Identification Security Enhancement Act of 2007 (U.S. Congress, 2007) and reversion to an earlier set of minimum standards.⁴ Subsequently, a majority of states took steps to comply with these new minimum requirements to verify source documentation—but not to coordinate with other states in a national identification database system. In May 2008, DHS extended the deadline to replace all licenses used for official purposes with REAL ID-compliant cards; the new deadline is December 1, 2014, for people born after December 1, 1964, and to December 1, 2017, for those born on or before December 1, 1964. At present, no REAL ID card has been issued in the United States.

Enhanced Driver’s License. While individual states search for a solution that fulfills the REAL ID requirements, some border states have created an alternative card—the Enhanced Drivers License (EDL), shown in Figure 4—that is cost-effective and convenient and meets driving and border-crossing needs. Four border states (Michigan, New York, Vermont, and Washington) have adopted standards shared by the REAL ID program and have already started issuing EDLs. Others (Arizona, California, and Texas) are considering this alternative. In addition to serving as a permit to drive, EDLs (like PASS Cards) can be used by American citizens, in lieu of a passport, to travel by land and sea between the U.S. and Canada, Mexico, and some countries in the Caribbean. DHS has also worked with Canadian officials to implement EDLs as an alternative to Canadian passports. Currently, four Canadian provinces (British Columbia, Manitoba, Ontario, and Quebec) issue EDLs to Canadian citizens, who can

⁴ The Repeal Act of 2007 repealed Title II of the Real ID Act of 2005 to earlier minimum standards set by Section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004 (U.S. Congress, 2004). On January 11, 2008, DHS published Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule with final regulations for implementing REAL ID (U.S. Department of Homeland Security, 2008a).

use this document to enter the United States when traveling from Canada, Mexico, or the Caribbean by land or sea. Although the REAL ID and EDL programs are both intended to strengthen identification verification capability, EDLs are not a substitute for the REAL ID. REAL IDs will provide proof of legal status in the United States for both citizens and legal aliens, while only U.S. citizens can obtain an EDL (U.S. Customs and Border Protection, 2009). Similarly to the PASS Card, EDL cards contain an RFID chip that stores non-encrypted information and includes a protective sleeve to protect against unauthorized data transmission when in use.

Figure 4: Enhanced Drivers License



RFID Technology in U.S.

E-Documents

As shown in Table 1, significant technical differences distinguish the four U.S. e-documents. The e-Passport uses “proximity” technology that limits the RFID reading range to a few feet. The embedded data include the same information typed on the passport data page, plus a digital photograph of the passport bearer, a unique chip identification number, and a digital signature to prevent its alteration or removal from the RFID. To prevent unauthorized reading, the card’s data are protected by a metallic layer that blocks transmissions when the e-Passport is closed. Data transmissions between the e-Passport’s chip and the RFID reader are encrypted and can occur only when the e-Passport is open. The e-Passport RFID readers are shielded to minimize eavesdropping.

The PASS Cards carry a “vicinity” RFID chip, which has a much larger reading range of 20 to 30 feet. This allows RFID readers to identify cardholders while they stand in line, or in their cars, waiting to talk to the border inspector at a checkpoint. The RFID chip stores no personal information, but only a unique identification number that is read by an RFID reader and linked to a secure database for use by the border inspector in processing the individual’s entry into the country. The identification number is transmitted without encryption. A protective sleeve for the card shields the chip from being read when the card is not in use. This protective measure is considered less effective than the e-Passport built-in metallic cage because it is highly dependent on adequate use of the sleeve. While an e-Passport’s data are protected once the passport is closed, a card protective sleeve can be lost, or its owner may forget to use it, rendering any data stored in the card vulnerable to skimming and tracking. The e-Passport and PASS Card use different, incompatible RFID standards that require different reader technologies.

Unlike the e-Passport and Pass Card, the REAL ID mandates the use of a contact-based card and does not require the use of RFID technology, but there is no impediment in the law to its use (U.S. Department of Homeland Security, 2009). Instead, a two-dimensional contact barcode, or MRZ, stores a minimum of 10 defined data elements, but there are no requirement for encryption or limitations on the number of data elements (U.S. Department of Homeland Security, 2008a). The mandated MRZ standard utilizes PDF417 barcode, which in theory presents no limitations on the amount of data it can encode; PDF417 “symbols” can be linked together to encode large amounts of data, including fingerprints and other images. The REAL ID allows biometrics, an addition that raises security risks. If a REAL ID containing biometric data is lost or stolen, the lack of encryption allows data to be easily transferred to a blank card and used to impersonate an individual when direct digital comparison between the cardholder and the Real ID is not possible.

Table 1. Technology of U.S. E-Documents

FEATURES	E-PASSPORT	PASS CARD	REAL ID	EDL/EID
Technology	Proximity RFID (passive chip)	Vicinity RFID (active chip)	Two-dimensional Machine-Readable Zone (MRZ)—not international travel standard	<ul style="list-style-type: none"> • Vicinity RFID (active chip) • Two-dimensional MRZ • International travel standard
RFID frequency	13 MHz (ISO14443 A- and B-compliant and ICAO-compliant)	918 MHz (UHF EPC Gen 2)	N/A	UHF EPC Gen 2
Reading range	Approximately 3 feet	Approximately 20 to 30 feet	Contact	Approximately 20 to 30 feet
RFID physical protection	Metallic shield (Faraday cage)	Identity stronghold secure sleeve	N/A	Protective sleeve
Data elements stored in card	<ul style="list-style-type: none"> • name • date of birth • gender • place of birth • issue date • expiration date • passport number • digital photograph • unique chip ID number • digital signature 	Unique identification number	<ul style="list-style-type: none"> • expiration date • holder's legal name • issue or transaction date • date of birth • gender • address • unique ID number • revision date • inventory control number of physical document • state/territory of issuance 	Unique identification number
Biometrics allowed	Yes	No	Yes	Yes
Data encryption	Data transmitted using Basic Access Control protocol	No	No	No
States issuing document	National	National	None	<ul style="list-style-type: none"> • Michigan • New York • Vermont • Washington

Note: EDL = Electronic Driver's License. EID = Electronic IDentity card. EPC = Electronic Product Code. MRZ = machine readable zone. RFID = Radio Frequency Identification.

Similar to the PASS Card, EDLs have a “vicinity” RFID chip that can be read from 30 feet away. The chip stores a unique, unencrypted identifier number that is used to access the traveler’s data in a secure, remote database. EDLs also include a machine-readable zone or a contact bar code that is ICAO-compliant. However, the MRZ for the EDL and the Real ID are not compatible—the Real ID includes MRZ technology but not the same international travel standard MRZ as the EDL (U.S. Department of Homeland Security, 2009a).

Comparing U.S. and Other International E-Document Programs

While the REAL ID national identification program has yet to be fully implemented here in the United States, national Electronic IDentity cards (EID) are a reality in many countries (e.g., Hong Kong, Malaysia, Estonia, Finland, Belgium, Portugal, and Spain) (Biometrics review, 2009). The use of these cards is rapidly being expanded to areas beyond national security, such as health care, e-commerce, banking, and library services. For example, besides using their EID for travel within the European Union, Belgian citizens who have access to a smartcard reader and EID software can use their EID card to sign documents electronically or pay taxes online. Belgium plans to progressively replace other cards such as Social Security cards and driver’s licenses beginning in 2012. A summary of the countries currently issuing e-Passports is provided in Table A1. Countries planning to implement e-Documents are shown in Table A2, and countries currently issuing national EIDs are shown in Table A3.

The use of fingerprint biometrics is also growing in Europe (Martin, 2009). In June 2006, the European Commission mandated that all member states must start issuing fingerprints on electronic passports by June 28, 2009. Studies show that identification based on latent fingerprints alone can be erroneous and that the number of such errors is higher than has ever been known (Cole, 2005; Cole, 2006). The fingerprint of an innocent person can be mistakenly matched to a known criminal (what is known as a *false positive*), or a wanted person can escape because of an incorrectly matched fingerprint (a *false negative*). These types of errors occur most frequently when a single fingerprint is matched against a large database of fingerprints, also known as a “one-to-many” identification. A false positive or false negative error rarely occurs when an e-Passport or other ID is presented to verify the identity of a person holding the document, since only a one-to-one verification match is executed at this time. Fingerprints may vary, however, due to skin condition, injuries, and aging. This poses a challenge to be faced, given our aging population. Also, fingerprints’ accuracy and reliability have been linked to people’s race/ethnicity (Swofford, 2005). For example, there is some evidence that it is more difficult to obtain fingerprints from people of Asian descent, especially women, because Asian hands have less-defined ridges (Walford, 2008). Experts claim that the use of fingerprints has proven to be 99.6% accurate and—in combination with facial recognition or iris scanning—is thought to provide a simple yet secure “gold standard” for identification (Ezovski & Watkins, 2007). Given the recognized chances for fingerprinting identification error today and the number of worldwide travelers per year ranging in the

millions, it can be expected that potential identification systems may fail to match the fingerprints of a small percentage of travelers to those stored in their passports. It is not clear what type of identification procedure will be followed in these cases, but it seems probable that customs border officers will use their discretionary power to make a decision based on other information (e.g., whether the passport looks genuine or the person matches the photo, and additional biometric data if available). The use of second-generation electronic passports containing fingerprints or iris biometric data in Europe is supported by a more secure data transmission protocol, called the Extended Access Control (EAC), rather than the Basic Access Control (BAC) protocol used in the United States (Bundesamt für Sicherheit, 2009; Liersch, 2009).⁵ The BAC protocol, which is based on a subset of the MRZ information—the document number, expiration date, and birth date of the holder—allows passive skimming and was proven to be vulnerable to exhaustive search. For example, an online “bruteforce” attack to the BAC protocol can take a few hours during which a reader connects to the chip while guesses on the subset of MRZ information are tested (Vaudenay & Vuagnoux, 2007). Recognized as a much more secure standard, the EAC protocol requires a bilateral agreement between the passport issuing country and the visiting country. The strength of EAC resides in that it provides for both chip authentication (to create a semi-authenticated message channel between chip and reader) and terminal authentication (which verifies the reader authority to access the stored data) (Vaudenay & Vuagnoux, 2007). Among a few reported weaknesses, the EAC protocol inherits some of the BAC problems, since it relies on BAC to derive the initial session key to access least sensitive information such as the passport bearer’s facial biometric (Pasupathinathan, Pieprzyk, & Wang, 2008). European countries have already started to store fingerprints on the RFID chip of their electronic passports. Since November 2007, all German electronic passports have contained two fingerprints, one from each hand, besides the digital photograph of the passport bearer. Currently, the use of biometric data in U.S. e-Passports is restricted to facial recognition technology applied to the digital photograph of the passport bearer, with fingerprints and other biometric information to be added to the RFID chip by 2017. It is important to note that because of the technology’s high false-positive match rates, experts consider facial recognition the least reliable for identification purposes when compared to fingerprints and iris scans (Hadley, 2004). It is known that recognition rates can vary with light exposure and facial expression, but it is not known why the variability of a person’s facial features, in contrast to other members of a population, can also skew results (Phillips, Flynn, Scruggs, Bowyer, & Worek, 2006).

⁵ American e-passports use the Basic Access Control (BAC) protocol to read information stored on the RFID chip. However, BAC has been proven to offer low protection from unauthorized interception (O’Connor, 2007; Zetter, 2006).



Critical Issues: Striking A Balance Between Security And Privacy

Existing standards for electronic storage of personal data and biometric identifiers have sparked debate that adequate safeguards are not in place in the United States to protect the identity and privacy of its citizens (U.S. Department of Homeland Security, 2007; Meingast, King, & Mulligan, 2007). The debate has focused on the following issues:

Contact-Based Versus Contactless Technology. The choice between contact-based technology (e.g., MRZ, where data are read by scanning the document upon physical contact) or contactless technology (e.g., contactless smart cards and RFID-enabled cards, where data are wirelessly read at a distance) is central to the discussion of privacy. Although deemed more secure, in general contact-based MRZs have low storage capacity (in theory the PDF417 encoding method is an exception to this claim) and cannot be reprogrammed. With respect to contactless technology, proximity and vicinity technologies offer different risks. RFID “proximity” technology was selected for the e-Passports because it does not have the disadvantages of MRZ and because the limited reading range offers lower privacy risks while allowing for speedier processing. RFID “vicinity” technology presents higher risks due to its larger reading range, which allows data to be read from a distance without the user’s consent unless otherwise protected. Specific vulnerabilities of contactless technology in e-Passports were addressed by adding a metallic lining to block access to the data when the e-Passport is closed, encrypting the data stored in the RFID chips at all times (including during transmission), and shielding e-Passport RFID readers to protect against eavesdropping. PASS card and REAL ID data are also inaccessible when the cards are inside their protective sleeve.

Data Management Policy. When designing an e-document system, a policy decision must be made whether to (1) store all personal and biometrics data on the chip embedded in the e-document, as with the e-Passport; (2) store it in a centralized database, as with the PASS Card program; or (3) store data in a network of distributed databases, as proposed by the REAL ID Act of 2005. If an e-document with personal data is acquired by a terrorist, there is high risk that the data can be manipulated and the e-document used to cross our borders. Protecting the data on this e-document is crucial not only to national security, but also to an individual’s identity. The consequences for the individual are more contained if the data on the e-document include only a unique identifier and not information that would enable access to other secure individual data (e.g., SSN). On the other hand, creation of a centralized database containing a large number of highly sensitive personal data may lead to misuse, purpose creep, and overconfidence in the correctness of the data. An error introduced into an individual’s data may affect the individual’s ability to perform daily transactions, and errors in documents may be difficult to correct, given that the central database is deemed, by definition, the verified source. Systems integration of several networked databases (e.g., Social Security, DMV) requires additional security layers to protect against access by unauthorized personnel and other misuse, but may provide more security than a single centralized database.

Data Safeguards and Encryption. Critics of the PASS card (“Passport cards,” 2006); “Smart cards lose,” 2008; Albrecht, 2008) point out that it offers fewer protections than the e-Passport, since the data stored in the RFID chip are unencrypted and can be wirelessly read from a distance without user notice, consent, or control. Its supporters counter that the PASS Card is reasonably secure, since RFID chips in the cards do not store any personal information that would entice illegal skimming. Security experts, however, argue that even though the PASS Card contains a single unique identification number, it is possible to reconstruct an individual’s identify. For example, when a unique identifier is read from a line of cars waiting to cross the border, it is possible to determine the specific car from which it originated and to link the unique identification number to the owner of the car using the car license plate—and then potentially to other personal data, for example by searching online for reverse license plate information to find out the car owner’s name and address (eHow, Inc., n.d.; Burbank, 2009). Encrypting data adds an additional layer of security and makes data theft much more difficult. Privacy groups claim that the REAL ID program fails to impose adequate privacy and security safeguards for personal data, since data are stored on standardized and unencrypted MRZ, which can be scanned, skimmed, and stored by readily available scanners and sold for commercial purposes (Center for Democracy and Technology, 2008; Ozer, 2008; American Civil Liberties Union, n.d.). As an alternative to encryption or data safeguards, the REAL ID Act encourages states to enact legislation prohibiting or limiting data capture and storage by non-law-enforcement parties.

Cost and Economic Impact. Security and privacy decisions are confounded with cost considerations (U.S. Department of Homeland Security, 2009b; Calabrese, n.d.). The price of U.S. passports increased after the introduction of e-Passports, which contributed to the creation of the cost-effective PASS Card in border states. Even so, the PASS Card program caused concern about potential negative economic impact on both sides of the border resulting from processing delays and a decline in trade (Whalen, 2009; Russell, 2009; The Impact of Implementation, 2009). A 2007 report published by the Canada-U.S. Fullbright Program cites estimates by the Conference Board of Canada that between 2005 and 2010 Canada’s tourism industry could suffer cumulative losses of \$3.2 billion in revenue, while a decrease of 7.4 million trips by Canadians to the United States, in the same period, could pose a cumulative \$2 billion loss for the American industry (Abelson & Wood, 2007). The REAL ID program was viewed by the states as an unfunded mandate that would impose significant financial burden on their administrations (e.g., implementing the “One Driver, One License” system). Full implementation of the REAL ID program was initially estimated by DHS to cost \$23.8 billion over a 10-year period. Recent legislation by Congress appropriated funds to help states implement the REAL ID. The DHS awarded \$17 million to Mississippi as the lead state to develop and design a verification hub for the REAL ID program.

Jurisdictional Issues. At the heart of the debate over privacy is the issue of who has the ultimate authority and responsibility to control and protect the enormous array of personal

identification data that have been collected about U.S. citizens (Garson, 2006; Cuff, Hansen, & Kang, 2008). Decentralized electronic systems and distributed databases may offer a diffuse target for identify theft and fraud but require the active cooperation of all stakeholders to verify identity and citizenship of individuals across state boundaries as required by various electronic identification programs. On the other hand, national databases do not provide the checks and balances associated with distributed databases, but may provide better overall protection against intrusion by unauthorized persons. The REAL ID and the PASS Card programs were established as voluntary programs but many have suggested that, over time, Americans may need to obtain a REAL ID to be able to access federal buildings and board commercial planes.

It is important to note that protection for the identity and privacy of individuals can be strongly improved by employing a complete Identity Management System that includes a Physical Key Infrastructure (PKI) to authenticate users and control access to the system, encrypting data, and protecting and securing all databases and data transmissions at all times (International Organization for Standardization, 2009).

Future Directions

The four U.S. electronic identification programs have made considerable strides towards addressing the 9/11 Commission Report recommendation that “secure identification should begin in the United States” (National Commission on Terrorist Attacks Upon the United States, 2004). Today, more than 92 million Americans (or 30% of the population) hold a passport or passport card that is WHTI-compliant. However, gaps exist (U.S. Government Accountability Office, 2009), and we identify below three areas that could yield significant improvements in the use of e-documents to protect our citizens. The cooperation and coordination programs suggested are intertwined with many technical issues, such as the development of more secure data transmission protocols, better methods to protect data stored in RFID chips, and studies to measure accuracy of identification using different types of biometrics.

Enhanced Global Cooperation. Increased cooperation with the European Union (EU) and other countries would enhance national security by increasing interoperability and standardization and help speed up the deployment and operation of border inspection systems of e-documents worldwide (Chartier & van den Akker, 2008; “WP1: Review of Standards and Procedures,” 2008; Houdeau, 2009). On September 2008, as part of the deployment of European second-generation e-Passports, the latest round of tests was performed in Prague by 27 EU members to confirm that their e-Passports containing fingerprint biometric data protected by the EAC protocol conform with EU standards, as well as to verify crossover interoperability between EAC inspection systems and e-Passports from different countries (“Prague ePassport,” 2007; entrust.com, 2008). Since the U.S. e-Passport uses BAC but not EAC protocol, it is necessary for the U.S. to increase its cooperation with the EU in order to take full advantage of biometrics data on e-documents. The proliferation of vendors and

systems makes standardization and interoperability even more difficult (Chartier & van den Akker, 2008). Countries in Asia and Africa that have already started issuing e-documents have chosen different technical schemes, and without global cooperation the issuance of these documents cannot fulfill its primary goals of helping identify terrorists and promoting safer travel worldwide (“Second generation,” 2008; Biometrics to the rescue, 2009; Molnar, 2009). Further research to speed up the roadmap for implementing better protocols (for example EAC) would enhance interoperability at the global level.

Coordination of U.S. Identification Programs. Policy coordination among states and the federal government can greatly benefit the implementation of the REAL ID and future e-document programs in the United States (Labay & Anderson, 2006; Thiesse, 2007; Glasser, Goodman, & Einspruch, 2007; Ayoade, 2007). Driven by distinct goals, the expansion of e-documents programs in the United States has been marked by policy, privacy, and jurisdictional issues and the use of incompatible RFID technologies. National programs such as e-Passport and PASS Card follow different system design philosophies, which require different infrastructures for data management and different RFID reader technologies deployed at our border inspection stations. The REAL ID program utilizes yet a third technology (i.e., MRZ), and because its implementation falls under the states’ jurisdiction, different state-specific solutions like EDLs are starting to emerge. Under DHS guidance and coordination efforts, states have been adopting standards for EDLs that are aligned with the REAL ID program, but the overall system operational architecture is still evolving with the new PASS ID Act just introduced in Congress in June 2009 (U.S. Congress, 2009). Coordination of U.S. identification programs is largely a political issue, and further research to understand how to present the benefits of such programs to the population and help achieve wider “buy-in” to the technology is key.

Emerging Technologies for Identification Systems. Ultimately our national security depends on the ability to link data stored in heterogeneous and geographically distributed systems while maintaining high privacy and security protections. Similar conditions and information-sharing problems exist in other fields, such as public health (Wunder & Roach, 2008; Moore & French, 2007) and banking (O’Connor, 2008) and are rapidly moving into other areas with the increased adoption of computerized systems. New emerging technologies can help craft a solution to these problems. Federated data grids allow secure and authenticated access to distributed data sources while controlling and/or avoiding the movement of data outside the original system. Relevance engines and associative memories can assist in determining the likelihood of an individual’s identity based on incomplete or dispersed data. A recent novel infrastructure, called Biovault, has been proposed that uses biometrics (fingerprints, iris pattern, etc.) to encrypt and decrypt data and provides for secure and safe communications/transactions, while avoiding interception of the biometrics of those individuals participating in the exchange. In the future it may be applied to digitally sign electronic documents (Tait & von Solms, 2009). These and other new technologies are worth exploring to

find an answer to these complex problems. Technology, if supported by global cooperation and coordinated domestic policies, can help reconcile the goals of national security and personal privacy.

Contact Information

Dr. Monica Nogueira, Director

Intelligent Systems Lab, Center for Logistics and Digital Strategy

Kenan-Flagler Business School, CB# 3440, Kenan Center

University of North Carolina, Chapel Hill, 27599-3440

919-843-4740

monica_nogueira@unc.edu

Monica Nogueira, PhD, is director of the Intelligent Systems Laboratory (ISL) of the Center for Logistics and Digital Strategy at Kenan-Flagler Business School (KFBS) at The University of North Carolina at Chapel Hill. In this capacity, she is responsible for overseeing the projects developed by the ISL for its corporate and institutional clients and works closely with UNC professors and students and the KFBS staff. Dr. Nogueira is an expert in data modeling and analysis, which she applies to design and build decision support tools that mine and correlate information from large and diverse datasets to extract relevant knowledge that enables users to act on those problems that are most significant to them. She uses her computer science expertise to design and implement new software applications that utilize state-of-the-art technologies to solve practical problems for ISL external and internal customers. Her primary research interests include new technologies and their practical uses to create new methodologies that support “intelligent” tools and their application to everyday problems in logistics and supply chains and data and text mining methodologies and tools for knowledge discovery and extraction. Dr. Nogueira has developed a number of projects and tools that demonstrate the use of radio frequency identification (RFID) technology for controlling the safety of perishable products (i.e., cold chain for food and medical drugs). In these projects, RFID is used as the integrator element that allows tracking and tracing of the perishables and total visibility throughout the supply chain, guaranteeing their safety.

Noel P. Greis, PhD, is director of the Kenan Institute’s Center for Logistics and Digital Strategy and professor of Operations, Technology and Innovation Management at the Kenan-Flagler Business School at the University of North Carolina at Chapel Hill. Dr. Greis is the co-director of the recently established UNC-Tsinghua Center for Logistics and Enterprise Development in Beijing, China, a joint center of Tsinghua University’s Department of Industrial Engineering and the Kenan-Flagler Business School at the University of North Carolina at



Chapel Hill. Dr. Greis's research is transforming the way we predict, evaluate, and respond to complex and critical events in domains such as medicine and public health, food safety, supply chain management and logistics, defense and security, as well as energy and the environment. Dr. Greis is an expert in the area of intelligent systems design and development and works with organizations to develop knowledge-based systems and predictive analytics that support decision-making in complex, disruptive, and dynamic environments. Dr. Greis is also an expert in the use of intelligent agent-based modeling and simulation to predict the behavior of complex systems—thus improving decision-making capability.

References

Abelson, D. E., & Wood, D. (2007). *People, security and borders: The impact of WHTI on North America*. Ottawa: Fullbright Foundation. Retrieved from [http://www.nnasc-renac.ca/PeopleSecurityandBorders \(English\).pdf](http://www.nnasc-renac.ca/PeopleSecurityandBorders%20(English).pdf)

Albrecht, K. (2008, September). How RFID Tags could be used to track unsuspecting people. *Scientific American*, 299(3), 72–77.

American Civil Liberties Union. (n.d.). *The PASS ID act of 2009: An inadequate fix for Real ID*. Retrieved from <http://www.realnightmare.org>

Ayoade, J. (2007). Roadmap to solving security and privacy concerns in RFID systems. *Computer Law & Security Report*, 23(6), 555–561.

Biometrics review: 2008/2009. (2009). *Biometric Technology Today*, 17(1), 9–11.

Biometrics to the rescue for global aviation security. (2009, April 10). *The Guardian*. Retrieved from http://www.ibia.org/newsevents/email_ibia.php?id=309#3235

Bundesamt für Sicherheit in der Informationstechnik. (2009, May 5). *Technical guideline TR-03110: Advanced security mechanisms for machine readable travel documents—Extended access control (EAC), password authenticated connection establishment (PACE), and restricted identification (RI)*. Version 2.01, Bonn, Germany.

Burbank, B. (2009, February 22). Free reverse license plate search online. *EzineArticles.com*. Retrieved from <http://ezinearticles.com/?Free-Reverse-License-Plate-Search-Online&id=2024618>

Calabrese, C. (n.d.). *Real costs: Assessing the financial impact of the real ID act on the states*. Counsel, Technology & Liberty Program, American Civil Liberties Union. Retrieved from [http://www.realnightmare.org/images/File/Outline of Real ID Costs.pdf](http://www.realnightmare.org/images/File/Outline%20of%20Real%20ID%20Costs.pdf)

Center for Democracy and Technology. (2008, February 1). *Real ID: What should Congress do now? CDT Analysis of the REAL ID Act and the Department of Homeland Security's Final Regulations*. Retrieved from http://www.cdt.org/security/identity/20080201_REAL%20ID_hillbrief.pdf

Chartier, P., & van den Akker, G. (2008, January 1). *RFID standardisation state of the art report—Version 1*. GRIFS. Global RFID Interoperability Forum for Standards, Project no. 215224, coordinated by EU's Seventh Framework Programme. Retrieved from http://www.grifs-project.eu/data/File/GRIFS_D1_3_State_of_the_Art_Report.pdf

Cole, S. A. (2005). More than zero: Accounting for error in latent fingerprint identification. *The Journal of Criminal Law & Criminology*, 95(3), 985–1078.

Cole, S. A. (2006). Is fingerprint identification valid? Rhetorics of reliability in fingerprint proponents' discourse. *Law & Policy*, 28(1), 109–135.

Controversial Real ID act approved. (2005). *Card Technology Today*, 17(5), 3–4.

Cuff, D., Hansen, M., & Kang, J. (2008). Urban sensing: Out of the woods. *Communications of the ACM*, 51(3), 24–33.

eHow, Inc. (n.d.) How to find the owner of a license plate. *eHow.com* website. Retrieved on from http://www.ehow.com/how_2087251_find-owner-license-plate.html

entrust.com. (2008, September 18). News release: *Entrust EAC ePassport PKI operates “flawlessly” at Prague, leveraging Slovenia and UK infrastructure: Entrust demonstrates perfect PKI certificate exchange for EAC interoperability test across multiple countries and vendors*. Retrieved from <http://www.entrust.com/news/index.php?s=43&item=629>

Ezovski, G. M., & Watkins, S. E. (2007, March 26–28). The electronic passport and the future of government-issued RFID-based identification. *IEEE Intl Conference on RFID*, 15–22.

Ferguson, R. B. (2007, February 28). *DHS confirms Real ID Act regulations coming; States rebel*. *eWeek.com*. Retrieved from <http://www.eweek.com/c/a/Mobile-and-Wireless/DHS-Confirms-Real-ID-Act-Regulations-Coming-States-Rebel>

Garson, G. D. (2006). Securing the virtual state recent developments in privacy and security. *Social Science Computer Review*, 24(4), 489–496.

Glasser, D. J., Goodman, K. W., & Einspruch, N. G. (2007). Chips, tags and scanners: Ethical challenges for radio frequency identification. *Ethics and Information Technology*, 9(2), 101–109.

Hadley, C. (2004). Your personal passport. *European Molecular Biology Organization Reports*, 5(2), 124–126.

Houdeau, D. (2009). Progress through uniformity. In N. Pohlmann, H. Reimer, W. Schneider (Eds.), *ISSE 2008 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2008 Conference* (pp. 262–267). Retrieved from <http://www.springerlink.com/content/q03v47pn7032w57l/>

International Organization for Standardization, International Electrotechnical Commission (ISO, IEC). (2009). *Information Technology—Security Techniques—A Framework for Identity Management (ISO/IEC WD 24760 [Working draft])*.

Labay, V., & Anderson, A. M. (2006). Ethical considerations and proposed guidelines for the use of radio frequency identification: Especially concerning its use for promoting public safety and national security. *Science and Engineering Ethics*, 12(2), 265–272.

Liersch, I. (2009). Electronic passports—From secure specifications to secure implementations. *Information Security Technical Report*, 14(2), 96–100.

Martin, Z. (2009, January 29). *Identity—The next generation electronic passport*. Go Kiosk website. Retrieved from <http://www.gokiosk.net/kiosk/2009/01/identity---the-next-generation-electronic-passport.html>

Meingast, M., King, J., & Mulligan, D. K. (2007, March 26–28). Embedded RFID and everyday things: A case study of the security and privacy risks of the U.S. e-passport. *IEEE International Conference on RFID* (pp. 7–14).

Molnar, G. (2009, September 21–23). Untitled presentation at the Fifth Symposium and Exhibition and on ICAO Machine Readable Travel Documents, (MRTDs), Biometrics and Security Standards, Montreal, Canada.

Moore, D. H., & French, D. D. (2007). Real ID act and radio frequency identification devices (RFID): The future of patient identification? *Journal of the American Medical Directors Association*, 8(8), 551–551.

National Commission on Terrorist Attacks Upon the United States. (2004, July 22). *The 9/11 commission report*. Retrieved from <http://www.9-11commission.gov/report/911Report.pdf>

National Veterans Committee on Constitutional Affairs. (2007, October 17). Supplement packet to: *The Real ID Act of 2005: Real tyranny against Americans*. Retrieved from http://files.meetup.com/1279133/Real_ID_Book_Suppliment_1.pdf

O'Connor, M. C. (2007, August 16). One year later, U.S. E-Passport's architect says system is a success. *RFID Journal*. Retrieved from <http://www.rfidjournal.com/article/articleprint/3567>

O'Connor, M. C. (2008, July). Banking group to set RFID roadmap. *RFID Journal*. Retrieved from <http://www.rfidjournal.com/article/articleview/4196/1/1/>

Ozer, N. A. (2008, January 25). Rights “chipped” away: RFID and identification documents. *Stanford Technology Law Review* 1. Retrieved from <http://stlr.stanford.edu/pdf/ozier-rights-chipped-away.pdf>

Passport cards to use vicinity RFID. (2006). *Card Technology Today*, 18(10), 4.

Pasupathinathan, V., Pieprzyk, J., & Wang, H. (2008). An on-line secure e-passport protocol. In L. Chen, Y. Mu, & W. Susilo (Eds.), *Proceedings of the 4th International Conference on Information Security Practice and Experience (ISPEC 2008)*, (pp. 14–28). Sidney, Australia: Springer.

- Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., & Worek, W. (2006). Preliminary face recognition grand challenge results. *IEEE Proceedings of the 7th International Conference on Automatic Face and Gesture Recognition (FGR'06)*, 15–24.
- Prague ePassport trials a success for EAC. (2007). *Card Technology Today*, 19(3), 1.
- REAL ID deadline relaxed. (2007). *Card Technology Today*, 19(3), 1.
- Rotenberg, M. (2006). Real ID, real trouble? *Communications of the ACM*, 49(3), 128.
- Russell, B. Z. (2009, July 14). Tighter border hurts economy, officials say: Travel between U.S., Canada has dropped since 2001. *The Spokesman-Review* website. Retrieved from <http://www.spokesman.com/stories/2009/jul/14/tighter-border-hurts-economy-officials-say/>
- Second generation ePassports put through their paces. (2008). *Card Technology Today*, 20(10), 5.
- Smart cards lose out in US passport card initiative. (2008). *Card Technology Today*, 20(1), 4–5.
- Swofford, H. J. (2005). Fingerprint patterns: a study on the finger and ethnicity prioritized order of occurrence. *Journal of Forensic Identification*, 55(4), 480–488.
- Tait, B. L., & von Solms, S. H. (2009). Biovault: Biometrically based encryption. *International Journal of Electronic Security and Digital Forensics*, 2(3), 269–279.
- The Impact of Implementation: A Review of the Real ID Act and Western Hemisphere Travel Initiative Hearing before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia of the Senate Committee on Homeland Security and Governmental Affairs, 110th Cong., 2nd Sess.* (2009, April 29) (testimony of Angelo Amador, from The United States Chamber of Commerce: Americans for Better Borders Coalition). Retrieved from http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4df58573-2d15-47fc-8a00-ebcd17628f73
- Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, 16(2), 214–232.
- U.S. Congress. (2004, December 17). *Intelligence Reform and Terrorism Prevention Act of 2004*. Retrieved from <http://travel.state.gov/pdf/irtpa2004.pdf>
- U.S. Congress. (2005, May 11). *The REAL ID Act of 2005*. Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/pdf/PLAW-109publ13.pdf>
- U.S. Congress. (2007, February 16). *REAL ID Repeal and Identification Security Enhancement Act of 2007*. Retrieved from <http://www.gpo.gov/fdsys/pkg/BILLS-110hr1117IH/pdf/BILLS-110hr1117IH.pdf>
- U.S. Congress. (2009, June 15). *Providing for Additional Security in States' Identification (PASS ID) Act of 2009*. Retrieved from <http://www.opencongress.org/bill/111-s1261/text>

U.S. Customs and Border Protection. (2009, May 7). *DHS, CBP testify on implementing the Western Hemisphere Travel Initiative at the land and sea ports of entry: Are we ready?* Retrieved from

http://www.cbp.gov/xp/cgov/newsroom/congressional_test/whti_ready_testify.xml

U.S. Department of Homeland Security and U.S. Department of State. (2008b). *Western Hemisphere Travel Initiative land and sea final rule*. Retrieved from

http://www.dhs.gov/xlibrary/assets/whti_landseafinalrule.pdf

U.S. Department of Homeland Security. (2009b). *Potentially high costs and insufficient grant funds pose a challenge to real ID implementation*. Retrieved from

http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_09-36_Mar09.pdf

U.S. Department of Homeland Security. (2006, October 17). *Fact sheet: Western Hemisphere Travel Initiative (WHTI)—Passport card technology choice: Vicinity RFID*. Retrieved from

http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm

U.S. Department of Homeland Security. (2008a). *Minimum standards for driver's licenses and identification cards acceptable by federal agencies for official purposes; Final rule*. Retrieved from

<http://edocket.access.gpo.gov/2008/08-140.htm>

U.S. Department of Homeland Security. (2009a). *Overview of enhanced driver's licenses*. Retrieved from

<http://www.cbp.gov/xp/cgov/travel/vacation>

U.S. Department of Homeland Security: Data Privacy & Integrity Advisory Committee. (2007, May 7). *Report No. 2007-01: Notice of proposed rulemaking for implementation of the REAL ID act*. Retrieved from

http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_05-2007_realid.pdf

U.S. Department of State. (n.d.). *Enhanced border security and visa entry reform act of 2002—ALDAC No. 1*. Retrieved from

http://www.travel.state.gov/visa/laws/telegrams/telegrams_1403.html

U.S. Department of State. (n.d.). *The U.S. electronic passport*. Retrieved from

http://www.travel.state.gov/passport/eppt/eppt_2498.html

U.S. Department of State. (n.d.). *U.S. passport card*. Retrieved from

http://travel.state.gov/passport/ppt_card/ppt_card_3926.html

U.S. Government Accountability Office. (2009, April 13). *Addressing significant vulnerabilities in the Department of State's passport issuance process, GAO-09-583R*. Retrieved from

<http://www.gao.gov/products/GAO-09-583R>

Vaudenay, S., & Vuagnoux, M. (2007). About machine-readable travel documents. Anti-counterfeit image analysis methods: A special session of ICSXII. *Journal of Physics, Conference Series*, 77, 1–9.

Walford, L. (2008, March 12). *ATM security in Asia moves to veins*. *ATMmarketplace.com* website. Retrieved from <http://www.atmmarketplace.com/article.php?id=9738>

Whalen, P. J. (2009, September 27). Border Blues: New travel rules are hurting binational trade, tourism. *The Buffalo News* website. Retrieved from <http://www.buffalonews.com/367/story/809277.html>

WP1: Review of Standards and Procedures for International Standardisation in relation to RFID. (2008, January 1). Project CASAGRAS—Coordination and Support Action for Global RFID-Related Activities and Standardisation, no. 216803, funded by EU's *Seventh Framework Programme*. Final white papers from May 2009, retrieved from <http://www.rfidglobal.eu/userfiles/documents/white%20papers%201.pdf>

Wunder, G., & Roach, B. (2008, July). Electronic pedigrees and counterfeit pharmaceuticals: The U.S. experience. *Washburn University School of Business Working Paper Series, No. 104*.

Zetter, K. (2006, August 3). Hackers clone E-passports. *Wired*. Retrieved from <http://www.wired.com/science/discoveries/news/2006/08/71521>



Appendix A

A list of 69 countries currently issuing e-Passports with embedded RFID and/or personal biometrics appears in Table A1 below. A list of countries planning the introduction of e-Passports and other forms of ID using RFID technologies is presented in Table A2. Issuing dates for e-Passports on both tables were mostly obtained from <http://www.SecurityDocumentWorld.com> on June 11, 2009. Countries currently issuing national EIDs are shown in Table A3.

Table A1. Countries Currently Issuing e-Passports

Country	Start Date	(Rank)	Country	Start Date	(Rank)
Albania	2009.01	(64)	Malta	2008.10.08	(61)
Andorra	2006.09.01	(32)	Monaco	2005.07.18	(06)
Australia	2005.10.24	(09)	Montenegro	2008.05	(56)
Austria	2006.06.16	(17)	New Zealand	2005.11.04	(11)
Bahamas	2007.12.05	(50)	Nigeria	2007.08.17	(48)
Belgium	2004.11.24	(04)	Norway	2005.10.03	(08)
Bosnia and Herzegovina	2009.10.15	(69)	Pakistan	2004.10.25	(03)
Brunei	2007.02.17	(40)	Philippines	2009.08.11	(68)
Cambodia	2007.03.06	(41)	Poland	2006.08.28	(28)
Czech Republic	2006.09.01	(30)	Portugal	2006.07.31	(18)
Croatia	2009.07.01	(67)	Qatar	2008.04.20	(55)
Denmark	2006.08.01	(19)	Republic of China (Taiwan)	2008.12.29	(62)
Dominican Republic	2004.05.01	(02)	Republic of Moldova	2008.01.01	(52)
Estonia	2007.05.22	(43)	Republic of Sudan	2009.05	(66)
Finland	2006.08.21	(22)	Romania	2008.12.31	(63)
France	2006.04.12	(14)	Russia	2006.09.01	(31)
Germany	2005.11.01	(10)	San Marino	2006.10.12	(34)
Greece	2006.08.26	(24)	Senegal	2007.12	(51)
Holland	2006.08.26	(23)	Serbia	2008.07.07	(58)
Hong Kong	2007.02.05	(39)	Singapore	2006.04.29	(15)
Hungary	2006.08.29	(29)	Slovakia	2008.01.15	(53)
Iceland	2006.05.23	(16)	Slovenia	2006.08.28	(27)
India	2008.06.25	(57)	Somalia	2007.01.21	(38)
Iran	2007.07.01	(45)	South Africa	2009.04.08	(65)
Ireland	2006.10.16	(35)	South Korea	2008.03.11	(54)
Italy	2006.10.26	(37)	Spain	2006.08.14	(21)
Ivory Coast	2008.07.30	(60)	Sweden	2005.10.03	(07)
Japan	2006.03.20	(13)	Switzerland	2006.09.04	(33)
Latvia	2007.11.20	(49)	Thailand	2005.05.26	(05)
Liechtenstein	2006.10.26	(36)	Turkmenistan	2008.07.10	(59)
Lithuania	2006.08.28	(25)	United Kingdom	2006.03.06	(12)
Luxembourg	2006.08.28	(26)	United States of America	2006.08.14	(20)
Macedonia	2007.04.02	(42)	Ukraine	2007.06.01	(44)
Malaysia	1998.03.01	(01)	Venezuela	2007.07.01	(46)
Maldives	2007.07.26	(47)			

Table A2. Countries Planning to Start Issuing e-Documents

Country	e-Passport Start Date	National EID Start Date
Armenia	April 2010	April 2010
Belgium (ex-pats e-ID)	—	End of 2010
Botswana	March 2010	—
Bulgaria	March 2010	March 2010
Canada	2011	—
Gambia	—	December 2009/2010
Georgia	2010	—
Guatemala	—	2011
Israel	2010	2010
Mexico	—	First quarter of 2010
People's Republic of China	2010	In use
South Africa	—	2009/2010
Tajikistan	February 2010	—
Turkey	April 2010	—
UK (2 nd generation)	October 2010	—

Table A3. Countries Currently Issuing EIDs

Country
Albania
Bahrain
Belgium
Estonia
Finland
Hong Kong
India
Italy
Lithuania
Macedonia
Malaysia
Montenegro
Oman
People's Republic of China
Portugal
Republic of Rwanda
Spain
Sweden
Thailand
United Arab Emirates