



**COMMENTS OF THE SMART CARD ALLIANCE
TO THE DEPARTMENT OF STATE FEDERAL REGISTER NOTICE,
"CARD FORMAT PASSPORT; CHANGES TO PASSPORT FEE SCHEDULE,"
22 CFR PARTS 22 AND 51, RIN 1400-AC22, PUBLIC NOTICE 5558**

Docket ID: DOS-2006-0329
November 3, 2006

SUMMARY

The Smart Card Alliance, whose members provide both ISO/IEC 14443-based contactless smart card and RFID products, believes the vicinity read RFID technology that has been proposed for use in the passport card program is the wrong technology to implement a secure identification card that will be required for U.S. citizens who do not have passports to verify their identity at land and sea border crossings.

The Department of State published a Federal Register notice on October 17, 2006, announcing the technology chosen for the proposed new passport card that is planned to be issued as part of the Western Hemisphere Travel Initiative. This notice states that the proposed passport card would use "vicinity read" radio frequency identification (RFID) technology that conforms to ISO/IEC 18000-6, Type C, "Radio frequency identification for item management -- Part 6," rather than the ISO/IEC 14443-based "proximity read" secure contactless smart card technology that is being used for the new electronic passports (ePassports).

We believe that vicinity read RFID technology is inappropriate for implementing a secure identification card that is used to verify a citizen's identity. Our concerns are that the passport card decision to use vicinity read RFID technology does not consider the following issues:

1. **Lack of Security Safeguards.** The vicinity read RFID technology proposed for the passport card does not support the necessary security safeguards to allow border officials to verify that the passport card is authentic and to protect the information that is on the card.
2. **Potential for Tracking and Citizen Distrust.** The vicinity read RFID technology proposed for the passport card, in combination with its weak cryptographic protections, will feed citizen distrust of the program due to the undeniable observation by some technologists that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve.
3. **Expansion in the Number of Unique Identity Documents and Required Border Infrastructure.** Using vicinity read RFID tags for the passport card adds another type of technology in identity documents and requires another infrastructure investment in readers and networks at land and sea borders and in central databases and support systems to implement the program.
4. **Reliance on Real-Time Access to Central Databases and Networks.** The proposal for the passport card program relies on an architecture of secure databases and

networks to communicate the cardholder's personal information to the border crossing point in real-time during the identity verification process, leaving the security of the process vulnerable to attacks that could disrupt RF or network communications.

5. **Questionable Throughput Expectations for Proposed Operational Scenario.** Even with the long range read of the passport card, the proposed Department of Homeland Security (DHS) operational scenario still requires citizens to stop at the border crossing for final verification. This significantly reduces or eliminates the efficiencies that DHS claims will result from having vicinity read RFID technology built into passport card.
6. **Operational Issues with Vicinity Read RFID Tags in Vehicles.** The challenges of reliably reading a high volume of long range passive RFID tags that are held within vehicles will make it difficult for DHS to realize the efficiencies assumed for the vicinity read RFID technology.
7. **Inadequate Open Discussion of Implementation Approach.** No third party standards body has been involved in the passport card program to develop specifications for or comment on the measures proposed for protecting and using personal information.

These issues are described in detail below, along with Smart Card Alliance recommendations for measures that DHS and Department of State could implement to improve the passport card program.

RFID tag technology that was designed to track packages and products is not the appropriate technology to use for securing human identification systems. The U.S. government selection of vicinity read RFID technology for the proposed passport card puts border crossing throughput as the primary goal, at the expense of information security and citizen privacy and while not actually materially improving throughput if border security is to be improved. The only proven technology existing today that meets all of the objectives of increased border security, citizen privacy and efficient border crossing is contactless smart card technology -- the technology that is being used for ePassport. Using contactless smart card technology would achieve the objective of a faster, more secure means for tens of millions of citizens to cross back into our borders from land and sea, while still protecting the security and privacy of individuals.

There are many advantages to using contactless smart card technology for the passport card program, including the ability to support electronic verification of authenticity to prevent counterfeiting and to use secure, encrypted communications to thwart eavesdropping and replay attacks, and ensure privacy protection for cardholders. A passport card based on contactless smart card technology can also leverage the infrastructure that is being put in place by DHS and the Department of State to support the new ePassport. Using the same secure contactless technology for the passport card and ePassport could well decrease the implementation time and cost of the program, increase public acceptance of the program, and improve the security of our land border points of entry.

The Smart Card Alliance, whose members provide both ISO/IEC 14443-based contactless smart card and RFID products, urges the Department of State and DHS to reconsider the technology choice and to select contactless smart card technology. Contactless smart card technology is already being used in ePassports and has been proven to be effective and secure for human identity applications. Further detail supporting the Smart Card Alliance position is included below.

BACKGROUND

Part of the Western Hemisphere Travel Initiative (WHTI), the proposed passport card is an option that can be used instead of a regular passport book when U.S. citizens are re-entering the United States at land and sea entry points from Mexico, Canada and the Caribbean. Today, only about

25 percent of U.S. citizens carry passports. Starting no later than June 2009, all Americans will need to provide proof of citizenship and identity when re-entering the U.S.

The Department of State and Department of Homeland Security have announced that the proposed passport card will use vicinity read RFID technology that conforms to ISO/IEC 18000-6, Type C, "Radio frequency identification for item management -- Part 6." This standard, published by the International Organization for Standardization (ISO) in July 2006, is based on the EPC Gen 2 Class 1 UHF standard developed by EPCglobal. EPCglobal is the organization working to develop standards for the Electronic Product Code™ (EPC), a new system that uses RFID for the automatic identification of consumer products. According to the State Department Federal Register notice, machines at border crossings would read information on the RFID tag, connect to a secure U.S. government database containing biographical data and a photograph, and display that information to the Customs and Border Protection (CBP) official. While the RFID tag in the card itself would not hold any personal information, each card will transmit a unique reference number that can be read from up to 20 feet away when interrogated by a reader.

The Department of State is also now issuing new ePassports which incorporate contactless smart card technology based on ISO/IEC 14443, "Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards," and implementing security mechanisms specified by the International Civil Aviation Organization (ICAO) for globally interoperable machine-readable travel documents. ePassports store an individual's biographic information on a secure smart card chip built into the passport and allow this information to be read locally by authorized readers. The ePassport implementation features short read range, data encryption, mutual authentication, shielding and other security measures to protect the ePassport holder's personal information.

SMART CARD ALLIANCE CONCERNS

1. Lack of Security Safeguards. The vicinity read RFID technology proposed for the passport card does not support the necessary security safeguards to allow border officials to verify that the passport card is authentic and to protect the information that is on the card.

ISO/IEC 18000-6 Type C (EPC Gen 2) RFID tags were designed for supply chain applications (tagging cases and pallets of consumer goods) and had the primary goals to be low cost, to be able to be read from a long distance (up to 30 feet), and to be able to support dense tag environments (where there are many tags within range of several readers). The standard defines minimal security, including only static 32-bit passwords that are used to "kill" the tag or to access controlled memory.

This leaves EPC Gen 2 Class 1 RFID tags open to a number of security vulnerabilities if used in an application with sensitive information.

- EPC tags release their identifiers and product information to any compatible reader, with no ability to authorize that the reader is allowed to access the information prior to releasing the data. The kill and access control passwords are also static, using no strong cryptographic mechanisms. Guessing or cracking the 32-bit passwords would not be difficult for a determined attacker. For the passport card application, this means that a determined criminal with an EPC reader could read passport cards and, as described below, duplicate the EPC tag.
- EPC tags are subject to cloning. Since EPC tags release their identifiers and product information to any compatible reader, the data that is read could be easily written to a blank EPC tag, creating a duplicate tag. For the passport card application, this means that it would be straightforward to create a duplicate passport card that would be usable by anyone who looks similar to the registered passport card owner.

- There is no ability to validate the authenticity of an EPC tag. Once a tag has been duplicated, it would be considered valid by any compatible reader. For the passport card application, this means that CBP officials would need to touch and carefully examine the physical security features of each passport card to determine that it is not a clone.
- EPC tags offer only minimal resistance to eavesdropping and hotlisting. To mask data transmissions, a tag can send a random, temporary 16-bit number to the reader. The reader combines (using an exclusive-OR function) this number with sensitive data like passwords to deter casual eavesdroppers. However, this implementation does not offer cryptographic strength to protect communications. An eavesdropper merely needs to overhear the tag's transmission to intercept data or passwords. For the passport card application, this means that anyone with an EPC reader in a vehicle behind or next to a vehicle whose passport cards are being read would have an excellent opportunity to overhear the transmission. Even if the passport card implementation uses the 16-bit session password, the criminal would be able obtain this password and then decrypt the true system password and the owner's unique reference number.

While these vulnerabilities may not be critical in a supply chain application because the information contained on the tags is not sensitive, they are serious issues for the passport card application which is communicating a unique number that is assigned to an individual and which is used to access personal information about that individual.

Contactless smart card technology, on the other hand, not only supports security features that ensure the integrity, confidentiality, and privacy of information stored on or transmitted by the card, but also provides features that can verify the authenticity of the identity document and its contents and help to prevent cloning, tampering and forgeries.

Contactless smart cards and readers conform to international standards, ISO/IEC 14443 and ISO/IEC 7816, and can implement a variety of strong industry-standard cryptographic protocols (e.g., AES, 3DES, RSA, ECC). The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes EPC Gen 2 tags lack – i.e., the ability to securely manage, store and provide access to data on the card, perform complex functions (for example, encryption and mutual authentication) and interact intelligently via RF with a contactless reader. Applications using contactless smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following:

- *Mutual authentication.* For applications requiring secure card access, the contactless smart card-based device can verify that the reader is authentic and can prove its own authenticity to the reader before starting a secure transaction.
- *Strong information security.* For applications requiring complete data protection, information stored on cards or documents using contactless smart card technology can be encrypted and communication between the contactless smart card-based device and the reader can be encrypted to prevent eavesdropping. Hashes and/or digital signatures can be used to ensure data integrity and to authenticate the card and the credentials it contains. Cryptographically strong random number generators can be used to enable dynamic cryptographic keys, preventing replay attacks.
- *Strong contactless device security.* Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers,

sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

- *Authenticated and authorized information access.* The contactless smart card's ability to process information and react to its environment allows it to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.
- *Strong support for information privacy.* The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required. The ability to support authenticated and authorized information access and the strong contactless device and data security make contactless smart cards excellent guardians of personal information and individual privacy.
- *Controlled manufacturing process.* Smart card devices are controlled through the entire manufacturing process, including during the manufacturing of the electronic components in the silicon foundry. This is part of the Common Criteria security certifications often imposed on smart card and smart card integrated circuit manufacturers. This very detailed secure control of product sources makes it harder for criminals to obtain non-programmed devices which could then be used to create cloned working products. Putting such controls on RFID tags would significantly increase their cost.

It is important to note that information privacy and security must be designed into an application at the system level by the organization issuing the contactless device, card or document. It is critical that issuing organizations have the appropriate policies in place to support the security and privacy requirements of the application being deployed and then implement the appropriate technology that delivers those features. The ability of contactless smart card technology to support a wide array of security features provides organizations with the flexibility to implement the level of security that is commensurate with the risk expected in the application.

2. Potential for Tracking and Citizen Distrust. The vicinity read RFID technology proposed for the passport card, in combination with its weak cryptographic protections, will feed citizen distrust of the program due to the undeniable observation by some technologists that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve. This raises serious privacy concerns that will have to be overcome if the program is to be embraced by Americans.

ISO/IEC 18000-6 Type C RFID technology was designed for tracking goods. It does not include the features necessary to prevent tracking by determined criminals.

The proposed passport card will include a unique reference identifier for the citizen. By using vicinity read RFID technology, the card will be able to be read at long range (up to 20 feet) by any compatible reader, with no ability to authorize that the reader is allowed to access the information prior to releasing the data. It is, therefore, theoretically possible that criminals can surreptitiously track citizens once they cross the border. The use of a unique identifier does not remove this risk to citizens' privacy since an individual's true identity could be determined using other means (e.g., researching the vehicle's license plate). This identity can then be associated with the presence of the tag that is read by a compatible reader in any location. While this may be difficult to do, the possibility will feed citizen mistrust of the program.

Reliance on citizens placing their cards in the shielding sleeves is not sufficient since the sleeves could be misplaced or not used.

Citizens, privacy groups and other organizations are very concerned about the use of RFID technology and the risk it brings for tracking and identifying citizens. A lesson can be learned from the public outcry to the initial proposal for the ePassport design. As a result of the outpouring of public opinion and recommendations from industry, the Department of State changed the ePassport design to incorporate additional security features to address public concerns.

An **ISO/IEC 14443-based contactless smart card solution** can address these concerns. A passport card using contactless smart card technology operates at a very short range and can be implemented so that it does not require a sleeve to protect the privacy and security of information stored on the card and communicated during the identity verification process. Such a system would use the strong cryptographic algorithms supported by contactless smart cards to use a random identification number generated by the smart card chip on the passport card to register the passport card's presence to the reader, perform mutual authentication between the card and the reader to ensure that both are authentic and valid, and encrypt communication between the card and reader. All of these capabilities are now included in the ePassport design and can be supported in a passport card using ISO/IEC 14443 contactless smart card technology.

The passport card program would gain higher public confidence by implementing a contactless smart card-based approach that includes security mechanisms to counter the risks of unauthorized access to citizen-unique information.

3. Expansion in the Number of Unique Identity Documents and Required Border Infrastructure. Using vicinity read RFID tags for the passport card adds another type of technology in identity documents and requires another infrastructure investment in readers and networks at land and sea borders and in central databases and support systems to implement the program.

Both U.S. citizens and foreign visitors will be presenting a wide range of identity documents that will need to be validated at borders, including the proposed passport cards, new ePassports, older U.S. passports, foreign ePassports and older foreign passports. To ensure the security of the border, all of the acceptable forms of identity documents will need to be verified.

The proposed new passport card does not eliminate the need for travelers to stop at a border crossing point. Even if everyone in a vehicle has a passport card, the CBP officer still needs to verify that vehicle occupants match the identity data returned from the central database. Many visitors or citizens will not have passport cards and will need to have their identity documents validated by stopping at the border crossing point.

This raises questions about whether the passport card program will actually yield any significant efficiencies. Where is the efficiency of the 20 foot read if the passport card is only held by a fraction of the border crossers or if a vehicle has occupants with a mix of documents?

This mixture of documents also raises questions about the need for investing in a new infrastructure of equipment and systems and in personnel training for yet another identity verification technology -- in parallel with investment already being made in the ePassport infrastructure. By using vicinity read RFID technology for the passport card, CBP will have to handle even more types of documents, creating inefficiencies in the border crossing process and increasing costs to tax payers.

While the Federal Register notice states that the technology is similar to that used in the FAST, NEXUS, SENTRI and I-94 programs, these programs differ from the proposed passport card both

in technology and processes that they use. The FAST, NEXUS and SENTRI programs use older RFID technology that predates the ISO/IEC 18000-6 Type C standard. These earlier version readers will not be able to read RFID tags compliant with ISO/IEC 18000-6 Type C. Similarly, the I94 program uses EPC Gen 1 Class 0 tags; readers designed to read these tags would also not be able to read the EPC Gen 2 tags proposed for the passport card. Even at border crossings that were equipped to handle these older programs, additional investment will be required to add ISO/IEC 18000-6 Type C readers for the passport card program.

It is also important to note that since the passport card will not contain the enhanced anti-counterfeiting features contained in the ePassport, additional equipment and time will be needed to verify visual watermarks or holograms on the passport card if security is to be maintained.

A more efficient solution is to implement the passport card using the same contactless smart card technology being incorporated in the new ePassport. This implementation would leverage the infrastructure that is being put in place to support the new ePassport, while also improving information security and privacy.

4. Reliance on Real-Time Access to Central Databases and Networks. The proposal for the passport card program relies on an architecture of secure databases and networks to communicate the cardholder's personal information to the border crossing point in real-time during the identity verification process, leaving the security of the process vulnerable to attacks that could disrupt RF or network communications.

The architecture relies on databases and networks that need to be reliable and available 24 hours per day, 7 days per week, 365 days per year. In addition to failures that could be expected in any networked system, an attacker could disrupt the security of the identity verification process by "jamming" the RF at a border crossing station. This could be done by a simple RF jammer emitting noise in the 902 to 925 MHz frequency band, rendering it impossible to remotely read any cards. The implementation is also vulnerable to attacks to network communications. In either case, border agents would need to resort to weaker manual identity verification processes.

The databases and networks would also need to be designed to allow only authenticated access to an individual's personal information. The DHS Privacy Impact Assessment (PIA), published August 10, 2006, states that passwords and role-based access would be used to protect access to citizens' personal information. Industry best practices for secure network and system access now call for multiple factors of authentication (including something you know, something you have and something you are). The current DHS plan uses only weak password-based security to protect access to personal information.

It is also important to note that if these networks and databases are not already operational and network connections are not installed at every border crossing point, significant investment will be required to equip the border with the necessary capabilities to accept passport cards.

Using **an approach that is compatible with the ePassport** would be more secure and more cost-effective. As with the ePassport, data could be stored on the passport card and read locally at all border crossing points. This has several advantages:

- The citizen maintains control of the private information, increasing the value of the passport card to the citizen.
- Passport cards would be able to be read locally at any border crossing point equipped with a reader, without needing real-time networked access to a secure government database.
- This architecture would provide immunity against an RF jamming attack on the proposed vicinity read RFID card that operates in the UHF frequency band.

- The authenticity of the card can be electronically determined at the border crossing, rather than putting the burden on the CBP officer to check the physical security features of the card to determine that it has not been tampered with or cloned.
- The implementation would leverage the investment already being put in place to read new ePassports.

5. Questionable Throughput Expectations for Proposed Operational Scenario. Even with the long range read of the passport card, the proposed DHS operational scenario still requires citizens to stop at the border crossing for final verification. This significantly reduces or eliminates the efficiencies that DHS claims will result from using vicinity read RFID technology.

The proposed solution favored by DHS using vicinity read RFID technology would work as follows at a land border crossing:

- A car approaching the border's yellow line passes under a portal approximately 20 feet from the Customs kiosk.
- Before the car reaches that yellow line, the driver and all passengers must remove their passport cards from the cards' protective sleeves and place the cards on the car's dashboard.
- As the car passes under the portal, data for all occupants is retrieved from a central government database, using the unique identification number contained on each card.
- The data is displayed on a CBP officer's computer screen while the car waits in line.
- When the car reaches the head of the line, the CBP officer compares the citizens presenting themselves for entry into the U.S. with the original issuance record retrieved from the database.
- If other security features are included on the card, such as holograms or watermarks, the CBP officer asks for all cards and examines them for authenticity.
- If some of the car's occupants do not have a passport card, the CBP officer collects passports and uses different readers to verify the passport information.

A similar operational scenario can be implemented with the more secure and privacy-protective contactless smart card technology used in ePassports. A solution using ISO/IEC 14443 contactless smart card technology could work as follows:

- A car approaching the border's yellow line pulls up to a card reader.
- The car's driver and/or passenger opens the window(s) and present the occupants' cards to the reader -- for example, by placing the cards in a reader tray.
- Using cryptographic protocols, the card authenticates the reader and confirms that the reader is authorized to access the stored information.
- Data stored on the card is read and authorized. As an alternative, data can be retrieved from a central database using a unique identification number on each card (as in the DHS proposed solution described above).

- Either data verification or the data itself is transmitted to the CBP officer while the car waits in line.
- When the car reaches the head of the line, the CBP officer visually verifies each occupant's identity.
- If some of the car's occupants do not have a passport card, the CBP officer collects passports and verifies their passport information.
- Optional security features, such as additional biometrics, could also be stored in the passport card chip and verified by the card reader. No assessment would be needed by the official.

We believe that the proposed use of vicinity read RFID technology puts too much priority on unproven efficiencies in an untried process and too little priority on issuance of a secure identity credential that protects citizens' private information. The Smart Card Alliance strongly recommends that DHS and Department of State conduct a trial to evaluate the performance of both vicinity read RFID tags and ISO/IEC 14443-based technologies before making a final implementation decision.

6. Operational Issues with Vicinity Read RFID Tags in Vehicles. The challenges of reliably reading a high volume of long range passive RFID tags that are held inside vehicles will make it difficult for DHS to realize the assumed efficiencies of the vicinity read RFID technology.

While vicinity read UHF RFID tags do enjoy a longer read range, their performance is still adversely affected by low dielectric materials between the tag and the reader. In the proposed scenario of reading the tags through the windshield of the citizen's vehicle, it will be the case that metallic films in and on the glass of some vehicles will prevent the reading of the tag. Furthermore, the expectation that several cards can be stacked on top of each other and still be read is highly unlikely as the tags in such close proximity will interfere with each other. Lastly, the wavelength of the UHF signal will make the system vulnerable to reflections and possible confusion of signals from tags in vehicles in adjacent lanes.

Analogies to the electronic tolling systems in place in several regions of the U.S. are not valid since these systems use a single powered transponder per vehicle, providing the RFID tag with additional range. The systems also provide drivers with both internal and external transponder options to handle possible issues with reading tags from inside a vehicle.

As recommended earlier, the Smart Card Alliance urges DHS and Department of State to conduct a thorough trial evaluating the operational performance of both vicinity read RFID tags and ISO/IEC 14443-based technologies before making a final implementation decision.

7. Inadequate Open Discussion of Implementation Approach. No third party standards body has been involved in the passport card program to develop specifications for or comment on the measures proposed for protecting and using personal information.

Instead, DHS has relied on private industry contractors to design, implement and operate the program without vetting the system through the time-proven method of allowing knowledgeable cryptographers, security experts, and privacy experts review the design and suggest changes. The technology decision was made with inadequate open discussion of system-level privacy and security issues, even to the extent that the DHS Privacy Impact Assessment (PIA) does not address the privacy risks of using vicinity read RFID technology.

ePassport standards were defined and debated in the international standards community, with specifications set by the International Civil Aviation Organization (ICAO), working in conjunction with the International Organization for Standardization (ISO). The specification considered the

needs of global implementations and was strengthened by the open discussion and critique of the implementation approach used.

As with the ePassport, the passport card program includes personally identifiable information about U.S. citizens and must be evaluated to the highest standards for its security and privacy protections. All aspects the program's collection, storage and use of citizens' personal information should be documented in the PIA.

The Smart Card Alliance recommends that the proposed system design be fully disclosed in the PIA and be posted for public comment. Furthermore, the recent appropriations act (Homeland Security Act 2007, Public Law 109-295) requires that NIST review and approve the security and privacy aspects of the card architecture before a final design is selected. The NIST review and certification should also be made public prior to any final technology decision.

CONCLUSION

RFID tag technology that was designed to track packages and products is not the appropriate technology to use for securing human identification systems. The U.S. government selection of vicinity read RFID technology for the proposed passport card puts border crossing throughput as the primary goal, at the expense of information security and citizen privacy and while not actually materially improving throughput if border security is to be improved. The only technology existing today that can achieve the objectives of increased border security, citizen privacy and efficient border crossing is contactless smart card technology. Numerous programs inside and outside of the U.S. use contactless smart card technology for secure identity applications, including the new ePassport and the Federal government and contractor personal identity verification (PIV) card.

There are many advantages to using contactless smart card technology for the passport card program, including the ability to support electronic verification of authenticity to prevent counterfeiting and to use secure, encrypted communications to thwart eavesdropping and replay attacks, and ensure privacy protection for cardholders. A passport card based on contactless smart card technology can also leverage the infrastructure that is being put in place by DHS and the Department of State to support the new ePassport. Using the same secure contactless technology for the passport card and ePassport could well decrease the implementation time and cost of the program, increase public acceptance of the program, and improve the security of our land border points of entry.

The Smart Card Alliance urges the Department of State and DHS to reconsider the technology choice and to select the contactless smart card technology that has been proven to be effective and secure for human identity applications and that is already being deployed in the ePassport program.

ABOUT THE SMART CARD ALLIANCE

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Members of the Smart Card Alliance include identification application technology providers and all of the industry segments that use smart card technology, including federal government and other non-federal agencies. The Smart Card Alliance invests heavily in education on the appropriate uses of technology for identification and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.



November 3, 2006

Office of Passport Policy
Planning and Advisory Services
Bureau of Consular Affairs
U.S. Department of State
2100 Pennsylvania Ave. NW, Suite 300
Washington, DC 20037

SUBJECT: Comments on the Department of State Federal Register Notice, "Card Format Passport; Changes to Passport Fee Schedule," 22 CFR Part 22 and 51, RIN 1400-AC22, Public Notice 5558

DOCKET ID: DOS-2006-0329

Dear Sir or Madam:

The Smart Card Alliance is submitting the attached comments in response to the Department of State Federal Register Notice, "Card Format Passport; Changes to Passport Fee Schedule," Docket ID Number DOS-2006-0329.

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Members of the Smart Card Alliance include identification application technology providers and all of the industry segments that use smart card technology, including federal government and other non-federal agencies.

The Smart Card Alliance appreciates the opportunity to provide input to the Department of State on the proposed Western Hemisphere Travel Initiative passport card. We would be happy to provide assistance with any technology analysis and provide material that provides additional details supporting our comments attached. Additional information about the use of smart cards in identity applications can be found on the Smart Card Alliance web site at <http://www.smartcardalliance.org>.

Please contact me at 609-587-4208 or by email at rvanderhoof@smartcardalliance.org if you have questions about the Smart Card Alliance comments.

Sincerely,

Randy Vanderhoof
Executive Director

Cc: Frank Moss, Deputy Assistant Secretary of State for Passport Services