Smart Card Alliance

Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID

June, 2006

Developed by:
Smart Card Alliance Identity Council

Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID

This paper provides support for the use of ISO/IEC 14443-based contactless technology for the Western Hemisphere Travel Initiative PASS card system. This technology can meet the program's operational requirement for high throughput while providing strong security, protecting individual privacy, and leveraging the ePassport infrastructure. The Smart Card Alliance recommends a technology trial to evaluate the performance of both EPC Gen 2 and ISO/IEC 14443-based contactless technologies before DHS makes a final implementation decision.

Background

In the past, fraudulent travel documents have been used to cross borders and violate immigration laws without detection. Today, for example, a U.S. citizen needs only a driver's license to reenter the United States after a visit to Canada. However, there are over 240 valid formats for a U.S. driver's license, and customs agents must rely on visual inspection and experience to assess potential security risks and identify counterfeit documents.

As part of the Intelligence Reform and Terrorism Prevention Act of 2004, the Western Hemisphere Travel Initiative imposes new requirements for admission to the United States. Starting in January 2008, everyone, including U.S. citizens returning from Canada, Mexico, Panama, the Caribbean, and Bermuda, must present secure travel documents establishing their identity and nationality to enter the United States. The Department of State and the Department of Homeland Security (DHS) plan to produce a less expensive, secure biometric ID card, called the People Access Security Service (PASS) card, as an alternative for U.S. citizens subject to this requirement who do not wish to use a passport. While the two agencies agree on many aspects of implementing the PASS card program, they currently do not agree on the best technology.

Technology Alternatives

DHS favors using ultra-high-frequency radio frequency identification (RFID) cards based on the Electronic Product Code™ Generation 2 (EPC Gen 2) specification. This technology allows cards to be read at a distance of up to 30 feet, which DHS regards as helpful for processing people in vehicles quickly and efficiently. The EPC Gen 2 technology was designed to automate the tracking of cases and pallets through a supply chain and to manage the inventorying of items on retail store shelves. For this reason, EPC Gen 2 was designed to read a large volume of "tags" inexpensively, at high speed, and at a relatively long distance. The technology supports 32-bit passwords to protect data written on the tag, but it does not use government-approved encryption algorithms. DHS intends to provide privacy protection for individuals by placing only a unique identification number on the card and using the number to retrieve personal information (a photograph and demographic information) from a central database when the card is used at a border crossing. EPC Gen 2 tags do not include extensive protection against cloning or counterfeiting.

The Department of State appears to be favoring a card that incorporates the same contactless smart card technology used in the new ePassport. This technology is also mandated for use in government employee and contractor ID cards under Homeland Security Presidential Directive 12 and is used for contactless financial transactions by American Express, MasterCard, and Visa. Contactless smart card technology complies with the ISO/IEC 14443 standard. A card using this technology can only be read from a few inches away and supports both strong privacy and security features and high throughput speed.

The proposed solution favored by DHS using long-range RFID cards would work as follows at a land border crossing:

- A car approaching the border's yellow line passes under a portal approximately 30 feet from the Customs kiosk.
- Before the car reaches that yellow line, the driver and all passengers must remove their PASS 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 database, using the unique identification number contained on each card.
- The data is transferred to a customs official's computer screen while the car waits in line.
- When the car reaches the head of the line, the customs official visually verifies each occupant's identity, using an image retrieved from the database.
- If other security features are included on the card, such as holograms or watermarks, the customs official asks for all cards and examines them for authenticity.
- If some of the car's occupants do not have a PASS card, the customs official collects passports and uses different readers to verify the passport information.

The proposed solution using ISO/IEC 14443 contactless smart card technology would work as follows:

- A car approaching the border's yellow line pulls up to a card reader.
- The car's driver rolls down the window and holds each occupant's card 2-4 inches from the card reader.
- Data stored on the card is read and authorized. As an alternative, data can be retrieved from a database using a unique identification number on each card (as in the DHS solution described above).
- Either data verification or the data itself is transmitted to the customs official while the car waits in line.
- When the car reaches the head of the line, the customs official visually verifies each occupant's identity.
- If some of the car's occupants do not have a PASS card, the customs official collects passports and verifies their passport information.
- Optional security features, such as additional biometrics, could also be stored in the PASS card chip and verified by the card reader. No assessment would be needed by the official.

Evaluation of RFID vs. ISO/IEC 14443 Contactless Technology

Two questions arise after reviewing these alternative approaches.

1. Is there really an efficiency advantage using the DHS RFID solution? What is the time difference between removing the card from its protective sleeve and placing it on the dashboard vs. opening the car window and holding the card up to a reader? At first glance, the DHS solution appears to have a throughput advantage. However, both processes require the cardholder to wait for inspection by a customs official.
2. What is the primary purpose of the PASS card: security or speed? The objective of the Western Hemisphere Trade Initiative PASS card is to strengthen border security without compromising individual privacy and without impeding the flow of individuals and vehicles. While convenience and trade facilitation are certainly very important considerations, they must be balanced against the primary focus of the program.

Implementing a solution based on low-security supply-chain RFID technology may actually intensify the border security problem. The RFID card favored by DHS can easily be read by unauthorized personnel who can obtain the individual's unique identification number. With this number, anyone who somewhat resembles the legitimate cardholder could then spoof the system to gain entrance to the United States by programming a supply-chain tag to look like a PASS card. No technique is currently available to check the authenticity of a card based on EPC Gen 2 technology electronically. 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 card and its contents, preventing tampering and forgeries.

The DHS EPC Gen 2-based solution also has the potential to require more time and incur increased costs. Because EPC Gen 2 technology is different than the technology used in the new ISO/IEC 14443-based ePassport, a separate reader infrastructure will be required to support travelers who have an ePassport but not a PASS card. And since the EPC Gen 2 cards will not contain the enhanced anti-counterfeiting features contained in the ePassport, additional equipment and time may be needed to verify watermarks or holograms if security is to be maintained.

The requirement for a protective sleeve is also an issue. As drivers are speeding away from the border, they may not always remember to replace the PASS card immediately in its protective sleeve. A cardholder may drive for miles within range of any reader capable of picking up and tracking the information on the card. Some individuals will undoubtedly lose the sleeve. An ISO/IEC 14443-based contactless smart card solution can be implemented that does not require a sleeve to protect the privacy and security of information stored on the PASS card and communicated during the identity verification process.[1]

By using ISO/IEC 14443-based contactless smart card technology in the PASS card and implementing a system flow similar to the one presented above, DHS and the Department of State can enhance the security of our borders without compromising personal privacy or impeding the flow of people crossing the border. Unlike a solution based on EPC Gen 2 technology, the contactless smart card-based solution supports features that can be used to verify the authenticity of the PASS card and eliminate the risk of terrorists, criminals, or illegal aliens who have a passing resemblance to legitimate cardholders spoofing or counterfeiting PASS cards to enter the United States undetected. This solution could also leverage the infrastructure that is being put in place to support the new ePassport.

Conclusion

The Smart Card Alliance, whose members provide both ISO/IEC 14443-based contactless smart card and EPC Gen 2 products, strongly recommends that DHS conduct a trial to evaluate the performance of both EPC Gen 2 and ISO/IEC 14443-based technologies before making a final implementation decision. We believe that a PASS card system designed using ISO/IEC 14443-based contactless technology will fulfill the operational requirement for high throughput while also providing strong security, protecting individual privacy, and leveraging the ePassport infrastructure.

[1] Such a system would use a random identification number generated on the PASS card to register the PASS 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 can be supported by ISO/IEC 14443-based contactless smart cards and readers.

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. Through specific projects such as education programs, market research, advocacy, industry relations, and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the United States and Latin America.

The Smart Card Alliance Identity Council is focused on promoting the need for technologies, legislation, and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud, and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

The Smart Card Alliance wishes to thank Identity Council members who participated in the development of this paper. Contributors included individuals from the following organizations: Anteon, Axalto, Fargo Electronics, Gemplus, Integrated Engineering, Philips Semiconductors, Saflink, Texas Instruments, Visa Canada.

Additional information about the Identity Council and about the use of smart cards for secure identity applications can be found at http://www.smartcardalliance.org.

Glossary

- **Biometric.** A measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
- **Contactless smart card**. A smart card that communicates with a reader through a radio frequency interface.
- **ePassport.** A travel document that contains an integrated circuit chip based on international standard ISO/IEC 14443 and that can securely store and communicate the ePassport holder's personal information to authorized reading devices.
- **EPCglobal.** The not-for-profit organization establishing and supporting "the EPCglobal Network™ as the global standard for real-time, automatic identification of information in the supply chain of any company, anywhere in the world" and "leading the development of industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks." Additional information can be found at http://www.epcglobalinc.org.
- **EPC Generation 2 (EPC Gen 2)**. The specification developed by EPCglobal for the second-generation RFID air-interface protocol. EPC Gen 2 was developed to support supply chain applications (e.g., tracking inventory). The current ratified standard operates in the ultra-high-frequency (UHF) range (860–960 MHz), supports operation at long distances (e.g., 25–30 feet), and has minimal support for security (e.g., static passwords to access or kill information on the RFID device). The specification can be found at: http://www.epcglobalinc.com/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf.
- **ISO/IEC 14443.** The international standard for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz.
- **RFID** (Radio Frequency Identification). Technology that is used to transmit information about objects wirelessly, using radio waves. RFID technology is composed of 2 main pieces: the device that contains the data and the reader that captures such data. The device has a silicon chip and an antenna and the reader also has an antenna. The device is activated when put within range of the reader. The term RFID has been most commonly associated with tags used in supply chain applications in the manufacturing and retail industries.
- **Smart card.** A device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules used in GSM mobile phones, and USB-based tokens.
- **Ultra-high frequency (UHF)**. Radio frequencies in the range of 860–960 MHz.