Smart Card Alliance

The Consequences to Citizen Privacy and National Security in Adopting RFID Technology for Border Crossing Identity Documents

October 2007

Developed by:
Smart Card Alliance Identity Council

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.

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.

The Consequences to Citizen Privacy and National Security in Adopting RFID Technology for Border Crossing Identity Documents

The Department of Homeland Security (DHS) is currently promoting the incorporation of radio frequency identification (RFID) technology in several border crossing documents that will be used to verify the identity of citizens re-entering the United States. The Smart Card Alliance Identity Council developed this white paper to discuss the security, privacy and operational issues with using RFID in human identification systems. The paper provides an overview of the use of RFID for supply chain applications, describes how RFID is proposed to be used in the DHS program, identifies key vulnerabilities with RFID systems that could be exploited, and proposes an alternative secure smart card-based solution for these border crossing identity programs.

RFID in the Supply Chain

Many people reading this white paper will already be familiar with RFID devices. These simple low-cost tag devices are positioned to revolutionize the supply chain by providing up-to-the-minute tracking information about the location of the products to which they are attached. As the RFID tags make their way through the product manufacturing and distribution system, readers at key locations can interrogate the tag and hence follow the associated products' progression. Each tag is created with one mission in mind: to faithfully transmit the tag's unique serial number to the surrounding vicinity each and every time the tag is stimulated by a suitable RF source.

During the design of this simple architecture for RFID tags, there was no need to give significant thought to the security, privacy or confidentiality of the tag's ID number nor was consideration given to what the tag was going to be attached. After all, the tag merely provides basic identification information to a specific tracking system. In order to be meaningful, the back-end system must contain the information which ties each specific tag to information about what it has been attached to and where it is now located.

This is the basis of a fundamental architectural problem if RFID technology is applied to applications outside of its original design.

RFID and Human Identity Applications

Consider the following evolution of an application using the RFID tag system design. This time, the same RFID tag is given to a human for identification purposes. The tag is able to faithfully transmit its unique number each time it is stimulated, in some cases up to a designed distance of 30 feet. An identification system would register the presence of the RFID tag's number and use it to index directly into a central database containing the enrolled identities of the tag holders. By using only the tag's unique number, a corresponding database entry would be accessed which provides some personal identifying information of the tag holder.

This application of RFID tags seems reasonable. Assign a unique tag for each identity; present the tag and the corresponding identity record is retrieved. No actual personal identification information is contained in the storage-restricted tag. Without automation for identity verification, the system will obviously rely on a visual and potentially verbal human verification process between the tag holder presenting the tag and the person attempting to verify identity.

Unfortunately there are several privacy and security shortcomings to this approach. One such vulnerability arising from this technology is directly related to the fundamental RFID card architecture. RFID tags transmit the tag number "in the clear," even if a password is required to read the tag. This exposes the tag number to interception during wireless communications. Once the tag number is intercepted, it is relatively easy to directly associate the number with an individual. This enables tracking an individual surreptitiously. Another privacy issue concerns the ability for an impostor to assume a genuine identity by cloning a person's RFID tag. If this is done, then it is possible to make an entire set of movements posing as somebody else without their knowledge. A further privacy concern is associated with maintaining all of the identity information in a centralized database and assuming the information will remain accessible to only authorized individuals.[1]

RFID Use in Border Crossing Documents: Issues and Vulnerabilities

DHS is currently promoting the use of RFID tags for several citizen identification programs. The Western Hemisphere Travel Initiative (WHTI) passport card (or PASS card), which is being positioned as a land border crossing citizen credential as an alternative to a Department of State issued passport, intends to incorporate RFID technology.[2] A second related program, the emerging enhanced driver's license, is also slated to incorporate the same RFID technology.[3] The DHS claim that RFID technology is secure and reliable continues to influence states to accept the technology, regardless of the risks outlined in this paper.

RFID technology cannot provide the necessary security to protect our borders. The proposed RFID technology does not include appropriate or adequate privacy safeguards for U.S. citizens. RFID technology has been designed for warehouse supply chain and inventory management applications[4] – i.e., tracking pallets, tubes of toothpaste and dog food – not for human identification card applications.[5]

The RFID technology proposed for the enhanced driver's license does not have any security features which protect the transmitted information. Because there is no security designed into the chosen RFID tags, tags can easily be copied and duplicated (as demonstrated recently by the Smart Card Alliance and Secure ID Coalition on Capitol Hill[6]) to create fraudulent driver's licenses and border crossing documents. Adding external paraphernalia to the card (i.e., a protective RF sleeve) will not solve the national security threat that RFID technology poses when used for human identification purposes.

As proposed by DHS, the simple RFID-enabled land border identity cards have many vulnerabilities and will be open to attacks from hackers, identity thieves and possibly even terrorists. Such attacks include skimming, cloning and denial of service. DHS is aware of these potential attacks and corresponding vulnerabilities, but has decided to proceed without addressing them. The DHS objective appears to be the rapid implementation of the WHTI program in accord with their legislative mandate, regardless of the risks to the nation inherent in their technology selection.

There are some further issues in specifying this technology in the current environment.

- Implementing RFID technology would essentially duplicate the reader infrastructure at border entry points. Long-range RFID technology is incompatible with the new ePassport infrastructure being deployed at all U.S. border entry points, adding significant, unnecessary cost to the programs.
- So far there has been limited, if any, practical testing of this technology at the border and, in fact, the one test that was conducted as part of a Government Accountability Office (GAO) review[7] reports numerous performance and reliability problems, including failure of RFID readers to detect a majority of travelers' tags during testing. One possible

[1] Documented cases of database breaches can be found at http://breachalerts.trustedid.com/?cat=191.

[2] DHS, *Fact Sheet: Western Hemisphere Travel Initiative (WHTI) Passport Card Technology Choice: Vicinity RFID*, October 17, 2006 (http://www.dhs.gov/xnews/releases/pr_1161115330477.shtm)

[3] Associated Press, *Washington to Offer Enhanced Driver's License*, March 5, 2007 (http://www.associatedcontent.com/article/190545/washington_to_offer_enhanced_drivers.html)

[4] Intermec, *Supply Chain RFID: How It Works and Why It Pays* (http://epsfiles.intermec.com/eps_files/eps_wp/SupplyChainRFID_wp_web.pdf)

[5] DHS Data Privacy & Integrity Advisory Committee, *The Use of RFID for Human Identity Verification*, December 6, 2006 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf)

[6] A video of the demonstration can be found at http://www.smartcardalliance.org/pages/activities-congressional-briefing-20070718

[7] GAO, *Border Security: US VISIT Program Faces Strategic, Operational and Technological Challenges at Land Ports of Entry*, GAO-07-248, December 2006 (http:// www.gao.gov/new.items/d07248.pdf)

consequence of the inherent unreliability of RFID tag reads is that it will force the DHS Customs and Border Protection (CBP) officer to fall back to visual/manual inspection and use of outdated printed machine reading technologies – adding significant delays to border processing times.

There are several other areas where testing might be expected to reveal issues.

- The lack of strong cryptographic features in the proposed RFID tags makes it impossible to effectively authenticate the enhanced driver's license or passport card. More time will be required by the CBP officer to manually determine the driver's license authenticity using the other security features printed on the card. This will mean that the officer will need to physically touch the card, dramatically increasing the time the officer spends processing each citizen, increasing the queue lengths, and impeding commerce across the border. When queue lengths increase and pressure is placed on the CBP officer to move more quickly, the comparison of the biometric image shown on the officer's workstation with the individual in the car may become perfunctory, allowing someone looking similar to the legitimate citizen to pass the inspection point using a copied driver license.

- Reliance on real-time access to central databases and networks adds additional vulnerability. Networks fail, as they did recently in Los Angeles on August 11, 2007, causing several thousand passengers to be delayed on arrival.[8] Secure storage of biometric and biographic data using reliable smart card technology would provide land border crossing officers an electronically verifiable token that can be used offline. This would eliminate such a network-failure-induced backlog: reliable data would be available from the smart card for the CBP officer to verify the identity of the individual. Cached watch list data could also provide adequate checks until the network returns to operation and the watch lists are updated.

The long range nature of the RFID tag introduces exploitable system vulnerabilities.

- The readers can be rendered useless by a commercially available RFID transceiver that is pointed at the CBP antennas, causing the system to be inoperable. Such a denial of service attack will wreak havoc by slowing the processing of returning citizens, and could facilitate the movement of individuals with forged RFID cards across the border.

- Many car windshields are covered with metallic films to reduce visual glare. This film acts as a shield against the ultra-high-frequency (UHF) radiation used in a long-range RFID system. Vehicles with such sun shields will force the CBP officer to manually enter the driver's license data into the workstation before the watch list data can be consulted.

- UHF radiation is subject to reflections, making it possible to confuse the CBP system. RFID numbers from adjacent vehicle lanes can confuse the system, slowing the work of the CBP officer as they match biographic and biometric data to the citizen in the expected vehicle lane.

Additional attacks are enabled by the vulnerabilities inherent in the RFID technology.

- A denial of service attack is possible by flooding the local reader system with multiple forged cards, all with the same (identical) valid RFID tag number. Manually performed card reads by a CBP officer may pull up the same or different record to add to the confusion.

- A variation of the denial of service attack is also possible by flooding the local system with multiple forged cards, all with valid but different RFID numbers. Again, manual card reads by a CBP officer may pull up the same or different identity records.

[8] Washington Post, *Computer Glitch Causes Delays at LAX*, August 12, 2007 (http://www.washingtonpost.com/wp-dyn/content/article/2007/08/11/AR2007081101502.html?tid=informbox)

- Another subtle attack is the presentation of a single forged card that looks genuine (with printed photo of imposter) and uses a valid (cloned) RFID tag number which points to the record of an enrolled person in the database. If the forged card is presented at the same time as the cards of multiple travelers in the same vehicle, the discrepancy may be overlooked.

Alternative Solution for Secure Border Crossing Documents

There are already several identification card programs in use within the Federal government today that satisfy the tough challenges of enhancing security, protecting privacy and facilitating fast throughput. One only has to look at the implementation of secure RF identification technology in the Department of State's ePassports and FIPS 201 Personal Identity Verification (PIV) cards being issued to Federal employees and contractors for shining examples of how to protect privacy, verify identity, and electronically authenticate the document along with its bearer. The ePassport and PIV card carry the entire identity credential electronically, facilitating offline identity authentication using the ID.

Understanding that DHS has architected a border crossing solution using a passport card with a simple RFID tag number that is linked with the citizen's identity information maintained in a central database, the Smart Card Alliance recommends an alternative secure solution:

> Use an inexpensive ISO/IEC 14443 proximity contactless smart card that supports secure transmission of the tag number during wireless communications. In addition to secure transmission, this secure contactless technology can also be used to electronically authenticate the ID.

Secure contactless smart cards are already widely used in transportation applications such as ticketing, contactless credit and debit cards, and secure physical access applications. These cards do not have to carry the full identity credential, just the database index number (the tag number) as desired by DHS. Yet they are capable of ensuring the confidential communication of the number between card and reader, reducing the risk of cloning and counterfeiting. Being proximity-based (4-inch range), a reader can be mounted by the side of the border crossing lane which will allows the card(s) to be 'tapped' to register the citizen(s) prior to pulling up to the CBP agent. A second benefit of this fully secured transmission capability is the elimination of the RF shielding envelopes that are being proposed to counter the weaknesses of long-range RFID-based vicinity tags (30-foot range).

Conclusion

The Smart Card Alliance is very concerned about a potential backlash and public outcry resulting from citizen identification applications that do not incorporate the necessary security features to protect the identity information and privacy of the cardholder. There is a simple solution to this problem that can avoid citizens from being put at risk. The solution requires using the more sophisticated smart card technology that can incorporate critical security features including shorter read-range of the card, encryption, and electronic authentication of the document, as well as more likely being able to support security technologies specified in the future. Smart card technology would not impede or slow down border crossing applications and would be a valuable aid to the CBP officer in verifying identities. The challenges of reliably reading a number of long-range passive RFID tags that are held within vehicles will make it difficult for DHS to realize the efficiencies assumed for the currently-selected vicinity-read RFID technology.

The Smart Card Alliance strongly recommends that DHS and border states contemplating the issuance of an enhanced driver's license incorporating passport card functionality consider doing so in a pilot using smart card technology. This pilot could use the same database pointer architecture previously defined for the passport card, but use a secure smart card chip to store the unique citizen identifier. Such a pilot would provide a factual basis for comparing the relative operational efficiencies of RFID and smart card technologies in a system that adequately protects citizen privacy and enhances border security.

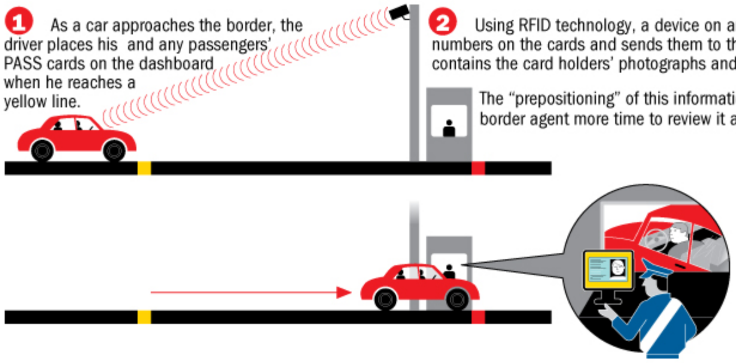
PASS cards: Smart card technology is better than RFID

OVERVIEW

The State Department in conjunction with the Department of Homeland Security is developing PASS cards–a new way for Americans to re-enter the United States from Canada and Mexico.

The purpose is to increase security at the borders, where currently all you need is a driver's license. PASS cards are intended to be a lower cost alternative to passports.

HERE'S ONE PROPOSAL: USING INSECURE RFID TAGS



1 As a car approaches the border, the driver places his and any passengers' PASS cards on the dashboard when he reaches a yellow line.

2 Using RFID technology, a device on an overhead gantry 30 feet away reads the numbers on the cards and sends them to the DHS central database. The database contains the card holders' photographs and information about their identities.

The "prepositioning" of this information will give the border agent more time to review it and make decisions.

3 The car moves on to the red line where a border official sees that the driver and passengers match the photos received from DHS servers.

PROBLEMS WITH THE RFID METHOD

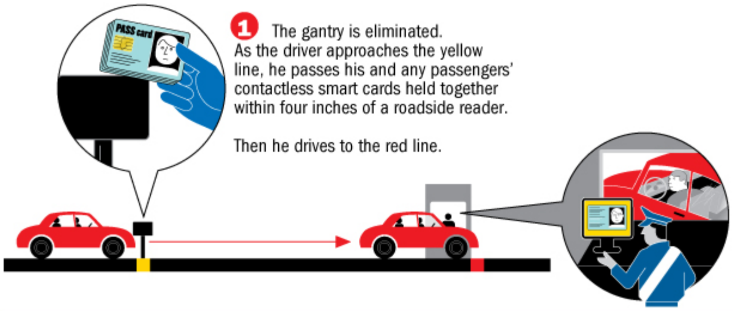
Because RFID technology is designed for product tracking, it is not a technology that protects people's identities...

● ...it's not secure
Anyone (with an RFID reader) within 30 feet of the traveler can read the card and clone it.

● ...there are privacy issues
Anyone with a PASS card can easily be identified as an American.

● ...it won't speed up traffic flow
The PASS card is not like a toll collector tag for your car, where you just roll through; here, all drivers must stop for a visual verification.

A BETTER METHOD: SECURE SMART CARDS



1 The gantry is eliminated. As the driver approaches the yellow line, he passes his and any passengers' contactless smart cards held together within four inches of a roadside reader.

Then he drives to the red line.

2 At the red line, the border official checks the prepositioned data on his computer screen to verify the driver's and passengers' identities.

No one other than the border official can read the cards because the information sent from the smart cards is encrypted.

ADVANTAGES WITH THE SMART CARD METHOD

Because a contactless smart card is **a small computer** with 100s of built-in security features that protect the information in it...

● ...it's secure
The card encrypts all communications, has a short read range of four inches, and only transmits to a validated reader.

● ...it protects privacy
No unauthorized person can "read" the information on the card preserving the citizens' privacy.

● ...it's just as fast
Information can be prepositioned in the same way as with insecure RFID tags.

Smart Card Alliance

For additional information, visit:

www.smartcardalliance.org