Smart Card Alliance

Questions and Answers about the Proposed Use of RFID for U.S. Border Crossing Documents

November 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.

Questions and Answers about the
Proposed Use of RFID for U.S. Border Crossing Identity Documents

The Department of Homeland Security (DHS) is currently promoting the incorporation of RFID tags for several citizen identification programs. The Western Hemisphere Travel Initiative (WHTI) passport 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. A second, related program, the emerging enhanced driver's license, is also slated to incorporate the same RFID technology.

Below are some frequently asked questions about the use of RFID technology for human identity verification and for the border crossing identity programs being considered by DHS.

1. What are Radio Frequency Identification (RFID) devices?

These simple low-cost tag devices were created to revolutionize the supply chain by providing up-to-the-minute tracking information about the location of the products to which they are attached. 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.

2. How would RFID work for human identity verification?

An RFID tag, containing a randomly selected unique number, would be provided to each person. When the tag is presented, it would transmit its unique number to a central identity system where the corresponding identity record is retrieved from a central database. Since the RFID-based system has no automated form of identity verification, the system will need to rely on a visual and potentially verbal human verification process between the tag holder presenting the tag and the person attempting to verify identity.

3. Can RFID tags be tracked?

Yes. RFID tags were created to "track" packages. As the 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. The same would be true for tracking a person carrying an RFID-based identity card. During the design of the RFID architecture used for supply chain applications, 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 the implications of attaching such a tag to a person instead of a product.

4. Can RFID tag numbers be intercepted?

Yes. The fundamental RFID system architecture specifies transmission of the tag number "in the clear," even if a password is required to read the tag. This exposes the tag number to interception during the wireless communications. Once the tag number is intercepted, it would be relatively easy to directly associate the number with an individual and to subsequently track an individual's movements surreptitiously.

5. Is information transmitted securely with RFID?

No. RFID technology does not have security features which protect transmitted information. RFID tags transmit the tag number "in the clear," even if a password is required to read the tag. Because there is no security designed into existing standards governing RFID tags, tags can easily be skimmed and duplicated to create fraudulent identity documents.

6. Can RFID tags be cloned?

Yes. RFID tags can be read and then easily written to another tag. In a human identification system, an imposter could 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. This is fundamentally identity theft, enabling fraudulent use of an otherwise legitimate citizen's identity.

7. With the proposed RFID-based passport card and enhanced driver's license, is personal information stored in a central database? Who has access to this information?

Yes. All the identity information would be maintained within centralized databases. DHS and/or other issuing organizations would define the policies for who has access to the information.

8. What are the risks of relying on central databases and/or networks?

Reliance on real-time access to central databases and networks will have very undesirable consequences in the event of infrastructure failures. Networks fail, as they did recently in Los Angeles on August 11, 2007, causing several thousand passengers to be delayed on arrival. The same failure could occur with the DHS systems used in verifying identities at border crossings, creating significant delays for citizens and commerce.

An alternative approach is to have biometric and biographic data available electronically on the identity document so that it is available locally. In the case of land border crossings, an offline electronically verifiable token would eliminate backlogs caused by network or database failures and ensure reliable data would be available for the Customs and Border Protection (CBP) officer to verify the identity of the individual. Cached watch list data could also be used to provide adequate checks until the network returned to operation and the watch lists were updated.

9. Would identity verification using the proposed RFID identity documents in the WHTI and enhanced driver's license programs require visual confirmation also?

Yes. The lack of strong cryptographic features in the RFID technology specification makes it impossible to electronically authenticate the RFID identification document. This will require that the CBP officer 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, pressure may be either placed explicitly on the CBP officer to move more quickly or self-imposed by the officer. In this case, the check 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 identification document.

10. DHS says that a protective sleeve will provide security for the RFID cards. Is this the case?

A radio-frequency opaque sleeve would prevent the transmission of the tag data; however this would only be masking a dangerous flaw and putting the onus on citizens, not the government, to protect their privacy and security. Adding external paraphernalia to the card (i.e., a protective RF sleeve) will add cost and increase the size of the RFID cards, but does not solve the national security threat that RFID technology poses when used for human identification purposes.

11. Do the proposed RFID-based WHTI passport cards and enhanced driver's licenses capitalize on the border crossing infrastructure already in place to support the new ePassport?

No. Implementing RFID technology would require duplicate reader infrastructures 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.

12. Has the RFID technology proposed for the WHTI passport card and enhanced driver's license been tested for use at the borders?

There has only 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 reports numerous performance and reliability problems with RFID, including failure of RFID readers to detect a majority of travelers' tags during testing.

13. Will the RFID-based passport cards and enhanced driver's licenses make border crossing faster and easier?

No. The lack of strong cryptographic features in the proposed RFID tags makes it impossible to effectively authenticate the identity document. More time will be required by the CBP officer to manually determine the authenticity of the identity document using 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. Citizens traveling in vehicles with ePassports will require separate lanes and vehicles with multiple passengers carrying mixed types of credentials can not be processed efficiently -- potentially making lines longer and the whole border crossing process more frustrating for citizens.

14. Is the proposed RFID-based system vulnerable to denial of service attack?

Yes. There are several ways a denial of service attack could occur. First, 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. Second, 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. Third, 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. Finally, a fundamental attack perpetrating identity theft is the presentation of a single forged card that looks genuine (e.g., 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.

15. The proposed RFID-based system will be reading tag numbers from hundreds of vehicles at border crossing points simultaneously. Will this work?

While the long-range RFID technology being proposed for these border crossing programs is successfully used in tracking hundreds of items in supply chain applications, reading and tracking tags in moving vehicles is a very different, and difficult, application. For example, 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. Also, UHF radiation is subject to reflections, making it possible to confuse the CBP system. RFID tag numbers read 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.

16. Is RFID a less expensive solution for identity documents?

No. There is a range of inexpensive ISO/IEC 14443 proximity contactless smart cards that support suitable security capabilities which can ensure the secure transmission of the same ID number during wireless communications and can also serve to electronically authenticate the ID. Proximity contactless smart cards are already widely used in secure payment and physical access applications. This technology could easily support DHS border crossing requirements of storing a simple tag number that is linked with the citizen's identity information in a central database.

17. Is there an identity technology that does address security and privacy concerns?

Yes. There are already several identification card programs 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 use proximity contactless smart card technology to carry the entire credential electronically facilitating offline identity authentication using the ID.