Department of Homeland Security and State Pilots for Enhanced Driver's Licenses: Concerns about Privacy, Security and Operational Impact of Technology Selection

Statement prepared by the Smart Card Alliance, August 2007

The U.S. Department of Homeland Security (DHS) and several states including Arizona, Vermont and Washington, have recently announced programs to develop and issue enhanced state driver's licenses that could be used as acceptable alternative documents for crossing the United States' land and sea borders. The Smart Card Alliance has serious privacy and security concerns for U.S. citizens participating in these programs based on the direction DHS has been recommending for the enhanced driver's license technology.

The Smart Card Alliance applauds state efforts to boost security at borders while facilitating trade and tourism; however, the Alliance also believes that ensuring the privacy and security of U.S. citizens is a primary requirement and that the technology choice for an enhanced driver's license must also address this critical requirement.

The Smart Card Alliance, a not-for-profit, multi-industry association, is in a good position to be objective on the merits of different technologies under consideration for border crossing cards because its members provide both the technology favored by DHS, long-range radio frequency identification (RFID) products, and the more secure and privacy-sensitive products the Alliance recommend for enhanced driver's license programs, secure RF contactless smart cards. Even as manufacturers of RFID, the Alliance attests to the fact that long-range RFID, the most likely technology to be selected by DHS, is an inappropriate technology for human identity documents.

Within the WHTI specification and in the Washington and Arizona enhanced driver's license projects, DHS has proposed a long-range vicinity-read RFID technology solution. This proposal raised serious privacy, security, and operational functionality issues among industry experts in responses to the Department of State's Federal Register Notice for the WHTI passport card. Industry concerns include:

- The lack of strong cryptographic features in long-range RFID-based cards, making it easy for criminals to read the unprotected, static citizen identifiers from the cards and create fraudulent documents.
- The reliance on real-time access to central databases and networks in order to verify every individual's identity, leading to vulnerabilities to infrastructure failures and attacks or to network and system security breaches.
- The challenges of reliably reading large numbers of long-range RFID tags at crowded border crossing points, making it unlikely that desired operational efficiencies will be achieved.
- The ability for criminals to use inexpensive long-range RFID readers to detect the citizen's electronic identity from a distance, putting U.S. citizens carrying the enhanced driver's license at risk of having their movements tracked.

The full Smart Card Alliance response to the Department of State Federal Register Notice for the WHTI passport card is available at http://www.smartcardalliance.org.

In addition, recent U.S. Government Accountability Office (GAO) reports have identified both performance and security issues with the DHS implementation of the US-VISIT program, which uses the same long-range RFID technology and architecture that has been proposed for WHTI-compliant documents.

- In the report *Border Security: US-VISIT Program Faces Strategic, Operational and Technological Challenges at Land Ports of Entry* (GAO-07-248), GAO reviewed DHS' use of long-range vicinity-read RFID technology in the US-VISIT program. The report stated: "US-VISIT's initial testing and analysis of this has identified numerous performance and reliability problems, such as the failure of

RFID readers to detect a majority of travelers' tags during testing." In US-VISIT program tests at five ports of entry, successful read rates were low at four of the five (in one instance as low as 14 percent).

- In the report *Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program* (GAO-07-870), GAO points out many flaws in the DHS implementation of the US-VISIT program's use of databases to manage sensitive, personally identifiable information. The GAO report stated: "These weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including personally identifiable information, and disrupt the operations of the US-VISIT program. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These risks are not confined to US-VISIT information. The CBP mainframe and network resources that support US-VISIT also support other programs and systems. As a result, the vulnerabilities identified in this report could expose the information and information systems of the other programs to the same increased risks."

These reports illustrate the risks that state programs will face if DHS proposes to use the same technology and architecture for the enhanced driver's license.

The only broadly-deployed, proven technology existing today that meets 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.

- Smart card technology is being widely used in identity management applications globally to enable strong identity assertion and to protect the identity document holder's privacy.
- Smart card technology uses cryptographic techniques that would ensure that the enhanced driver's license is authentic, prevent tampering and forgeries, and allow for encryption of any personal information.
- The adoption of smart card technology for the enhanced driver's license would also support interoperability with other federal identity management initiatives including smart card use by First Responders nationwide to facilitate emergency access to disaster sites, the new Personal Identity Verification (PIV) card being issued to all federal employees and contractors in response to Homeland Security Presidential Directive 12, the Department of Defense Common Access Card, and the new State Department-issued ePassport.

DHS has repeatedly defended the choice of long-range RFID technology by saying that it will move people through the border points faster. The Smart Card Alliance disagrees with this position. There are inherent wait times in the border crossing process that allow enough time to read a smart card chip in a passport card, enhanced driver's license or ePassport prior to reaching the document checkpoint. An enhanced driver's license based on 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, which is now being issued to millions of U.S. citizens.

The Smart Card Alliance is committed to advocating technologies that are appropriate for different identity applications. RFID technology was designed for automating the tracking of products and pallets through a supply chain, not for validating human identities. The Alliance urges states that are considering enhanced driver's licenses programs to challenge the DHS-selected technology and consider contactless smart card technology to achieve a faster, more secure means for citizens to cross our borders from land and sea, while still protecting their security and privacy.

Additional information about the use of RFID and secure contactless smart card technology in identity applications can be found at http://www.smartcardalliance.org.

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.