The REAL ID Act: Why Real ID Cards Should Be Based on Smart Card Technology

July, 2006

Developed by:
Smart Card Alliance Identity Council

The REAL ID Act: Why Real ID Cards Should be Based on Smart Card Technology

This paper provides support for the use of smart card technology to implement state driver's licenses issued to comply with the requirements of the REAL ID Act of 2005, which was passed to improve the security of state-issued driver's licenses and personal identification cards.

Background

In the United States, driver's licenses are issued by individual states. States also issue identification cards for use by non-drivers. States set the rules for what data is on a license or card and what documents must be provided to obtain a license or card. States also maintain databases of licensed drivers and cardholders.

The REAL ID Act of 2005 stipulates that after May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements" specified in the REAL ID Act.

The Act includes the following requirements:

- A driver's license or identification card must include certain specific information and features.
- A driver's license or identification card cannot be issued unless certain specific documentation is presented.
- The state must verify all documentation presented with an application.
- Driver's licenses or identification cards issued to persons who are present in the United States only temporarily can be valid only for the amount of time for which the persons are authorized to be in the United States.
- Controls and processes must be established to ensure the security of the issuance process.
- Each state must maintain a motor vehicle database and provide all other states with electronic access to the database.

The REAL ID Act also stipulates that the technology incorporated into the driver's license or identification card must meet the following requirements:

- It must support physical security features designed to prevent tampering, counterfeiting, or duplication of the credential for fraudulent purposes.
- It must be a common, machine-readable technology, with defined minimum data elements.

The Department of Homeland Security has the authority to issue regulations and set standards for compliance with the REAL ID Act.

Smart Card Technology and Identity Applications

Smart card technology is currently recognized as the most appropriate technology for identity applications that must meet certain critical security requirements, including:

- Authenticating the bearer of an identity credential when used in conjunction with personal identification numbers (PINs) or biometric technologies
- Protecting privacy
- Increasing the security of an identity credential
- Implementing identity management controls

The following active Federal government programs currently use smart card technology:

- The Federal employee and contractor Personal Identity Verification (PIV) card

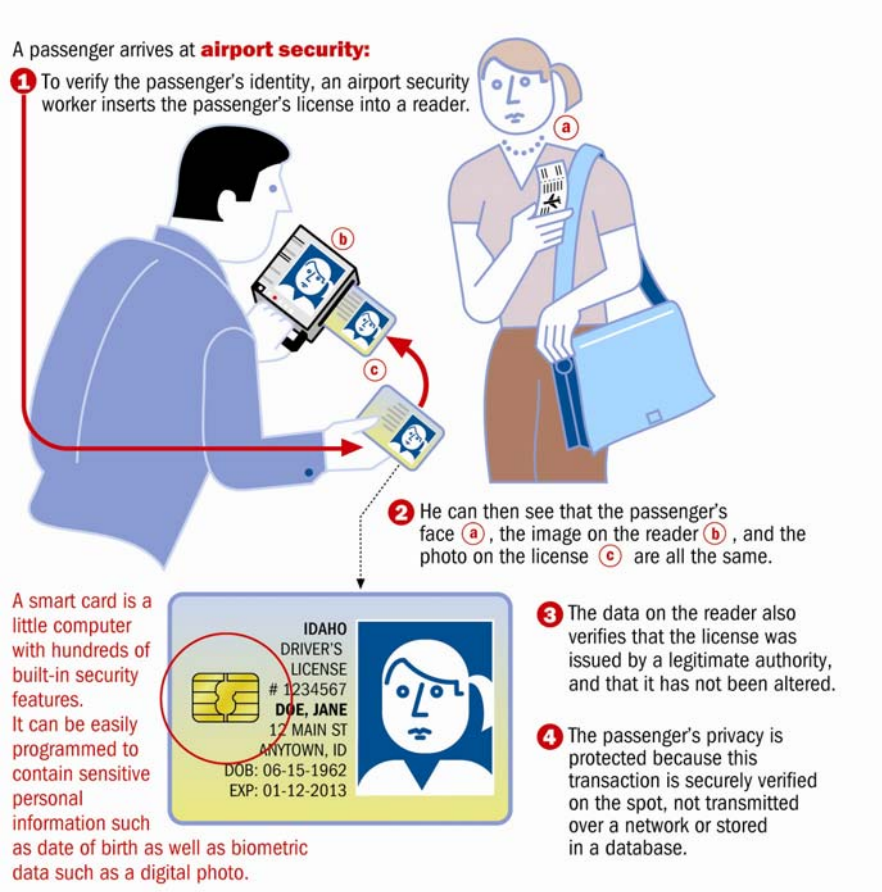
- The new United States ePassport
- The Department of Homeland Security (DHS) Registered Traveler program
- The DHS Transportation Workers Identification Credential (TWIC) program
- The DHS First Responders Access Credential (FRAC) pilot program implemented in the National Capitol region

Countries around the world (such as Germany, France, Malaysia, and Hong Kong) use smart cards for secure identity, payment, and healthcare applications. In addition, public corporations (including Microsoft, Sun Microsystems, Chevron, and Boeing) use smart employee ID cards to secure access to physical facilities and computer systems and networks.

In response to Homeland Security Presidential Directive-12, the National Institute of Standards and Technology (NIST) has published the Federal Information Processing Standard 201 (FIPS 201), providing specifications for an interoperable Federal PIV card. The standard calls for a combined contact/contactless smart card that can authenticate the cardholder for both physical and logical access. The FIPS 201 standard not only applies to Federal employee and contractor IDs; it is also being used to specify the underlying requirements for the TWIC, Registered Traveler and FRAC credentials.

States could incorporate the same proven PIV card technology into a state-issued Real ID (i.e., a driver's license or identification card issued to comply with the REAL ID Act). The PIV-based Real ID could then be used to authenticate the bearer in a "federal" situation, such as checking in at an airport (Figure 1). This Real ID card could also incorporate biometric factors (such as a facial image or fingerprint template) to help verify the cardholder's identity.

Figure 1: Using a Smart-Card-Based Real ID for Airport Check-in



States that want to issue a Real ID card that uses the FIPS 201 standard would need to incorporate smart card technology into the card. However, the states would not necessarily have to deploy any significant new infrastructure to use the smart card features. Each state individually could decide whether and how to use the personal identity verification applications in situations unrelated to Federal use.

Examples of how state divisions of motor vehicles (DMVs) and law enforcement agencies could use and benefit from the use of smart cards are listed below. These and other applications could be phased in over time as the opportunity and economics of the applications evolve for each state.

- **Driver's license renewal**. Renewal of driver's licenses could be expedited by an applicant coming to a DMV office or kiosk, inserting the smart card and getting a new card automatically.
- **Driving privileges**. A DMV could revoke driving privileges for various infractions (for example, DUI, tickets) and still allow the individual to use the card for identification purposes.
- **Ticketing.** Law enforcement officers could issue tickets by reading the smart card chip and getting all driver demographic data from the card automatically.
- **Driver histories.** Driver history could be kept on the card enabling improved safety on highways where access to backend systems may not be available.

The Benefits of Smart Card Technology

Unlike alternative, less secure ID card technologies (such as magnetic stripe, printed bar code, optical, or RFID), smart card technology supports numerous unique features that can strengthen the security and privacy of any ID system.

Strong Identity Authentication. One essential characteristic of a secure ID system is the ability to link the individual possessing an identity document securely to the document, thus providing strong authentication of the individual's identity. Smart card technology supports PINs, biometric factors, and visual identity verification. For example, the REAL ID Act requires that each person applying for a driver's license or identification card be subjected to a facial image capture. This facial biometric factor can be stored directly in the secure chip in the smart card and used to verify that the individual presenting the card is the individual to whom the card was issued.

If states want to implement other biometric factors (for example, fingerprints), the biometric that is captured when the cardholder applies for the card (or is enrolled in the identification system) can be stored securely on the card. It can then be matched either on or off the card (in a reader or against a database) to verify the cardholder's identity. In addition, states can establish databases to achieve the goal of "one credential, one record, and one identity."

Strong Credential Security. Protecting the privacy, authenticity, and integrity of the data encoded on an ID is a primary requirement for a secure ID card. Smart cards support the encryption of sensitive data, both on the credential and during communications with an external reader. Digital signatures can be used to ensure data integrity and authenticate both the card and the credentials on the card, with multiple signatures required if different authorities create the data. To ensure privacy, applications and data must be designed to prevent information sharing.

Strong Card Security. When compared to other tamper-resistant ID cards, smart cards represent the best balance between security and cost. When used with technologies such as public key cryptography and biometrics, smart cards are almost impossible to duplicate or forge. Data stored in the chip cannot be modified without proper authorization (a password, biometric template, or cryptographic access key).

Smart cards also help deter counterfeiting and thwart tampering. Smart cards include a wide variety of hardware and software capabilities that can be used to detect and react to tampering attempts and counter possible attacks. When smart ID cards will also be used for manual identity verification, visual security features can be added to a smart card body.

Adding a smart card chip to a Real ID would exponentially increase the difficulty of making a fraudulent ID card. The vulnerabilities of printed plastic ID cards are well known—fake state IDs are readily available for purchase over the Internet or in rogue ID card facilities. Smart cards deter forgers and can ensure that only the person to whom the card is issued will be able to verify themselves when the card is presented. No other technology can offer such secure, trusted, and cost-effective identification capabilities.

Strong Support for Privacy. The use of smart cards strengthens the ability of a system to protect individual privacy. Unlike other identification technologies, smart cards can implement a personal firewall for an individual's data, releasing only the information required and only when it is required. The card's unique ability to verify the authority of the information requestor and the card's strong security at both the card and data level make smart cards an excellent guardian of a cardholder's personal information. Unlike other forms of identification (such as a printed driver's license), a smart card does not reveal all of an individual's personal information (including potentially irrelevant information) when it is presented. Information embedded on the chip can be protected so that it cannot be surreptitiously scanned or skimmed, or otherwise obtained without the knowledge of the user. Personal information stored on the smart card can be accessed only through user-presented PINs and passwords or by biometric matches at the place of use. By allowing authorized, authenticated access to only the information required for a transaction, a smart card-based ID system can protect an individual's privacy while ensuring that the individual is properly identified.

Flexibility as a Secure Multi-Use Credential. The driver's license is currently a multi-use credential. It not only indicates that the cardholder has driving privileges, it also serves as the default credential for establishing that the cardholder can board an aircraft, engage in age-related retail purchases, establish banking relationships, complete retail point-of-sale transactions, and apply for employment. Smart card technology can support these current uses along with any additional applications that enhance citizen convenience and/or government service efficiency. For example, smart cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This capability can generate significant savings for states. A smart card-based driver's license or ID card could not only indicate privileges and allow physical access to services, it could also allow individuals to file taxes, request official papers (e.g., birth certificates) online, or access secure networks. Multiple applications (with their required data elements) can be stored securely on the smart ID card at issuance or added after the card is issued, allowing functionality to be added over the life of the driver's license or ID card.

Standards-Based Technology. Smart card technology is based on mature international standards (ISO/IEC 7816 for contact smart cards and ISO/IEC 14443 for contactless smart cards). Cards complying with standards are developed commercially and have an established market presence. Multiple vendors can supply the standards-based components necessary to implement a smart card-based ID system, providing buyers with interoperable equipment and technology at competitive prices.

Cost-Effective and Flexible Offline Verification. In addition to the privacy and security benefits afforded by smart cards, the technology also delivers features that support cost-effective offline verification and efficient use of the ID card once the card has been issued.

Verification of a cardholder's identity is often required at multiple locations or at points that do not have online connections. A smart card-based ID system can be deployed cost-effectively at multiple locations by using small, secure, and low-cost portable readers that take advantage of the smart card's ability to provide offline identity verification. For example, verifying a cardholder's identity with biometrics would not require access to an online database: the smart card can securely hold the necessary biometric identifier, with the secure chip on the card comparing it to the live biometric. The credential on a card can be authenticated by a reader using digital signatures contained on the ID card, making it a trusted credential—online or off.

One key issue that has been raised by different states and by the American Association of Motor Vehicle Administrators (AAMVA) is the cost of smart card technology. While a smart ID card or driver's license may cost a little more than a plastic card, the cost of the card itself is a small fraction of the total cost of implementing an identity system that complies with the REAL ID Act. When considering costs, it is important to understand the advantage of an ID that is strongly tied to the bearer and enforces citizen privacy. By incorporating smart card technology into a Real ID, states can place a portable security agent in the hands of the cardholder, ensuring that the state's security policy is enforced and that only an authorized cardholder can be authenticated before specific identity information is released. Any additional costs associated with the technology are a small price to pay for such robust security. Moreover, the ability of smart card technology to support additional applications can generate both cost savings and potential new revenue sources. In addition, smart card technology is flexible. Unlike today's printed plastic cards, smart cards can be updated and managed throughout the life of the card.

Conclusion

The Smart Card Alliance strongly recommends that smart card technology be adopted as the underlying infrastructure for state driver's licenses issued to comply with the requirements of the REAL ID Act of 2005. Smart cards have been proven to be the most cost effective and secure identity authentication and verification technology. They are already widely used for secure identification in both the public and private sectors, are based on international standards, can provide all of the features required to meet the security requirements of the REAL ID Act, and can deliver strong privacy protection for the cardholder's personal information. Once states have adopted smart card identification technology, they can then decide whether to use the trusted Real ID credential for other applications beyond the Federal points of use according to their needs, budgets, and timeframes. Failure to embrace smart card technology will undermine the fundamental goal of the REAL ID Act—ensuring that the Real ID is not fake and that it is being used by the intended bearer.

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: Gemalto, Identification Technology Partners, Integrated Engineering, nCryptone, Philips Semiconductors, Saflink, Texas Instruments, Unisys, Viisage, Visa Canada. The Smart Card Alliance also thanks Gemalto for contributing the airport check-in illustration.

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.