COMMENTS OF THE SMART CARD ALLIANCE TO THE DEPARTMENT OF HOMELAND SECURITY FEDERAL REGISTER NOTICE:

"MINIMUM STANDARDS FOR DRIVER'S LICENSES AND IDENTIFICATION CARDS ACCEPTABLE BY FEDERAL AGENCIES FOR OFFICIAL PURPOSES; PROPOSED RULE," 6 CFR PART 37, RIN 1400-AC22

Docket No: DHS-2006-0030

May 7, 2007

The Smart Card Alliance is hereby submitting comprehensive comments in response to the Department of Homeland Security (DHS) Notice of Proposed Rulemaking (NPRM) for REAL ID driver's licenses and identification cards [REAL ID NPRM] (6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Proposed Rule).

The purpose of the REAL ID Act of 2005 is to provide a trustworthy driver's license or identification card issued by States whose purpose:

> "includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine."

The REAL ID Act emphasis is also on the application, proofing and vetting of the individual's identity, and the authentication of the individual's documented credentials.

The actual REAL ID document is required among other things to support:

> "(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
> (9) A common machine-readable technology, with defined minimum data elements."

It is the opinion of the Smart Card Alliance that the published DHS REAL ID NPRM fails to adequately address (8) and (9) above, by:

- Providing weak document security by using only printed security features and selecting a static technology (PDF-417 2-dimensional bar code) which will lead to counterfeiting and fraudulent card creation;
- Providing no linkage of the bearer of the card to the card itself by relying on authentication of the bearer by human inspection of visual card components only;
- Providing no ability to secure the information stored in the machine-readable technology (MRT) and protect citizen privacy;

and therefore will not meet the purpose and intent of the REAL ID Act of 2005.

In addition, the REAL ID NPRM:

- Fails to consider other national and international standards for identity documents that have already addressed the need for strong document security and protection of citizen privacy.
- Incorrectly dismisses smart card technology from consideration by states and mis-states its applicability to a REAL ID driver's license or identification card.
- Does not consider how smart card technology provides a cost-effective solution for REAL ID driver's licenses and identification cards that not only improves privacy and security, but also allows states to leverage their significant investment in REAL ID documents and processes for other identification programs and government applications.

The Smart Card Alliance supports driver's license reform and DHS efforts to specify processes and technologies to meet the requirements of the REAL ID Act. However, the REAL ID NPRM falls woefully short in its specification of the common MRT to be used by all states. 2D bar code technology is inadequate to meet the security and privacy requirements mandated by the REAL ID Act and is not consistent with international and U.S. standards that have been set for secure identity documents. The selection of an antiquated, insecure technology for the next generation of driver's licenses is also short-sighted in not recognizing the opportunity that this affords for states to issue driver's licenses that can be used for identity verification for other government applications.

The Smart Card Alliance recommends that DHS reconsider the MRT chosen for REAL ID driver's licenses and identification cards and specify smart card technology as the common MRT to be implemented in all REAL ID documents. The same smart card technologies that have been chosen to improve and protect the identity documents used in a wide range of Federal and international identity applications should be used to secure the federally-mandated REAL ID driver's licenses and identification cards that citizens will be required to use (and almost certainly pay for) if they are to gain access to the locations and services restricted by the REAL ID Act. Smart card technology is cost-effective and proven, can meet the security requirements of the REAL ID Act, and can protect the privacy of citizens' personal information. In addition, smart card technology offers states a technology platform that provides the flexibility for REAL ID driver's licenses and identification cards to respond to future opportunities.

The incorporation of smart card technology into REAL ID driver's licenses and identification cards makes the REAL ID document a valuable citizen identity credential within our demanding information society. Having an electronic identity verification device in the hands of all citizens can enable a host of applications that presently lack a trusted identity authentication credential. The Federal Trade Commission (FTC) recently released a strategic plan for better authentication in our society as a countermeasure to identity theft. A smart card-based REAL ID credential is the most appropriate platform to significantly improve the trust and reliability of identity in our society. A trusted federally-specified, state government-issued citizen electronic identity credential would also form the foundation to stimulate e-commerce and e-government applications in our society.

DETAILED SMART CARD ALLIANCE COMMENTS

1. The REAL ID NPRM provides weak document security by using only printed security features and selecting a static technology (PDF-417 2-dimensional bar code) which will lead to counterfeiting and fraudulent card creation.

The NPRM recommends the use of printed security features and PDF-417 2-dimensional (2D) bar codes to provide electronically readable features to enable automated scanning, verification and privilege decisions (Section II.H.8). The NPRM fails to recognize the weaknesses of relying solely on static physical card features and their inability to deter fraud and counterfeiting. Special considerations should be placed on static printed media to protect the media from threats such as forgery, counterfeiting, alteration, and cloning.

The Document Security Alliance[1] published a paper titled "Visual Security For Government Credentialing," dated March 31, 2005. This comprehensive paper defines over fifty security features that can be used in combination to provide document security. It recommends a comprehensive approach using at least four security features: two overt, one embedded in card substrate material, and one fused to an overlaminate material.

In the considered opinion of the Smart Card Alliance, this concept of layered security features is necessary and should be required by DHS. These security features increase cost, but the REAL ID driver's licenses and identification cards represent high value targets for forgery, counterfeiting, alteration and cloning. These visual features must also be considered in concert with appropriate electrical features (e.g., smart card chips, cryptographic checksums, digital watermarking) to significantly reduce the risk of fraud.

Federal Information Processing Standard 201 (FIPS 201): Personal Identity Verification (PIV) of Federal Employees and Contractors and the International Civil Aviation Organization (ICAO) standard, Document 9303 Machine Readable Travel Documents (MRTD), both carry an additional requirement that we recommend for REAL ID driver's licenses and identification cards. All data printed on the surface of the card should be electronically stored in a smart card chip within the credential. This data should be digitally signed by the issuer. This provides a significant deterrent to forgery and alteration that is verifiable. Using this approach, the verification model of REAL ID driver's license or identification card becomes:

- Look at printed features visually.
- Read data from the chip.
- Verify signatures to confirm the issuer certifies that the data is correct.
- Show the data electronically and compare the data to the printed features.
- Verify that the bearer matches the electronic and printed document information.

This robust method enables various levels of authentication and verification to suit the needs of the REAL ID Act.

Machine-Readable Technology

The REAL ID Act of 2005 requires a machine-readable technology (MRT) to be incorporated on the REAL ID driver's license or identification card. The REAL ID NPRM discusses the purpose of the MRT to provide automated reading of some data elements of a REAL ID driver's license or identification card for law enforcement purposes. As a potential solution, the REAL ID NPRM specifies a static printed PDF-417 2D bar code as the medium for the machine-readable technology.

By using PDF-417 2D bar codes with static codes printed on the surface of a plastic card, REAL ID documents would have a number of critical vulnerabilities:

1. Once obtained, the PDF-417 2D bar code can be readily photocopied, duplicated, collected and distributed.
2. The PDF-417 2D bar code can be substituted on a REAL ID driver's license or identification card with little difficulty by overlaying a replacement bar code over the original. If this substitution goes undetected, any machine read will produce information that does not correspond to the visual information and may result in incorrect authentication checks or issuance of incorrect renewed licenses.
3. Any encryption used to scramble the data contained in the printed bar code is subject to a brute force attack. This means that interested parties or hackers can try extensive methods to decrypt the information at their leisure once the bar code has been obtained. Any use of a common cryptographic key to perform encryption across REAL ID

[1] Document Security Alliance website is http://www.documentsecurityalliance.com

documents will quickly be discovered, rendering the encryption of the 2D bar code ineffective for the life of all of the credentials.

Bar codes do not raise the bar for security or privacy for REAL ID driver's licenses and identification cards. On the basis of the above discussion, the Smart Card Alliance does not agree with the REAL ID NPRM proposal to use a static, printed PDF-417 2D bar code (or any printed codes) for machine readability. There is insufficient security provided by printed information for it to be a serious contender for protecting the security of information and the privacy of citizens. We strongly recommend the incorporation of smart card-based chip technology into all REAL ID credentials to address the challenges of the MRT.

2. The REAL ID NPRM provides no ability to secure the information stored in the machine-readable technology (MRT) and protect citizen privacy

The privacy of a citizen's personal information endures only as long as security protections are in place to prevent access to, or tampering with, that information.

DHS, in recommending the PDF-417 2D bar code, which can be read by a standard 2D bar code scanner[2], is allowing access to all of the personal information encoded in the machine-readable zone (MRZ) of the REAL ID driver's licenses or identification card [Section II.H.8].

That personal information will include (as noted in the 2005 AAMVA Driver's License/Identification Card Design Specifications[3] for mandatory data elements) name, address, date of birth, eye color, height, and sex. Anyone reading the MRT will have access to all of this personal information, even if they are only looking for proof of age. In addition, the AAMVA specifications also allow for optional data elements in the MRZ to include weight and ethnicity.

As a solution to this potential invasion of privacy, the Smart Card Alliance recommends the use of smart card technology which would allow for the segregation of data elements, thus allowing a merchant to read the age of the card holder without revealing any additional information. Using driver's licenses as a proof of age credential is common practice today and most likely will continue in the future.

In Section II.H.9, DHS notes that Annex D of the AAMVA standard requires "that all of the data on the 2D bar code be unencrypted." As 2D bar codes are a static visible technology, the personal information of the card holder is vulnerable to skimming or substitution by unauthorized users. Encryption of the printed bar code will not alleviate this vulnerability as the information is static and therefore susceptible to a brute force attack. As noted earlier, the privacy of personal information relies on the security protections in place.

Smart card technology is currently recognized as the most appropriate technology for identity applications where personal information resides in a credential. Strong credential security is a key element in protecting the privacy of citizens holding a REAL ID driver's license or identification card, and smart cards offer the following security protections:

- Smart cards support the encryption of sensitive data, both on the credential and during communications with an external reader.
- Smart cards support digital signatures which can be used to ensure data integrity, authenticate both the card and the information on the card, and authenticate that the reader attempting to access information is authorized to do so.
- Smart cards support multiple digital signatures required if different authorities create data stored on the card.
- Smart cards support such technologies as public key cryptography and biometrics.

Thus, issuing "smart" REAL ID driver's licenses and identification cards with all of these security protections will ensure the privacy of citizens nationwide.

---

[2] 72 Fed. Reg. 10,837-8 (March 9, 2007).

[3] D.12.3.1 Minimum mandatory data elements (2005)

Smart Implementation Scenarios

A balance between machine readability for law enforcement and protecting citizen privacy from commercial entities exploiting the MRT is the crux of the issue at hand.

Limiting the MRT to access for law enforcement purposes creates a challenge: how can the information be provided in such a manner so that only one class of people (law enforcement) is able to read this information using machine-readable technology. From a practical standpoint, this one class is also not one straightforward entity. In fact, there are 56 major entities (e.g., states, districts) that make up the class. Law enforcement organizations are further complicated through the federal, state, county and city jurisdictions within those entities.

Consider the implementation of one of the Real ID operational requirements. The REAL ID Act requires that any law enforcement official within the 56 issuing entities must be able to authenticate a REAL ID driver's license or identification card using the MRT, which is presented to them on a REAL ID document issued from any of the 56 issuing entities. As a result, interoperability is a primary requirement that must be addressed.

A clear case exists for smart card technology to satisfy this requirement. Smart cards are proven devices that securely protect data and only divulge information to authorized parties. With the embedded security features contained within a smart card, a system can be devised to address both the protection of information and the provision of this information for only authorized law enforcement purposes. Below are three scenarios that could be considered to achieve the goal of the requirement.

Scenario 1: Authentication of REAL ID credentials using online reference to the issuer

In this proposed scenario, we demonstrate that only a law enforcement official can request access to the machine-readable information contained in the smart card-based REAL ID driver's license or identification card and that the operation can only be completed with permission from the issuing entity (state).

Step 1: All law enforcement officials are issued a specific REAL ID credential (or dedicated smart ID card) that contains information in the chip indicating their specific status as a law enforcement officer. The ID cards can be protected by personal identification number (PIN) codes and/or biometrics to further ensure the card is only used by the intended official.

Step 2: Citizens are issued smart card-based REAL ID driver's licenses and identification cards that contain a payload of information about the license holder in secure memory within the smart card chip.

Step 3: When a law enforcement officer wishes to authenticate a REAL ID document issued by any state in the field or at a facility, the officer first presents his or her dedicated smart ID card to a suitably equipped terminal and uses a PIN code or biometric for identity verification. The officer then presents the citizen's REAL ID credential to the terminal. The terminal determines the entity that issued the citizen’s REAL ID document and contacts either a central registration service or the issuing entity with an inquiry request. The request is authenticated by the issuer using the officer's ID card presence and other information appended to the original request. In practical terms, this can be achieved by creating a digital signature from the officer's ID card and appending it to the request.

Once the request is authenticated by the issuer, a secure instruction is sent back to the terminal and presented to the citizen’s REAL ID driver's license or identification card, informing the card that it is now authorized to release the machine-readable information (or a portion of it) to the terminal for use by the officer. With suitable connectivity and availability of systems, this authentication and release of machine-readable information can be achieved quickly and securely.

Scenario 2: Authentication of REAL ID credentials by the local terminal

Step 1: As in the first scenario, all law enforcement officials are issued a specific REAL ID credential (or dedicated smart ID card) that contains information in the chip indicating their specific status as a law enforcement officer. The ID cards can be protected by PIN codes and/or biometrics to further ensure the card is only used by the intended official.

Step 2: Citizens are issued smart card-based REAL ID driver's licenses and identification cards that contain a payload of information about the license holder in secure memory within the smart card chip.

Step 3: On a periodic basis, suitably equipped terminals are loaded with issuing entities' access codes from either a central registry service or by cross agreements between the entities.

Step 4: When a law enforcement officer wishes to authenticate a REAL ID document issued by any state, the officer first presents his or her dedicated smart ID card to a suitably equipped terminal and uses a PIN code or biometric for identity verification. The officer then presents the citizen's REAL ID credential to the terminal. The terminal determines the entity that issued the citizen's REAL ID document and uses the appropriate, locally-available entities' access codes to create a one-time authorization for the citizen's REAL ID document to communicate the machine-readable information to the law enforcement official. This mechanism can validate the REAL ID driver's license or identification card, as well as provide access to the machine-readable information from any of the 56 entities. The one difference with this scenario is that it would be done offline and would not enable any outstanding warrants or identity document revocation to be determined.

Scenario 3: Law enforcement access using diversified symmetric keys.

Step 1: As in the first two scenarios, all law enforcement officials are issued a specific REAL ID credential (or dedicated smart ID card) that contains information in the chip indicating their specific status as a law enforcement officer. The ID cards can be protected by PIN codes and/or biometrics to further ensure the card is only used by the intended official. Specifically, each law enforcement card contains a securely-maintained, system-wide shared secret (a symmetric key).

Step 2: Citizens are issued smart card-based REAL ID driver's licenses and identification cards that contain a payload of information about the license holder in secure memory within the smart card chip. Access to this payload is controlled by every card having a unique access key called a diversified key. This unique diversified key is derived from the system-wide shared secret and the specific card serial number and is loaded onto the REAL ID document when it is issued. Thus the system-wide shared secret does not reside within the citizens' cards – only within law enforcements officers' cards.

Step 3: When a law enforcement officer wishes to authenticate a REAL ID document issued by any state in the field or at a facility, the officer first presents his or her dedicated smart ID card to a suitably equipped terminal and uses a PIN code or biometric for identity verification. The officer then presents the citizen's REAL ID credential to the terminal. The terminal determines the citizen's REAL ID document serial number and requests the officer's card to create the one-time authorization to the citizen's REAL ID card that will enable it to communicate the machine-readable information to the law enforcement official. The officer's card then creates a cryptogram derived from the shared secret it knows and the citizen's card serial number. The cryptogram generated by the officer's card can only be validated by the specific citizen's card and is used to provide one-time authorization for the officer to access the citizen's information. This mechanism can validate the REAL ID driver's license or identification card, as well as provide secure and private access to the machine-readable information written by any of the 56 issuing entities. Again, the one difference with this scenario is that it would be done offline and would not enable any outstanding warrants or identity document revocation to be determined. Clearly, a common shared secret among all law enforcement ID cards that allows access to any citizen card may present a vulnerability to the security of the

machine-readable information if the shared secret and card key diversification algorithm are discovered.

Variations

In the above scenarios, a specific law enforcement ID card is needed to enable access to information on the citizen's REAL ID document. A variation could be to equip terminals with embedded smart cards, called secure application module (SAM) cards, that would perform the initial authentication rather than the officer having to present the law enforcement ID card every time. SAMs can hold shared secrets and perform the card-specific requests as described in Scenario 3.

Beyond Card Authentication into a Digital Society

Once a decision is made to incorporate a smart card chip into a REAL ID driver's license or identification card to satisfy a specific purpose (such as to provide secure and private access to machine-readable information by law enforcement officials), there is a small step to making the REAL ID document a valuable citizen identity credential within our demanding information society. Having an electronic identity verification device in the hands of all citizens can enable a host of applications that presently lack a trusted identity authentication credential. The FTC recently released a strategic plan for better authentication in our society as a countermeasure to identity theft. A smart card-based REAL ID credential is the most appropriate platform to significantly improve the trust and reliability of identity in our society. A trusted federally-specified, state government-issued citizen electronic identity credential would also form the foundation to stimulate e-commerce and e-government applications in our society.

3. The REAL ID NPRM fails to consider national and international standards for identity documents that have already addressed the need for strong document security and protection of citizen privacy.

The REAL ID Act of 2005, 49 USC §202, requires minimum features, data and technologies to be provided on a REAL ID driver's license or identification card:

> (b) MINIMUM DOCUMENT REQUIREMENTS.—To meet the requirements of this section, a State shall include, at a minimum, the following information and features on each driver's license and identification card issued to a person by the State:
>
> (1) The person's full legal name.
> (2) The person's date of birth.
> (3) The person's gender.
> (4) The person's driver's license or identification card number.
> (5) A digital photograph of the person.
> (6) The person's address of principle residence.
> (7) The person's signature.
> (8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.
> (9) A common machine-readable technology, with defined minimum data elements.

49 USC §205 further grants the authority to the Secretary of Homeland Security to administer rules and compliance to requirements, in consultation with the Department of Transportation and the states.

A large number of countries, including Australia, Canada and the United States, have no national identification cards and, because of the widespread use of cars, driver's licenses are often used as the standard form of identification. This is the core of the intent of the REAL ID Act: provide a strong, secure, standard means of identification that augments the right to drive.

Many European countries require adults to carry an ID card at all times. Citizens of EU countries which have no national ID cards must carry their passports when traveling in these countries.

The United States is one of the few countries to co-mingle the right to drive with the right to travel internationally to neighboring countries (i.e., Canada, Mexico, Bermuda and the Caribbean). The Western Hemisphere Travel Initiative (WHTI) seeks to establish a new form of identification, the passport card, which enables U.S. citizens to re-enter the United States using only the passport card in lieu of a U.S. passport. The passport card is not associated with the right to drive.

Some states seek linkage of their REAL ID driver's licenses and identification cards with the right to cross borders. The current memorandum of agreement between the State of Washington and DHS contemplates the use of the passport card technology as an optional feature on that state's driver's license. This supports their plan to offer value to their citizens by aiding in the ability to cross the northern border and return easily.

There are three concepts that must then be considered when defining *standards* for a REAL ID driver's license or identification card:

- Identity
- Right to drive
- Right to travel

The combination of these three concepts provides significant incentives to manufacture fraudulent cards. Fraudulent cards will aid individuals of ill intent to:

- Perpetrate identity theft
- Evade law enforcement with respect to driving records and accountability of the driver to their own actions (e.g., DUI, problem drivers)
- Enter the United States illegally

The NPRM on REAL ID driver's licenses and identification cards states (Section II.H.6):

> DHS seeks comments on whether the proposed adversarial testing standards will lead to the development of a secure document solution that deters amateurs from producing deceptive counterfeits and/or alterations. DHS also seeks comments on other alternative approaches DHS could pursue on document security to achieve the same objective and how those approaches compare to a performance-based independent adversarial testing.

The DHS NPRM further states (Section II.H.8):

> The proposed regulation would mandate the use of the PDF-417 2D bar code as the common MRT standard and DHS proposes to adopt most of the mandatory data elements described in the 2005 AAMVA Driver's License/Identification Card Design Specifications, Annex D, as its MRT data elements model.

The Smart Card Alliance supports the use of appropriate technologies for security and privacy of citizens' information when placed on a REAL ID driver's license or identification card. DHS has proposed setting the standard of care for REAL ID Act compliance to be very low, requiring "…a secure document solution that deters amateurs…" This proposal regarding *amateurs* does not appropriately address the risks of well-funded attackers (e.g., al Qaeda) or motivated smugglers across our nation's borders, nor motivations to evade law enforcement. The tools to produce sufficiently credible fraudulent ID documents using printed media are widely available and must be considered a significant threat to REAL ID driver's licenses and identification cards and our nation.

Using *static* technologies *printed* on a card cannot be considered adequate to deter even amateurs in counterfeiting and forging a REAL ID driver's license or identification card when the combined capabilities of identification, right to drive and right to travel are offered by states issuing REAL ID documents.

DHS also invited comments (Section VI.(4)) on states incorporating:

> "a separate WHTI-compliant technology, such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF 417 barcode requirement."

The selection of technology for WHTI passport cards has not yet been formally made. DHS has been actively pursuing a recently-invented and unproven, "vicinity read" RFID technology that is typically used in inventory tracking for WHTI passport cards. This proposed RFID technology is designed for tracking products and pallets, is insecure, is untested, is only capable of transmitting a simple static number at a long range (over 30 feet), presents a serious privacy threat to citizens, and creates a vulnerability for exploitation by terrorists and criminals.

The Smart Card Alliance strongly recommends that smart card technology be used for passport cards and potential REAL ID driver's licenses or identification cards that could be used for border crossings. Use of smart card technology can take advantage of the experience of the numerous smart card-based U.S. government identity programs (such as ePassports, FIPS 201 PIV cards, Transportation Worker Identification Credential cards), which have all adopted smart card technology for secure, privacy-sensitive identity credentials.

It is also important to note that reading a REAL ID driver's license or identification card from a distance (i.e., with long-range, vicinity-read RFID technology) is not an operational requirement that is recognized for secure documents. International and national standards for identity documents (e.g., ICAO Document 9303 MRTD standard used for the ePassport and FIPS 201 PIV card standard) use secure, contactless smart card technology as appropriate to their mission. In all instances, these national and international standards support the use of secure contact and/or contactless smart card technology. These standards recognize the need for:

- Active electronic verification of the identity document.
- Protocols that protect the privacy of the individual bearer. The identity documents do not release information without appropriate authentication and encryption, and they do not enable tracking of the individual through RFID beacon behavior.
- Establishing a chain of trust between the issuer, the bearer and the identity card document through use of digital signatures.

The REAL ID NPRM (section VI) also makes the following requests for comments:

> (2) Whether the data elements currently proposed for inclusion in the machine readable zone of the driver's license or identification card should be reduced or expanded; whether the data in the machine-readable portion of the card should be encrypted for privacy reasons to protect the data from being harvested by third parties, and whether encryption would have any effect on law enforcement's ability to quickly read the data and identify the individual interdicted. What would it cost to build and manage the necessary information technology infrastructure for State and Federal law enforcement agencies to be able to access the information on the machine readable zone if the data were encrypted?
>
> (4) If a State chooses to produce driver's licenses and identification cards that are WHTI-compliant, whether citizenship could be denoted either on the face or machine-readable portion of the driver's license or identification card, and more generally on the procedures and business processes a State DMV could adopt in order to issue a Real ID driver's license or identification card that also included citizenship information for WHTI compliance. DHS also invites comments on how States would or could incorporate a separate WHTI-compliant technology, such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF417 barcode requirement.

National and international standards are available that enable selection of appropriate, secure smart card technologies that protect the privacy of citizens and support security of their information and access to that information for appropriate uses. The Smart Card Alliance suggests that DHS consider the use of existing national and international standards appropriate

to the objectives of the REAL ID Act and the states. To that end, the Alliance offers the following three standards for consideration by DHS to strengthen the resistance of REAL ID driver's licenses and identification cards to forgery and fraud and to enhance citizen privacy:

- Identification and the right to drive – international standards for driver's licenses
- Right to travel – international standards for passports and identity documents
- Identification and interoperability for additional Federal official uses – FIPS 201-compliant ID documents

International Driver's License

The Smart Card Alliance requests that DHS reference ISO 18013 "Personal Identification – ISO Compliant Driving License" in the REAL ID NPRM. The United States is now recognized as a leader in applying smart card technology to identity documents, including the ePassport and FIPS 201-compliant programs. The Alliance recommends the use of standards-based technology, such as ISO 18013, for states that seek to support identification and the right to drive.

ISO 18013 is in three parts. Part 1 describes the structure and topology of the ID card. Part 2 describes the data model for appropriate machine-readable data. Part 3 describes the use of a smart card chip. ISO 18013 is closely aligned with current AAMVA standards for printed features of an identification document. To promote security, privacy and interoperability, use of smart card technology defined in ISO 18013 Part 3 is strongly recommended by the Alliance.

The international driver's licenses standard provides security, integrity and multiple technologies using smart card chips to ensure a chain of trust between the issuer (using digital signatures on the chip for all data printed on the card), the credential (using authentication protocols to the chip), and the bearer (using a printed photo that must match the photo stored on the chip).

Passports

The Smart Card Alliance requests DHS consider use of ICAO 9303 MRTD-compliant ePassport and MRZ standards (incorporating smart card technology) for states that seek to support identification, the right to drive, and the ability to cross borders.

ICAO 9303 defines the use of optical character technology in its MRZ and a secure, reliable smart card chip that provides significant privacy benefits and security for personal information stored in the identity document. It enables use of ID-1 style cards (i.e., credit card format).

The Smart Card Alliance recommends that DHS use the international driver's license formats for the main features of the printed card, but add the MRZ as defined in ICAO 9303 and used for the ePassport.

FIPS 201

The Smart Card Alliance requests DHS consider use of a FIPS 201-compliant smart card chip for states that seek to support identification, the right to drive and enhanced interoperability with Federal initiatives, such as the First Responder Access Credential (FRAC) and the Transportation Worker Identification Credential (TWIC).

The Smart Card Alliance recommends that DHS use the international driver's license formats for the main features of the printed card, but add a FIPS 201-compliant chip that provides significant privacy benefits and security for personal information stored in the ID document.

This approach will enable the states to have broader participation in the National Incident Response System for individuals needing such capability and enable broader citizen benefits, using the full public key infrastructure (PKI) capabilities enabled by FIPS 201.

Summary

The Smart Card Alliance recommends that DHS not only require that states protect REAL ID driver's licenses and identification cards against attacks from *amateurs*, but also require the incorporation of technology that can resist attacks from dedicated, well-funded professionals.

The risks to the nation are real and the opportunities for fraud, identity theft and illegal entry into the country must be considered beyond an issue of amateurs. Additional technologies are available and have already been standardized, both nationally and internationally. These standards all recommend the use of smart card technology and enhance security and privacy of citizens using the security features supported by smart card technology.

4. The REAL ID NPRM incorrectly dismisses smart card technology from consideration by states and mis-states its applicability to a REAL ID driver's license or identification card.

Section II.H.8 of the NPRM states:

> "The integrated contactless chip was not deemed an appropriate technology for this particular document, as there is not an identifiable need for driver's licenses and identification cards to be routinely read at a distance".

This statement about contactless chips is a misleading assertion and shows a lack of understanding of smart card technology. [It should be noted that prior to the issuance of the REAL ID NPRM, numerous requests were made directly to the DHS REAL ID project office by Smart Card Alliance members to meet and educate DHS on smart card technology and its benefits. No audience was granted, with input only accepted from ITAA.] Further, while contact smart card technology is stated as an option that was evaluated along with 2D bar code, its security and privacy advantages were not considered in selecting the technology.

Smart card technology has the capability to provide significant improvements to REAL ID driver's licenses and identification cards by protecting information, verifying the user and only communicating specific information securely to authenticated parties. Smart card technology provides security and privacy-enhancing features that are fully understood and used in a variety of other U.S. government identification programs, such TWIC, FIPS 201 PIV card, ePassport, First Responder Access Card, and the commercial Registered Traveler program. None of the identity cards in these programs are "routinely read at a distance" as they contain proven, cost-effective, tamper-resistant contact and/or contactless smart card-based technologies.

Smart card technology has considerable features that can benefit REAL ID driver's licenses and identification cards:

- The technology makes the documents exponentially harder to counterfeit by storing an electronic copy of the printed information securely in the embedded chip.
- Smart cards rigorously protect the electronic credential and preserve the privacy of the citizen's personal information.
- The technology provides a secure manner to deliver the identity credential data to authorized law enforcement officials.

Smart card technology has been proven to be very cost effective and is the only technology that provides a highly tamper-resistant identification mechanism that can tie the cardholder to the document and that ensures only authorized access to identity information is provided to external requests.

5. The REAL ID NPRM does not consider how smart card technology provides a cost-effective solution for REAL ID driver's licenses and identification cards that not only improves privacy and security, but also allows states to leverage their significant investment in REAL ID documents and processes for other identification programs and government applications.

The Department of Homeland Security currently calls out the use of 2D bar code technology as the means of storing identity information on REAL ID driver's licenses and identification cards. The Smart Card Alliance strongly believes that substantial justification exists for specifying smart card technology for REAL ID documents. The justification results from a small difference in the

cost of a smart card-based REAL ID driver's license or identification card compared with the substantial benefits that accrue to the organizations and the individuals that use them.

Smart Card Cost Estimates

Driver's licenses today consist of a plastic card, composed of Teslin or other material, and are personalized for each driver with printed information such as name, date of birth, address, height, eye color and a color facial photograph. The typical cost of a completed personalized driver's license to a Department of Motor Vehicles ranges from $3 to $5, depending on volume, type of plastic card and processing costs.

Smart card technology can be incorporated into existing card bodies as either a contact, contactless or dual-interface implementation.[4] For a contact-only implementation, a contact module inclusive of a chip can be embedded into the card as it is manufactured (not post-issuance). Smart card contact-based chips range in functionality and complexity and therefore range in price. The typical incremental cost for adding a contact-based microcontroller smart card chip ranges from $2 to $3 depending on volume (measured for millions of units) and functionality. This would result in a potential total combined price range of $5 to $8 for a REAL ID driver's license.

If a digital certificate were to be added to the credential, an additional cost would likely be applied.

Contactless smart card technology comes in several varieties as well. The incremental cost for the simplest and smallest form of ISO/IEC 14443 contactless smart card technology is around $1.50 to $2 (for millions of units), resulting in a potential total combined price range of $4.50 to $7 for a REAL ID driver's license.

For dual-interface smart card technology (which combines both contact and contactless interfaces), incremental costs range from $3 to $5, resulting in a potential combined price of $6 to $10 for a REAL ID driver's license.

If REAL ID driver's licenses and identification cards adopt smart card technology across the country, it is quite possible costs may be somewhat less due to the potential large volumes aggregated across 56 issuing entities.

Clearly reading equipment infrastructure would be needed for the law enforcement application discussed elsewhere in this document. USB contact smart card readers can be bought for under $10 today, and are already included as a standard feature in several laptops. USB contactless smart card readers are typically around $25 to $50 and are less commonplace than contact readers today. The full cost of deploying a smart card system would need to be calculated once an implementation scenario is selected. However, the incremental cost for the cards is small.

Smart Card Technology Benefits

The benefits associated with use of smart card technology cover a wide range of areas, some of which have been detailed in this response. These benefits (among others) include:

- Improved security
  - As presented in this document, 2D bar code technology can be easily counterfeited. No method exists for securing the information stored in the bar code. This weak security limits the amount and type of information that can be stored on the REAL ID driver's license and limits its use.
  - A smart card-based REAL ID driver's license or identification card provides the strongest possible security and credibility to the relying party. It provides the greatest

[4] The embedded smart card chip 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).

possible assurance that the document is an authentic credential. The benefits of strong security in the credential go directly to the goals of the REAL ID Act and to the heart of the charter of the Department of Homeland Security, namely improved national security.

- Improved privacy
  - As discussed in this document, 2D bar code technology can be easily counterfeited and since the only way that the bar code card is tied to the bearer is by a picture printed on the card, changing either the bar code data or the picture results in a changed or stolen identity. This opens the door to a variety of potential fraudulent transactions and increased cost to the issuer and cardholder to rectify the fraud.
  - A smart card-based REAL ID driver's license or identification card provides the strongest possible privacy protection. The information stored in the chip cannot be extracted (or modified) without the permission of the bearer and/or issuer. Personal control over the release of private information in a smart card-based REAL ID document provides a significant improvement over the current proposed machine-readable technology.
  - Identity theft was identified as a growing threat in 2002 by the General Accounting Office[5] and has been estimated to exceed $50 billion per year in the United States by the Better Business Bureau®[6,7] and other organizations.
  - 60 percent of identity theft complaints relate to Internet activities.[8] Consumer to-and-from government Internet transactions represent a significant opportunity to provide better services, reduce costs and increase revenues for states. Smart card-based REAL ID documents can provide a secure basis for these Internet transactions.
- Wider credential use
  - A driver's license currently represents a single-privilege credential, namely the right to drive. The REAL ID Act targets the use of the driver license as a secure multi-purpose basis of identity. 2D bar code technology fails to meet the multi-purpose identity goals.
  - A smart card-based REAL ID driver's license or identification card supports the greatest possible use of the credential. It provides the ability for the REAL ID driver's license to be used for a wide range of applications and meet the fundamental goals of REAL ID Act by strongly establishing identity.
  - A smart card-based REAL ID document can have data written to it over time. In addition a number of techniques now exist that can associate privileges other than driving with the credential. The DHS-supported First Responder Authentication Credential (FRAC) is an example of how Emergency Support Function (ESF) codes can be associated with a credential (even without a network connection at transaction time). This means that a wide variety of other non-driving privileges can be associated with the smart card-based REAL ID driver's license or identification card. Each of these privileges can provide economic justification for the states as a result of additional uses; in some cases, these additional uses can increase revenue to states.
  - A smart card-based REAL ID driver's license or identification card can provide the basis for accessing government information technology (IT) systems. Substantial benefits accrue to citizens in this case. For example, citizens could use their REAL

---

[5] GAO, "Identity Theft: Prevalence and Cost Appear to be Growing," GAO-02-063, March 2002 (http://www.gao.gov/new.items/d02363.pdf)

[6] Better Business Bureau, "New Survey Shows Identity Fraud Growth is Contained and Consumers Have more Control Than They Think, January 31, 2006 (http://www.bbbonline.org/IDTheft/safetyQuiz.asp)

[7] Fight Identity Theft web site (http://www.fightidentitytheft.com/)

[8] Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data, January - December 2006," February 2007 (www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf)

ID driver's licenses to securely access government online applications (e.g., for filing taxes or requesting official papers online). This provides citizens with a new and important use of their driver's license or identification card and immediately addresses fraud and identity theft and issues around stolen or forgotten passwords. Additionally, options exist to enable physical access for these credentials making them able to address the convergence of logical and physical access.

- Strong electronic authentication provides a potential revenue stream for the states. Currently a driver's license provides a basis of identity for a wide variety of retail, banking and other commercial organizations. States derive no revenue from this. By providing a strong basis for identity, its wider use as an electronically verifiable credential creates a possible government service that has significant value and for which a price can be charged.
- Smart card-based identity verification has been shown to scale for many millions of users in identity applications worldwide. One of the major goals of the REAL ID Act involves using REAL ID documents to access Federal and transportation facilities. Systems already exist to check smart card-based IDs using strong electronic authentication.
- Smart card-based REAL ID driver's licenses and identification cards provide the best means for moving people quickly through security checkpoints. Just as the FRAC provides a means to quickly admit first responders (and those involved with recovery as well), a smart card-based REAL ID driver's license provides a means of quickly, securely and cost effectively moving people through security checkpoints. This is true in airports, on vessels, and back into neighborhoods when natural disasters or other emergency situations have taken place.

• Single issuance, multiple updates

- 2D bar code technology prints the information associated with a particular driver's license or identification card *once*. In order to change the information on a credential, the card must be reissued or databases must be made available that can be queried to find out the status and attributes of the credential.
- As mentioned above, a smart card-based REAL ID document can have data added to it over time, while, at the same time, having sections of the card where personal information exists "locked down" so that any permanent information cannot be modified.

• FIPS 201 leverage

- A wide variety of products and credential programs use the smart card technology mandated by Homeland Security Presidential Directive 12 (HSPD-12) and the Federal Information Processing Standard 201 (FIPS 201). Many benefits accrue from following standards: leveraging infrastructure, leveraging products, and interoperability.

As discussed in this document, the incremental cost for adding smart card technology to a REAL ID driver's license or identification card is relatively small. This small additional cost exponentially increases the difficulty to counterfeit the document or use the document for fraudulent purposes and brings along many advantages for determining card authenticity, protecting citizen privacy, and providing a workable, protected law enforcement application. With the addition of a digital credential, the REAL ID driver's license can form the basis of citizen-to-government interaction and can be leveraged for many commercial applications that are desperately seeking a trusted citizen identification credential.

The smart card-based solution exists, is widely used, and is accepted globally in the marketplace. Since smart card technology provides the only means of truly meeting the goals of the REAL ID Act and has strong economic, security, privacy and operational benefits, the Smart Card Alliance believes that there is an overwhelming justification for a mandate of smart card-based REAL ID driver's licenses and identification cards.

CONCLUSION

The realities of the post 9/11 world demand that the security of U.S. citizens no longer be compromised by identification documents that are easily duplicated, modified or counterfeited. The fundamental purpose of the REAL ID Act is to dramatically improve the veracity of identification documents presented by citizens and legal residents of the U.S. seeking access to some federally controlled facilities and commercial air travel. Because the driver's license has become the de facto standard identification document in the U.S., the structure for the document proposed in the REAL ID NPRM must be consistent, if not optimally designed with these other purposes in mind. Lastly, and most importantly, the structure of the driver license described by DHS must maintain the privacy of the citizen. On all three requirements, security, utility, and privacy, the structure of the driver license prescribed by the REAL ID NPRM is inadequate to meet the intent of the REAL ID Act and the needs of the states and citizens of the U.S.

This paper has discussed in detail the reasons that a 2D bar code is inadequate to meet the explicit requirements for a REAL ID driver's license or identification card. From a security perspective, it provides negligible additional protections against cloning, tampering and counterfeiting, which are the fundamental reasons for improving and standardizing state-issued driver's licenses. From a privacy perspective, protection of personal information is non-existent using the proposed 2D bar code. Anyone reading the proposed REAL ID driver's license using commercially available scanners will be able to automatically collect all information about the bearer of the document, regardless of the need for the information during a specific presentation of the ID. From a standards perspective, the proposed MRT ignores existing international and federal standards designed and vetted through years of experience improving the security, privacy, and utility of identification documents.

In stark contrast to the problems associated with the design described by the NPRM, smart card technology exists today that fully addresses each of these issues and better meets the intent of the REAL ID Act. Supported by national and international standards, smart card solutions can dramatically improve the security of the REAL ID document by using advanced semiconductor technology, secure operating systems, secure communication protocols, and strong cryptographic techniques. These same aspects of modern smart card technology will also provide strong protection of citizen privacy, preventing the wanton distribution of personal information.

Perhaps most important of all is the unique opportunity afforded by this moment in time in the U.S. to define the REAL ID driver's license in a way that not only meets the intent of the REAL ID Act but also sets a course for the machine-readable technology that will be implemented in state-issued driver's licenses and identification cards for years to come. States will invest an enormous amount of money and resources in implementing the new driver's license and what is chosen today will likely become the minimum standard for the foreseeable future. Choosing an antiquated MRT will perpetuate the problems and limitations associated with this technology. The citizens of the U.S. deserve better than this.

The incorporation of smart card technology into REAL ID driver's licenses and identification cards makes the REAL ID document a valuable citizen identity credential within our demanding information society. Having an electronic identity verification device in the hands of all citizens can enable a host of applications that presently lack a trusted identity authentication credential. The FTC recently released a strategic plan for better authentication in our society as a countermeasure to identity theft. A smart card-based REAL ID credential is the most appropriate platform to significantly improve the trust and reliability of identity in our society. A trusted federally-specified, state government-issued citizen electronic identity credential would also form the foundation to stimulate e-commerce and e-government applications in our society.

The Smart Card Alliance recommends that DHS reconsider the MRT chosen for REAL ID driver's licenses and identification cards and specify smart card technology as the common MRT to be implemented in all REAL ID documents. The same smart card technologies that have been chosen to improve and protect the identity document used in a wide range of federal and international identity applications should be used to secure the federally-

mandated REAL ID driver's licenses and identification cards that citizens will be required to use and almost certainly pay for if they are to gain access to the locations and services governed by REAL ID Act.

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. Members of the Smart Card Alliance include identification application technology providers and all of the industry segments that use smart card technology, including federal government and other non-federal agencies. The Smart Card Alliance invests heavily in education on the appropriate uses of technology for identification and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.