→ DRIVER LICENSE CARD STANDARDS: ACHIEVING HIGH SECURITY AND ADOPTION

This report was specially prepared as a
REAL ID Discussion Document

by Digimarc Corporation

DIGIMARC

DIGIMARC

KEYS TO CARD SECURITY

- Design against a set of identified counterfeiting and fraud threats
- Layer card security features and link them to each other
- Innovate to stay ahead of the counterfeiter
- Use multiple card personalization techniques to raise the counterfeiting cost
- Ensure the supply chain is secure, preventing the counterfeiter from easy access to raw materials
- Leverage human and machine authentication

Introduction

The U.S. Department of Homeland Security (DHS) has proposed a set of requirements for the REAL ID compliant driver license document. Many of the suggestions made by DHS draw on best practices from the card security industry and leading standards setting associations, such as the Document Security Alliance. However, the standards are overly specific on security feature and card material requirements, such as imposing a mandate that states must use polycarbonate card stock and this could be seriously detrimental to the security of driver licenses and dramatically increase the cost to the states and citizens.

Digimarc has nearly 50 years of experience successfully producing billions of secure driver license and identity documents. The company serves 32 U.S. states, providing driver licenses and ID credentials, producing more than 60 million secure IDs per year, and has helped its customers through each major driver license system transition over the last five decades.

The most effective secure credentials are designed to defend against a set of defined counterfeiting and fraud threats. Leading vendors draw on industry best practice techniques and lessons from banknote and secure document design to apply technologies and manufacturing techniques to defend against counterfeiting and fraud. The card producer's goal is to cost effectively deliver a document that thwarts attempts to alter documents or produce wholesale counterfeits from scratch. The card architecture, the set of security features and their relationship to one another on the card, in combination with personalization techniques, affects the quality of the defense.

Driver licenses are produced from blank or pre-printed card materials that are then personalized to a single card holder. Personalization adds the demographic data (name, address, etc), portrait, and machine readable features such as a 2D barcode and digital watermarks to the document. Several techniques exist to personalize a card, including digital color printing techniques and laser engraving.

Digimarc offers a variety of card architectures to meet the security and budget requirements of its U.S. and international customers. The DHS standards require

polycarbonate cards and prohibit dye sublimation as a personalization technique. Polycarbonate as a card material is not itself a security feature, nor a secure material. It is simply one of the materials that can host security features.

Confining a State driver license issuer to polycarbonate material, and specifically limiting the choice to a solid polycarbonate card a) ensures that states will be forced to obtain the most expensive base card, b) increases states' cost by over $200 million per year without a related increase in security, and c) makes the counterfeiter's job easier. Additionally, since the vast majority of states use different secure card technologies today and do not use laser engraving as their principal personalization technology, the path to adoption is longer. Further, the standards are extremely difficult, at best, to implement in an over-the-counter workflow – which is currently used by the majority of state issuing authorities. These requirements could put adoption of the new standards by states at risk and may lead states to choose to oppose compliance rather than productive dialog and adoption. Moreover, it is doubtful that adopting states that choose to implement the standards would be able to completely rework their issuance processes and systems to achieve REAL ID compliance by the intended compliance dates.

Maximum Cost, Without an Increase in Security

The result of the recommendation to use polycarbonate cards is maximum card cost to the states by requiring use of the most expensive card materials. Limiting the choice further to solid polycarbonate cards restricts the options to only a small number of non-U.S. suppliers. Confining personalization to laser engraving threatens security by restricting the portrait to black and white and increases costs by requiring the most expensive personalization approach. Unfortunately all of these costs would come without a comparable security increase over alternatives.

For example, deployed polycarbonate cards have costs as high as $6 to $7 per card. Comparing a polycarbonate card to a secure card constructed from co-extruded polyester, the polycarbonate card costs 2x to 5x more with no security gain. This may result in an additional cost to states, which would likely be passed along to citizens, of over $200 million per year – potentially $1.2 billion of increased costs over just the first five years. The co-extruded polyester card can support a color portrait, laser engraving,

laser etching, and tactile personalization. Other card architectures which do not rely on solid polycarbonate are available from vendors such as Digimarc, Datacard and G&D which should be considered as viable alternatives.

Multiple Personalization Techniques

Digimarc believes that increased resistance to counterfeiting is achieved by combining personalization techniques: color imaging, laser engraving or laser etching, and the application of tactile personalization (something a card inspector can feel). This combination of techniques places the burden on a would-be counterfeiter to attack multiple technologies and features, an effective strategy used by secure document designers for hundreds of years.

The draft proposed REAL ID recommendations, as recently discussed with the states, essentially require the use of laser engraving for 100% of the variable information (since "dye sublimation" is ruled out in item # 3 of the draft DHS recommendation), eliminating all personalization techniques other than laser engraving. Counterfeiters would then need only to become equipped and expert in a single technology, and the industry as a whole would garner no benefit from the innovation and vendor investment to advance card design

Counterfeit Resistance

Some companies in the industry have suggested that cards made with solid polycarbonate construction are "impossible to counterfeit". Solid polycarbonate laser engraved cards can be successfully counterfeited using common black and white photography techniques. Further, unlike the alternative card architectures, many solid polycarbonate cards lack over-laminates for security and can be personalized after issuance, allowing a fraudster to alter a picture on a circulating driver license to steal someone's identity.

Alternative card architectures, such as co-extruded polyester cards, using multiple personalization techniques, demonstrate equivalent or better resistance to counterfeiting at a much lower cost.

DIGIMARC

Arming the Counterfeiter

The driver license industry has embraced card standards as a means to improve overall security. REAL ID standards can build upon the good work that has been already been done to further raise the security bar.

Digimarc believes that an element of a successful standard is to properly introduce variability in a way that does not dilute security while making the counterfeiter's job more difficult. Slight differences from one state to another help prevent nationwide attacks. This result is accomplished in part by using multiple personalization techniques and leaving a set of choices to each state. It is also accomplished by encouraging vendors to innovate in card architectures and security features, and to introduce advancements over time that comply with long-lived standards. Restricting card construction and personalization in the standard, such as the requirement for polycarbonate, defeats each of these security techniques.

In addition, the supply chain itself must be secure to avoid providing the counterfeiter with the raw material needed to produce cards. The proposed standards threaten these principles. Polycarbonate cards are typically shipped as completed card blanks, simplifying the counterfeiter's job. Alternative card architectures are supplied with raw laminate and core material, and then completed in a central issue factory. This process complicates supply chain attacks, making it more difficult for a counterfeiter to obtain base materials.

Recommendations

Digimarc would like to respectfully recommend that the final DHS requirements:

1) Base the standards on a set of defined threats.

2) Include a set of recommended common security features that allow an inspector of the driver license to readily determine authenticity through a combination of visual and machine inspection. These features should include:

a) Use of intricate, fine-line, multicolored background design produced via offset lithography to include microline printing and an intentional error/field check
b) Serial / inventory number on the card stock, either printed or carried in a 1D barcode;
c) Ghost image;
d) Optically variable security feature;
e) UV security feature; and
f) Covert machine readable feature, such as digital watermarking, linked to and securing data and security features on the card

3) Require the inclusion of three overt, three covert and one forensic security feature as the minimally compliant set.

4) Require multiple personalization techniques including at least a color portrait and a tactile personalization feature

5) Requires a card architecture that is resistant to photo swapping and data alteration, can support multiple personalization techniques including laser engraving of at least a ghost image, can support the required security features, and complies with REAL ID card certification tests.

6) Require a 2D barcode as a standard data carrying feature

7) Define or refer to a set of standard security tests be defined along with a certification process to certify the card architecture and design is compliant, including demonstrated resistance to photo swapping and data alteration.

In this way, vendors will continue to innovate in card architectures and security features to stay ahead of the counterfeiter, states will be able to more cost effectively implement the REAL ID standards, a degree of variability will be introduced to make the counterfeiter's job harder, all while ensuring that the resulting standards achieve the desired national security impact.