AAMVA
American Association of
Motor Vehicle Administrators

Design Principles and Guidelines
for Secure DL/ID Cards (SCDP)

August 2014

DRIVER STANDING COMMITTEE
CARD DESIGN STANDARD COMMITTEE

Contents

Executive Summary 2

Scope 3

Terms and Definitions 4

Process 5

Knowing the Stakeholders 6

Internal Consultations 10

Threat Analysis 15

Manufacture 17

Training and Communication 19

Performance Monitoring 21

Final Thought 23

Annex A (informative) Glossary of Features 24

Annex B (informative) Conformity Assessment 31

Annex C (informative) Main Threats to the Security of a DL/ID 32

Bibliography 36

Executive Summary

Imagine investing time, money, energy, and resources into a new secure document and then realizing that you did not get out of it what you had hoped to. This is one of the challenges that face issuing authorities when it comes to designing a new driver license or identification card. The reality is that it is possible to be in compliance with the American Association of Motor Vehicle Administrators' (AAMVA's) Driver License/Identification (DL/ID) card design standard (CDS) and yet still not achieve an *optimal* outcome in the effectiveness of your card's design.

This Secure Card Design Principles (SCDP) whitepaper is intended to lay out a set of principles, guidelines, and practices that can maximize the probability of developing and maintaining a DL/ID that will be resistant to compromise. Where the CDS provides the "building blocks" for designing a secure DL/ID card, this SCDP further describes a process for how to use those "blocks." There are many considerations to keep in mind beyond just the physical document and the particular security features (see Annex A) that it may contain.

Understanding the landscape with regards to your stakeholders is critically important to ultimately having a secure document. Assessing their needs and understanding the stakeholders' relationship to the issuing authority (IA) becomes a very necessary first step in the process. Organizing and conducting internal consultations is also important in helping you to identify the vision and goals and to identify existing issues with your current generation document that is in circulation.

Manufacturing idiosyncrasies are also a very key area to address. The roles that quality, security, durability, and cost all play can make or break your secure document's success. Training and communication are also something that must be intentional and strategic; a commitment to both continuous and regular training must be made by the IA so that people understand what is being done with the security of the cards.

Performance monitoring is also important. Knowing how well your particular card holds up helps to inform you as to what changes you may want to make to your next-generation design. Coordination with fraud investigation is another valuable source of information about what works and what does not.

The following is a product of a special ad hoc group that was organized through AAMVA's Card Design Standard Committee. Special thanks go to our industry partners at 3M, Canadian Bank Note Company, Datacard Group, DeLaRue, Gemalto, Giesecke & Devrient, MorphoTrust USA, and Valid USA.

Scope

The primary audiences for this paper are the issuing authorities (IAs) in the United States and Canada. The primary application is for cards, although the principles can be applied to other documents as well. Although following the CDS to the letter (e.g., by including the required number and type of security elements) cannot completely guarantee that a card will not be successfully attacked, the chances of better protection go up significantly. The goal of the SCDP is to build on the CDS by providing additional guidelines for designing a secure card. Issuing authorities should consider the following when designing a secure document (much of the focus of this paper will be on cards).

This document may be freely distributed.

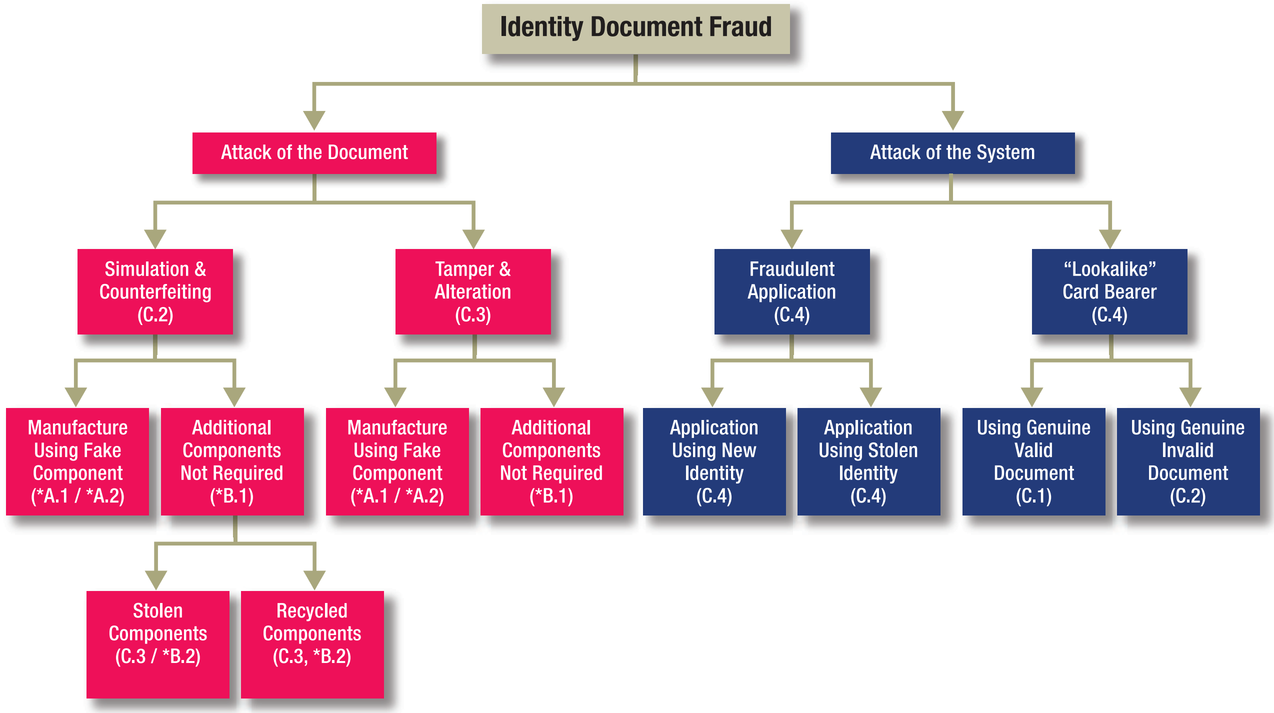
Terms and Definitions

CI	central issuance
DL/ID	driver license/identification [card]
IA	issuing authority, a governmentally authorized agent or organization that issues a DL/ID card
LE	law enforcement
Level 1 (first-line inspection)	examination without tools or aids that involves easily identifiable visual or tactile features for rapid inspection at point of usage
Level 2 (second-line inspection)	examination that requires the use of a tool or instrument (e.g., ultraviolet [UV] light, magnifying glass, or scanner)
Level 3 (third-line inspection)	examination done at a forensic level
OTC	over the counter (instant issuance)
SDP	security during personalization

Process

Identification of Threats

(also described in Annex C of this document and the DL/ID standard)


Identity Document Fraud
Attack of the Document
Attack of the System
Simulation & Counterfeiting (C.2)
Tamper & Alteration (C.3)
Fraudulent Application (C.4)
"Lookalike" Card Bearer (C.4)
Manufacture Using Fake Component (*A.1 / *A.2)
Additional Components Not Required (*B.1)
Manufacture Using Fake Component (*A.1 / *A.2)
Additional Components Not Required (*B.1)
Application Using New Identity (C.4)
Application Using Stolen Identity (C.4)
Using Genuine Valid Document (C.1)
Using Genuine Invalid Document (C.2)
Stolen Components (C.3 / *B.2)
Recycled Components (C.3, *B.2)

The numbers above correspond to threats that are defined in the CDS, which can be found in Annex C.

The purpose of this document is to improve the security of the physical license by addressing the threats shown in red above. The threats shown in blue are outside the scope of the SCDP.

Knowing the Stakeholders

One of the most critical tasks involved in designing a DL/ID card is understanding the potential uses of the card. Failure to identify all associated "stakeholders" before the design phase of the project can result in project delays or shortened card lifespan. After a list of stakeholders has been compiled, their needs must be assessed and addressed if deemed appropriate for the intent of the DL/ID card. Many stakeholders' needs are compatible. Many times there are stakeholders on both sides of the equation (those that issue and those that depend on what is issued): a design feature that benefits one entity may negatively impact another. Everyone's needs should be considered to the extent they can. In summary, an IA should consult all stakeholders but still remains responsible for compiling the ultimate set of requirements addressing all stakeholders' needs.

A common method of identifying stakeholders and assessing their needs is to first divide them into groups based on the nature of their needs or their relationship to the data contained on or in the card.

Core stakeholders are entities who will be directly impacted the most, either positively or negatively, by the card design. The most obvious are the IA and law enforcement (LE).

- IA: The quality, durability, and security of the license will impact directly the IA and the IA's broader governmental organization. The license design can, to a degree, be considered to reflect the brand of the IA.
- LE: During a traffic stop, an officer must be able to efficiently and effectively extract specific information from a card visually or electronically. Failure to do so has at the very least a negative impact downstream for that stakeholder's interaction with the card and could cost the person his or her life because of an unnecessary distraction.
    - Identify a unique individual. Are the font type and size adequate for adverse conditions? Does it adhere to industry standards for data location and identifiers? Are data encoded to a barcode or magnetic strip?
    - Identify the person's current authority to operate a specific class of vehicle
    - Identify any provisions for their operation (restrictions and endorsements)
    - Organ donor status

Additional stakeholders are entities indirectly affected, either positively or negatively, by the card design. An example is traffic courts that must establish the relationship between a unique identity record and an accident or citation provided by an LE officer.

Why is it necessary for the IA to identify stakeholders and assess their needs? Doing so has a number of important advantages:

- It results in more and varied ideas than would be the case if the design were conducted in the bubble of a single agency with like-minded people.

- It provides an opportunity for all stakeholders to provide input to the design process. As such, these stakeholders are more likely to support and champion the final product. This will strengthen the IA's position if there is opposition to the card design. Having the stakeholders on board makes a significant difference.

- It increases the credibility of your agency. Involving and assessing the needs of stakeholders establishes your organization as concerned, fair, and transparent.

Additional stakeholders (and their needs) may include:

- Medical first responders (emergency medical technicians and firefighters)
  - Identify a unique individual: Is the font type and size adequate for adverse conditions? Does it adhere to industry standards for data location and identifiers?
  - Medical conditions identified on or in the card?

- Donor status, travel, and transportation (Transportation Security Administration, car rental)
  - Identify a unique individual
  - Identifiable level 1 and 2 security features and compliance indicators
  - Identify the person's current authority to operate a specific class of vehicle

- Retailers, identity- or age-based, and general retailers (liquor, tobacco, pharmacies, firearms, and ammunition)
  - Date of birth of the card holder
  - Unique card format age designation
  - Easily identifiable level 1 security features
  - Military veteran Indicator

- Miscellaneous businesses, insurance
  - Identify a unique individual

- Financial entities (banks, paycheck loans, retail credit)
  - Identify a unique individual
  - Easily identifiable level 1 security features

- Employers (I–9 process)
  - Identify a unique individual
  - Clear data designations to ease data entry

- Government Agencies (Social Security Administration, Family Services, courts)
  - Identify a unique individual
  - Clear data designations to ease data entry
  - Easily identifiable level 1 security features

- Voting and voter registration
    - Identify a unique individual
- Public and private schools and daycare
    - Identify a unique individual
- Hospitals
    - Identify a unique individual
    - Clear data designations to ease data entry
    - Organ donor status
- Legislators
    - Attractive appearance that bears the state's "brand" or identity
    - Knowledge that the card security aligns with industry best practices

After the stakeholder list has been compiled, an assessment of their needs must be completed. These needs can be unique or shared, but commonly the needs of the key primary stakeholders will fulfill those of the secondary stakeholders. The initial assessment can either begin with face-to-face stakeholder meetings representing common groups or by providing them with a common set of questions designed to identify their needs with face-to-face discussions following at a later date.

Potential questions could include:

- For what do you use a state-issued driver license or photo identification card in your business or daily activity?
- Does the current DL/ID card address those needs?
- What changes in the DL/ID card would better fulfill your needs?

When conducting a face-to-face stakeholder meeting (focus group), it is critical not to assume that they actually know what data and features are on the DL/ID card even if they interact with the card on a regular basis. Providing card samples, card data, and security feature call-out documents will enhance their education and many times help them realize that their needs have already been met. Explaining the reasoning behind industry card standards and best practices as well as state and federal required card features and formats will remove much of the mystique. Examples could include the "dusty rose" header coloring or overlapping features that partially obscure data they want to see or font size that is constrained by the necessary minimum number of characters that the card must be capable of handling. Education builds acceptance or at least understanding.

Because it is common for agencies to keep card designs somewhat consistent over time, it is most likely that these discussions will expose potential design compromises that result in a superior product by modifying or eliminating a low-value data, security, or appearance feature.

LE at all levels must be able to rely on government-issued identification documents and know that the bearer of such a document is who he or she claims to be. Obtaining fraudulent identification documents presents an opportunity for criminals or terrorists to board airplanes, rent cars, open bank accounts, steal identities, or conduct other criminal activities without being detected. Because LE officials at all levels depend on secure documents to safely and effectively perform their mission, their input should be of primary concern and sought by those attempting to create secure documents. This should be a collaborative and ongoing effort between document administrators and federal, state, and local LE.

LE's primary mission is public safety, and they pursue this mission by focusing on criminal investigation and crime prevention. Secure documents play a significant role in both. Large or small, all criminal enterprises attempt to hide their activities from LE. One prevalent way is the use of fraudulent documents to conceal identity or activities. Some examples of these activities are:

- Terrorism
- Financial crime or fraud
- Identity theft
- Illegal immigration

Because each level of LE has different roles, responsibilities, and needs when handling secure documents, all levels of LE need to be included in this collaborative effort. Even within a single LE agency or department, there are different missions, needs, and uses of secure documents and their security features. The use of security features by LE officials is based on three factors: time, training (feature awareness), and equipment.

LE at all levels, but in particular, those tasked with patrolling the roadways and responding to criminal activity, must quickly assess the document in less than ideal conditions, with limited time, training, and equipment. To do this, they depend primarily on level 1 security features as they come into daily contact with secure documents at traffic stops and crime scenes. In these situations, rarely will the official look beyond level 1 security features. This makes features that are quickly and easily identifiable by touch or the unaided eye most beneficial.

On the other hand, LE agencies or officials with investigative, administrative, or security emphases will generally have more time, training, and equipment to use level 1; level 2; and on occasion, level 3 security features.

For example, an FBI taskforce conducting a large investigation will have the time, expertise, and equipment to take advantage of level 1, 2, and 3 security features. Conversely, a patrol officer making a traffic stop in adverse conditions may have only moments to determine whether the document he or she is holding is fraudulent and the vehicle operator is wanted, posing an immediate threat. In this situation, clear and easily identifiable level 1 features are critical.

It is a tendency to emphasize the role of level 2 or 3 features because they are often what large-scale or "serious" criminal investigations rely on when secure documents are a part of the investigation. Although level 2 and 3 features are critical for these situations and others, they are of limited value in many daily interactions between LE and secure documents. In these interactions, LE is likely to depend on level 1 security features the most.

Because of these factors, it is critical to seek input from a broad spectrum of LE officials when designing secure documents. Focusing on only one level of LE will provide document administrators with a skewed vision of LE needs when creating secure documents.

Internal Consultations

Consult technology experts on new developments. It is vital for anyone designing a secure card to have an understanding of current technologies, which can usually be obtained from the vendor community and the AAMVA community, especially jurisdictions that have undergone a request for proposal (RFP) recently.

In this exercise, the people charged with developing the DL/ID need to have a good grasp on what the technologies are really about that exist today and what threats they are designed to counteract. Experts within the vendor community as well as the LE community, DHS, and CBSA laboratories are good sources of information. The very people who actually develop new materials, processes, and security features are an excellent source because these technical professionals are the people who must know what exists today and what new things are on the drawing boards in order to do their jobs on a routine basis.

AAMVA members who have designed RFPs and designed new DL/IDs within the past 2 years are also good sources because they have paved the way in their own states, already canvassing the technical community. Additionally, jurisdictions with upcoming RFPs or active RFPs get considerable attention and all the new technology (materials, manufacturing equipment) is usually rolled out to this audience. Getting another state's input on feature sets and card materials or designs allows another set of eyes to examine technology. Conduct internal requirements gathering for the new card design. Requirements gathering is integral to the success of any project. This process must be detailed and thorough to adequately get the desired end product. Vendors will make proposals on the specifics of the RFP. Do not make assumptions that the vendor will know what you are trying to accomplish. Requirements gathering should include a team of individuals representing the issuing agency along with technical experts on secure cards. Involve as many stakeholders as possible. Ensure that they are well educated as to level 1 features (how to detect, preserve, and report). Use multiple media (e.g., video, websites, tutorials) to educate stakeholders and make use of liaison opportunities (interministerial, interagency).

- Start from the top down by first identifying management's vision and goals for the new document.
- Involve all internal stakeholders in the dialogue. Gather requirement from all departments that may have an impact on the card design, including design, security, data content, data layout, document readability, configuration of issuance sites (central, hybrid, over the counter [OTC]), and card lifetime
- Design considerations checklist
  - ❑ Purpose of document: Which services are enabled?
  - ❑ Verification: Who will verify the license? Expertise, readers, training?
  - ❑ Lifetime: storage, use, frequency, environment, validity period?
  - ❑ Security assessment: value, threats, new technologies, best practices
  - ❑ Preferred issuance configuration: central issuance (CI), OTC, hybrid?
  - ❑ Financial: capital budgets, ongoing budgets, sponsorship or funding, price of license

    - ❑ Branding: preferred colors, crests, logos, text
    - ❑ Legal: state or federal mandates
    - ❑ Interoperability: standards, legacy systems, cross-border agreements

- Develop a document summarizing all internal requirements.

- Consult with industry on latest technology developments and trends.

- Request updates through RFI (Request for Information).

- Consult with other government departments, agencies, or laboratories on latest developments. (AAMVA could assist in providing information.)

- Conduct case studies involving similar documents. Consult with other government bodies issuing the same or similar document and get their experience and lessons learned.

- Design (should still allow IAs to not all come up with the same solution)

Levels 2 and 3 features are critical to success for further forensic and expert analysis. However, too heavy a reliance on levels 2 and 3 can create a false sense of security if front-line staff are not equipped or trained to fully authenticate those features (e.g., seeing UV ink or holograms can create a false positive and in fact being readily falsified).

Simplicity can provide for more cost-effective production.

- Level 1 is most critical. However, do not rely on only one feature; it is also important to implement level 1 at multiple layers and technologies.

- Required functional performance (different for different stakeholders)

Good technology + Poor design = Poor security

Quality, security, durability, and cost are key characteristics of driver licenses and should be considered when designing the document.

Quality: A high-quality license will be consistent in appearance and closely match all other licenses issued in the same ID program. The security features—in particular, the primary portrait—will be crisp and clearly defined to allow easy authentication. Machine-readable features, such as chips, optically readable characters (OCR), and barcodes, will read consistently and accurately. Laminates will have the necessary optical clarity. Overall, a high-quality driver license will look and feel like one.

Security: The security of an ID is a measure of how well it resists deliberate attack. Document attack is either by simulation to produce a counterfeit or by tamper in an attempt to alter the information within the ID. The security of the document depends on how difficult it is to simulate or tamper with and also how easily the genuine document may be verified as being genuine. Simple is good; this is basic common sense for an overall effective design. One must adhere to this principle if two basic functions are to be attained: (1) ease of authentication and (2) automatic and widespread recognition of the credential as not only secure but also representative of a particular jurisdiction.

Simplicity or simpler to verify translates to less training, less costs, and less confusion. The simplest features can be described in terms of an action and a predicted outcome, for example, “Tilt the card away from you and look for the feature to change from X to Y.” A test of simplicity: consider if the feature could be described by phone. Ease: think of field environment and verification conditions; what would make it easy to verify a document? For example, in low-light conditions, a tactile feature can be useful and is often cited by LE as valuable.

For ease of authentication, one must use a combination of level 1 features in combination with the card design layout to effect a visually uncomplicated, “simple,” and secure design. The accumulation of too many obvious features can cause confusion in authenticating the credential. A good principle to consider is the selection of one or two very obvious level 1 features that are backed up by both other level 1 and level 2 features. Focusing the design around one or two features allows the designer to build the card design with these as the foundation. All threats need to be addressed using a variety of features yet without compromising the visually uncomplicated appearance.

Form follows function. Consequently, automatic and widespread recognition will follow from a well-designed, secure card.

As stated earlier, it is imperative that level 1 features are quickly and easily validated (e.g., raised lettering, insets, and translucent features). Having too heavy a reliance on level 2/3 features will not enable front-line analyzers to detect fraudulent documents.

A review of the CDS Annex B is imperative in understanding which features can operate as level 1, 2, or 3 security features.

Durability: The durability of a DL/ID defines its resistance to change. A document is exposed to a variety of environmental hazards during its life, such as light, flex, and extremes of temperature and humidity. It may also be subjected to accidental attack (e.g., laundry) or deliberate misuse, such as using a card for something other than intended (e.g., scraping ice off a windshield). An ID with high durability will survive the required validity period without significant visual change and without compromise to its performance.

Cost: The cost of the document refers to the cost to produce it. This will include the fixed and variable costs associated with enrolment, manufacture, personalization, issuance, shipping, and the many administrative functions necessary to manage and secure these functions.

The properties of QSDC—quality, security, durability, and cost— which are all important, may be given different priorities by the various stakeholders. For example, issuers of licenses may rate cost as the most important criteria. Durability will also be important to issuers because reissuing too many licenses can impact budgets. Document examiners, however, will probably want the best security features that they can get, with little consideration of cost or budgets. A citizen who owns the license wants it to look good, and quality is probably the most important consideration, together with the cost to him or her (the lower the better).

Measurement of these criteria can be difficult, and thus the setting of metrics for the required functional performance can be challenging.

The quality of an image or indeed of the whole license is somewhat subjective.

Durability measurement presents different challenges because there are many lists of test methods but which methods to use and how to interpret them. The extrapolation of the result of some accelerated laboratory tests to predict longevity for a 10-year license is a risk. (Reference the Durability Annex E in the CDS.)

The principles of license security are well proven and described elsewhere in this document, but ranking or scoring features is also very subjective.

Cost, of course, can be specified precisely, although breaking down the overall cost of a license can be difficult because so many factors are involved. Additionally, there is a potential cost to "getting it wrong"—a weak design lacking the upfront investment can yield a much higher overall cost because additional measures are then required to redo design(s).

Security during personalization (SDP) is a way to add additional security to a license. SDP uses a security feature (or features) to render, often redundantly, variable personal information. For example, a person's portrait image is repeated using a different printing technology, or the date of birth is repeated using tactile lettering. These features are powerful because they deliver key aspects of effective security features, for example:

- Defend against counterfeiting
- Defend against alteration
- Easy to verify with confidence
- Typically level 1 overt features
- Encourage verification of personal data
- Reduce the value, to the criminal, of stolen or recycled components

The SDP feature is created by bringing together, at a late stage in the manufacturing chain, specialized engineering, restricted components, and expert know-how. This combination delivers an effect that presents personal information in a way that is different from that possible with commonly available commercial equipment, thus defending against criminal attack by counterfeiting and alteration.

Layer, interlock, overlap, and integrate features to maximize their effectiveness—three features alone are nowhere near as strong as three features that are linked together in chain-like fashion. A fraudster who sees multiple features or variable data elements linked and layered together sees a strong line of protection and in most instances will not even attempt to attack. This is particularly true when variable data elements are attached to (linked) or layered with security features. An example of this is the inclusion of personal data within a "perforated" feature allowing one to see a pattern or image with data through the card. A counterfeiter has to make every single card different from the last one, which is time consuming and prone to error. To make things worse for the counterfeiter, one could layer this type feature with another one, for example, an obvious preprinted feature, making it necessary to connect any counterfeited feature to another one he or she has to create. When this happens numerous times, it is a very high wall for the counterfeiter to climb, and invariably this means the document will not be counterfeited.

Layering materials with various layers of printing has application of features at various manufacturing stages and depth in the document. It makes a document more complex and more difficult to counterfeit.

Interlocking or overlapping: Materials, data or features that are directly interlinked prevent from attacking one element, component, or layer without affecting the other(s).

Integration: Materials, data, or features that are securely integrated into the document are less susceptible to being separated from the document and reused for fraudulent purposes.

- Designate a card or document design team to represent internal or external stakeholders in the design process.
- Identify representatives from various internal departments to be part of the card design team.
- Include in the team external stakeholders with interests in how the document looks, functions, reads, and so on.

Threat Analysis

Design to address existing and potential threats. A key step in designing a secure credential is to define the threats that your existing credential faces today. This is vital in that it defines the starting point. What are fraudsters focusing on in today's card? How are they making their counterfeits? Where are they passing the counterfeits, and for what purposes? The retail community and LE community within the state or jurisdiction are the places to find these answers. One might also contact the local FBI or RCMP offices to understand the level of identity theft in the area, one of the biggest and growing threats across the country. A subsequent step is in getting a solid understanding of why the current card does not stop these threats. Enlisting the aid of industry experts in attack scenarios is extremely helpful in rounding out the analysis of the current situation—putting the stake in the ground representing where you are today.

Another step is in deciding what threats might be witnessed across your jurisdiction in the coming five plus years (or whatever the contract life is for the card). To do this, a canvassing of the surrounding jurisdictions' current counterfeit threats and how they have evolved is quite useful. What is happening in the neighbor states is often a harbinger of things to come. Contact with experts throughout the country will serve to round out the analysis of what is coming because many keep tabs on counterfeiters as they occupy "secret" internet chat rooms; monitoring this activity often tells of what they are working on to be able to meet the "new" credential challenges.

The design not only has to stop current threats, but it also must put in place protections from those threats to come.

Potential design lifetime =
Card lifetime + Program lifetime
(including program implementation time)

Design lifetime = The period of time that a particular security design has to resist fraudulent attack

Card lifetime = The validity period of the license, typically 5, 7, 8, or 10 years

Program lifetime = The period of time over which particular security design is issued

For example, the design lifetime for a 7-year card from a 10-year program is 7 + 10 = 17 years.

Identify and analyze collected data on existing threats and fraud, anticipate future threats, and integrate security features targeting specific threats and methods of attacks.

Analyze historic counterfeit and falsified cards (collected from verification and forensic authorities), as well as technology developments and integrate features addressing potential threats. The idea is to stay one step ahead of the fraud.

- Design with verification in mind: level 1, simplicity, ease

How will the document be verified in the field? Include features matching field verification practices.

Design with manufacturability in mind (design only what can be reliably and consistently manufactured). To ensure a secure card, it must be manufactured consistently and at a high-quality level. Any document that suffers from inconsistency, whether it is in quality of features or quality of variable information, including photos, is easily counterfeited. To a fraudster, a card that exhibits variability in the properties of a feature (e.g., various shades of blue instead of the same shade of blue every time) is an easy target. If the manufacturing process exhibits excessive variability, document reviewers are forced to accept a wide variety of cards and may stop authenticating a feature.

To facilitate authentication, the card design should specify tolerances for all features. Tolerances include field positions, color variations, and so on. Vendors should be monitored for compliance with tolerances throughout the program life.

Every manufacturing process has variation. The document should be designed in a way that this variability is minimized. On the other hand, not everything that can be "designed" can be manufactured; designs should take manufacturing capabilities into account.

. . . the fraudster tends to imitate the outcome, not the process.

The ideal document uses materials, features, and technologies that are not easily accessible to the general public. The material from which the card is made should not be readily available in the general public domain. There are materials that are claimed to be unavailable that are, in fact, readily available. Therefore, claims made by the manufacturers need to be reviewed by independent experts who are not associated with those manufacturers. Features that are currently under counterfeit attack in other jurisdictions should also be reviewed. For example, the use of holographic overlays offers a false sense of security. These are a mainstay of Chinese counterfeiters and are often easily found on an internet search. Therefore, one cannot effect a secure design if this is at the center of the credential's security. DHS (ICE, USSS), CBSA, FBI, and AAMVA are good sources of information. The basic tenet here is simple: if the genuine material or feature is available to the fraudster, then it will be used by the fraudster.

Widely available materials and features make the document less secure and more vulnerable, and they can be accessible to fraudsters; however, using only genuine components and materials whose availability is restricted is just one important defense because criminals often do not use the same materials or processes as are used for the genuine license. It is critical to remember that **the fraudster tends to imitate the outcome, not the process.** So, the genuine features need to resist simulation and alteration by criminals using commonly available materials and processes that give a similar visual result. As a minimum, limited availability know-how, materials, and technologies should be involved in the design and manufacturing of a secure document.

Manufacture

Durability is important. Cards that are not durable or become "worn out" make for easier targets. Secure manufacturing standards exist (ANSI NASPO, ICAO Secure Issuance Guidelines) that cover both vendor manufacturing and IA issuance. Durability tests should be conducted to provide for an objective third-party analysis of card lifespan and weaknesses (see Annex E in the AAMVA Card Design Standard).

It is also very important to understand the nuances accompanying the type of issuance to be used—instant (OTC) versus centralized (CI).

Some comparisons can be related to the QSDC methodology introduced earlier.

- ***Quality:*** The close similarity between all genuine documents is key to security. Every machine exhibits variability, and variability is always additive. So, the most consistent documents are produced using fewer machines and from a single site.
- ***Security:*** In addition to the "close match output" described earlier, the security of the document also relies on the security (resistance to theft) of its components. These are more easily protected and controlled when issued from a single site. They are also less likely to be intercepted in transit when moved to or from a single site. A further CI security benefit is that larger machines tend to offer more opportunity to add the SDP features described earlier. Larger secure sites may also have better security, so the chances of theft (either internal or through a break-in) are also decreased.
- ***Durability:*** The durability of a document depends to a degree on the precise control of personalization processes, particularly if the document is laminated. There is more control and less chance of out-of-spec lamination in a CI site with fewer machines.
- ***Cost:*** Secure document manufacture is no different from any other process; that is, there are economies of scale. A single large site is almost always less expensive to operate than two or more smaller sites. That said, one must weigh the benefits described earlier of a CI model with those of instant issuance. In instant issuance, if one site goes down, other sites are usually available, although they may be some distance away.

Ensure preproduction proofing and approvals. These include written specifications and could also include preproduction samples. Approved specifications and retained samples may be used as references against which the final product can be compared for the life of the contract. Also ensure compliance of the design to the CDS by submitting preproduction samples to the AAMVA Courtesy Verification Program (CVP). Card durability should be tested after the first preproduction run, well before the document is issued to the general public. Ideally, the tested document is composed entirely of actual components (as opposed to similar materials) and manufactured using the same machinery and processes as will be used in production to provide the most valid assessment of durability and integrity before launch. These test results should be used as baselines for tests conducted later during the program.

- Develop quality and consistency standards or guidelines
- Ensure continued compliance of the design and print quality to the CDS by, for example, submitting production samples to the AAMVA CVP (see Annex B)

Training and Communication

Given geographic challenges (populace spread out over large expanses) and fiscal constraints, it is imperative that jurisdictions develop tools that use evolving technologies such as video conferencing with staff and stakeholders, online tools, and tutorials (document samples—authentic and counterfeit). A commitment to continuous and regular training must be made. Failure to do so will provide for dilution of security. Also, a well-maintained email list allows for the quick dissemination of alerts and details about document compromise.

Counterfeiting Implications include:

- Identity theft leads to financial risk for individuals (unwanted debt), jurisdictions (expensive investigations and prosecutions), and insurers (fraudulent claims and improperly qualified drivers involved in crashes).
- Identity theft can lead to illegal activity (organized crime, terrorism).
- Identity theft can provide for infraction or license loss implications.

Too often, security features are simply unknown to the LE officials or the feature requires equipment not readily available to most LE officials. For the secure documents to be effective and useful to LE, level 1 and select level 2 security features need to be known and usable by all LE officials. This can only be achieved through the development of coordinated and training programs designed to make LE aware of these features.

This can best be accomplished through ongoing collaborative efforts among document administrators, LE associations, and state criminal justice regulatory agencies. All states have a criminal justice or LE regulatory entity that maintains training certifications and sets standards for initial and ongoing in-service training for sworn LE. These organizations, as well as federal equivalents and LE associations such as the IACP, are essential to ensure all LE receive the necessary training.

In the United States and Canada, the DL/ID card is the main identity credential that most of us rely on to prove who we are. No airline, travel agency, bank, mutual fund company, mortgage company, or even bar, restaurant, or hotel will take anything less than your DL. Therefore, what we are really talking about is the person's identity represented by this secure credential. If you are without it, there is little you can do in these countries. If it is compromised, you have a significant problem. Counterfeit cards may be used to become someone else, yielding access to their credit and bank accounts. This is a huge problem that has caused billions of dollars in damage to individuals across these countries.

Of course, there are other uses of counterfeit DL/IDs, including underage drinking and tobacco use and credit card abuse and scams, and their use in many criminal enterprises is well documented.

Many illegal aliens buy high-quality counterfeits so they may establish an identity in this country illegally. After they have entered into the actual jurisdiction's system, they have established themselves fraudulently into the country's identity system of choice.

- Develop various levels of information to be released to various target audiences, for example, level 1 (selected), general public; levels 1 and 2, verification authorities and stakeholders (various levels); and level 3, strictly "forensic and as per need basis."
- Maintain a document design version control and associated communication programs.

Every version of the document in the field should have a number and an associated communication program; version control ensures that the appropriate communication material is linked to the respective document version. For example, when a new feature is introduced, associated documentation under the same version number is distributed in the field.

- Conduct regular training session with target audiences. Develop effective online training packages.

Performance Monitoring

This is a very important aspect that must be kept in mind throughout the lifecycle of the DL/ID. As the cards are in circulation, periodic testing to see how they (a specific design) are holding up (durability wise) provides valuable data; this potentially relates to both the physical substrate or features of the card and functioning (machine readable or detectable aspects). Coordination with fraud investigation also becomes another good source of data on what about the cards is working and not working.

Here are some tasks that should be undertaken:

Establish a process to collect document performance data and define a repository to store performance data. A specific place and method to store the document performance data in the field should be agreed upon. This should be communicated to all authorities that are involved in document verification and handling.

AAMVA plays a critical role here, identifying the need for all jurisdictions to report both successes (design features, manufacturing or testing breakthroughs and failures [best practices]).

The Association can further its efforts of maintaining a compendium of all member jurisdictions' inventory and a secure listing of security features.

- Fraud investigation (what to do when you discover it)
- Ensure continued compliance of the design and print quality to the CDS by, for example, submitting production samples to the AAMVA CVP.
- Stimulate public and stakeholder feedback and monitoring for fraud (publications, bulletins on what to look for, how to assess fraud, and what actions to take in case of fraud).
- Encourage stakeholders to notify the jurisdiction of any fraud or fraud attempts and the results of any fraud investigations.
- Monitor national and international fraud development (stay abreast of fraud development nationally and internationally even it did not show up in your jurisdiction—it's only time before it does—fraud does not have borders).

When developing an RFP for a new contract period, include provisions that mandate an annual review of not only material and feature development.

A written summary of adherence to standards in place at the time, counterfeit threats being experienced at the time, and a review of the document's ability to withstand attack is a huge asset for the jurisdiction. This can also serve as a means to provide an annual review of the manufacturer's consistency of manufacture and quality levels being delivered.

Technology evolves and is used by license designers and criminals alike. Criminals attack the weakest elements of a system, and designs become increasingly vulnerable with the passage of time. Licenses become increasingly vulnerable to attack if they do not take advantage of new technologies as they emerge. This effect is magnified as the validity period increases. For example, a license valid for 10 years issued over the life of a 10-year contract could be using technology that is 20 years old to defend against criminals with access to state-of-the-art current technologies. The problem is even worse when the time required to design the license is added.

One approach to defending against this problem is to introduce regular technology upgrades—for example, every 5 years—that keep the defenses fresh. For contract periods exceeding this period, IAs may want to include refresh options in the vendor contract.

It is not only card security that may benefit from a technology refresh. Quality, durability, and cost improvements are also regularly achieved by introducing changes to technology and materials.

Key areas to monitor are:

- Materials
- Personalization technologies
- Security features (physical and electronic)

New developments present new opportunities for development of new and improved documents:

- Build a plan to mitigate potential problems.
- Collect and evaluate document performance metrics as input for the new or next-generation document designs (collected data on the document performance in the field identifies the areas for improvement, changes the new document design should focus on).

Final Thought

DL/IDs will continue to be targets of attack no matter what precautions are taken or countermeasures are put into place. It is not a question of stopping the attempts; rather, it is about reducing the likelihood that fraud attempts will succeed. Although we cannot hope to eliminate the threat, we can be more vigilant in our defenses and strategies. There may be no such thing as a 100% fraud-resistant DL/ID, but the final product will be exponentially more difficult to mimic and imitate for the fraudster if the prescription of this whitepaper is followed.

Annex A (informative) *Glossary of Features*

Anti-scan pattern
A pattern usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the pattern cannot be distinguished from the remainder of the background security print but when the original is scanned or photocopied the embedded pattern becomes visible.

Areas of different surface reflection
Surface embossed structure with different reflectivity/roughness, e.g. matt or glossy.

Background printing
Printed graphical security design consisting of e.g. guilloche, rainbow printing, micro text, etc. lying below or above the dynamic data.

Card blanks
A card that does not contain any of the dynamic data elements.

Card core inclusions
The opaque or translucent inner layers of a laminated card, e.g. colored or with a modulation of opacity simulating a watermark.

Chemically Reactive
Contains a security agent that is sensitive to chemicals, i.e., polar and non-polar solvents and bleach, commonly used to alter documents. The chemical reaction is for the ink to run, stain, and bleed to show evidence of document tampering.

CLI/MLI (changeable/ multiple laser image)
Combination of a lens structure integrated to the surface of the document with elements engraved or printed into a bottom layer. Resulting effect consist in multiplexing of at least 2 images each of them being visible separately depending of the viewing angle.

Core inclusions
A material which is included within the inner layers of the card body, such as colored layer. One example of this is displaying a watermark effect, another being a laser absorption layer for displaying dynamic data

Counterfeit
An unauthorized copy or reproduction of a genuine security card made by whatever means

Covert Device – Readable and Storage Technology
Unique individual Near IR or IR invisible data mark, 2-dimenional encrypted bar code, capable of storing independent information or details.

Covert variable pixel manipulation
Covert dot matrix images that are converted to visible text with a special reader or lens

CMYK colors The ‘process’ colors, cyan, magenta, yellow and black used in combination for commercial color printing, normally in the form of half-tone patterns, and by digital printing devices to approximately represent the visible color spectrum and enable the printing of ‘color pictures’.

Deliberate error A feature purposely made with an intentional mistake

Diffraction An optical effect produced by periodic microstructures embedded into material layer and producing decomposition of white light into rainbow continuous spectrum that may be seen at specific viewing angles”

Digital Seal A method of securing and validating data by electronic means using digital signature technology. The issuing authority “signs” the information contained in the MRT

Duplex security pattern A design made up of an interlocking pattern of small irregular shapes, printed in two or more colors and requiring very close register printing in order to preserve the integrity of the pattern.

Dynamic data Information specific to the document and the holder.

Effect pigments See *optical* or *non-optical effect pigments*.

Embedded data Data that is visible, encoded or concealed within a primary visual image or pattern.

Embedded thread, fiber or planchette Small, often fluorescent particles or platelets incorporated into a card material at the time of manufacture that can be seen later under certain lighting conditions. The embedded elements may have magnetic or other machine-readable properties that may be used to enhance the levels of security provided

Embossed surface pattern A design or image formed on the surface of a DL/ID, for example during the card lamination process.

Fibers Small, thread-like particles embedded in a substrate during manufacture and may include an UV feature too.

Fine Line Foreground A pattern of continuously fine lines constructed by using two or more lines overlapping bands that repeat a lacy, web-like curve.

Fluorescent ink Ink containing material that glows when exposed to light at a specific wavelength (usually UV) and that, unlike phosphorescent material, ceases to glow immediately after the illuminating light source has been removed.

Forgery Fraudulent alteration of any part of the genuine DL/ID e.g. changes to the dynamic data elements. (portrait, signature, biographical and all personal data).

Front to back (see through) register A design printed on both sides of a card that forms an interlocking image when held to a light source.

Ghost Image A lighter reproduction of the original image that appears in the same area as the personal data such that the image appears to be in the background and the personal data can still be read without interference

Guilloche design A pattern of continuous fine lines, usually computer generated, and forming a unique pattern that can only be accurately re-originated by access to the software and parameters used in creating the original design.

Half-tone image A method of representing images by printing, usually in the form of dots of black and/or colored ink. Varying tones are achieved by varying the size of the printed dots relative to the unprinted, white background area surrounding the dots.

Impostor A person who applies for and obtains a DL/ID by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that other person's DL/ID.

Infra-red drop-out ink An ink which is visible when illuminated with light in the visible part of the spectrum and which cannot be detected in the infra-red region.

Infra-red fluorescent ink In daylight invisible ink, which can only be seen when applying light in the infrared spectrum (630nm).

Iridescent ink An ink that contains transparent pigments consisting of a thin film deposited on tiny mica flakes. They cause interference with the incident light. This creates shiny, pearl-like shimmering effects with changes in color when the angle of view or illumination changes.

Laminate A transparent material, which may have security features such as optically variable devices contained within it and which is designed to be securely bonded to the DL/ID to protect the dynamic data elements and the security features within the card structure.

Laser embossing A process whereby a laser is used to create tactile elements on the card surface.

Laser engraving A process whereby a laser is used to alter the card-body material to display information. The information may consist of text, images, pictographs and security features.

Laser perforation

A process whereby information is created by perforating the card-body material with a laser. The information may consist of text, images and pictographs and appear positive when viewed in reflected light and negative when viewed against a light source.

Latent image/data

A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles. A latent image / data is – subject to the condition of the correct viewing angle – visible to the human eye without further equipment.

Lenticular feature

Security feature in which a lens structure is integrated in the surface of the document such as a changeable/multiple laser image (CLI/MLI).

Look through element

An area of the card designed to permit the transmission of visible light through the card body. The light transmitting area may be transparent or comprise grey levels.

Machine-readable technology (MRT)

Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc. Verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other machine or visual information

Magnetic media fingerprinting

Tracks unique, random patterns of magnetic media formed as a by-product manufacture of card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.

Metallic ink

Ink exhibiting a metallic-like appearance.

Metameric inks

A pair of inks formulated to appear to be the same color when viewed under specified conditions, normally daylight illumination, but which are mismatched at other wavelengths.

Micro optical imaging

Text, line art, gray scale images and multi—reflectivity images are engineered into optical WORM media at high resolution (over 12,000 dpi). Difficult to simulate the printing resolution.

Micro- printed text

Very small text printed in positive and/or negative form, that may be used in conjunction with rainbow printing and which can only be read with the aid of a magnifying glass and not exceeding 0.3mm in height.

Multi-layer card

A card-body comprising two or more layers of material securely bonded together to form a single structure.

Non-optical effects pigments Any ink containing visible or invisible pigments which is not designed to be controlled by eye such as metallic ink, magnetic ink, conductive ink, bleeding ink or which is not showing any predictable behavior upon wavelength activation.

Non-standard type fonts Type fonts that are of restricted availability.

Optical effect pigment Visible or invisible pigments incorporated in an ink which is designed to be controlled by eye, such as optically variable ink also called color shifting inks, or iridescent inks.

Optical media fingerprinting Tracks unique, random patterns of optic media (e.g., fibers) on card. The pattern is recorded at the time the card is encoded and this pattern can later be compared to the pattern detected when the card is scanned.

Optically variable element An element whose appearance in color and/or design changes dependent upon the angle of viewing or illumination, such as holograms or optical diffractive structures.

Optically Variable Ink Printing ink containing optically variable pigments which show variations in color depending on the angle of observation or lighting. Optically variable inks can be either opaque or transparent and include iridescent inks and metameric inks.

Overlay An ultra-thin film or protective coating that may be applied to the surface of a DL/ID in place of a laminate and which may contain optically variable elements.

Personalization The process by which the dynamic data elements (portrait, signature, biographical and all personal data) are applied to the DL/ID.

Personalized tactile element A surface element giving a distinctive ‘feel’ to the DL/ID, such as laser embossing (also referred to as raised laser engraving).

Phosphorescent ink Ink containing a pigment, which glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then fading after the light source is removed.

Photo-substitution A type of forgery in which the portrait on a DL/ID is substituted for a different one after the DL/ID has been issued.

Physical security The range of security measures applied within the production environment to prevent theft and unauthorized access to the process.

Pre-printed serial number on card blanks Identifier printed on card and/or on main components of the card before transfer to the personalization center(s).

Random pattern resulting in unique codes Any random feature intrinsic or individually applied to each document by any technology giving uniqueness feature that can be controlled either by eye or with any kind of tool.

Rainbow (split-duct) printing A technique whereby two or more colors of ink are printed simultaneously by the same unit on a press to create a subtle merging of the colors resulting in a gradual color change.

Redundant personalized data Dynamic text and/or image to be printed more than once for redundancy checking by whatever means.

Security background printing Printed elements that are devoted to secure blank cards and do not include any dynamic data.

Security bonding The card periphery incorporates a security bonding material that bonds all of the layers together. Tamper evidence is seen if access is attempted to obtain the internal structures of the card.

Security feature Feature of a document that is linked to a specific method of verification and thus helps insure the document's integrity and/or authenticity as a properly issued document that has not been tampered with.

NOTE: Physical security elements applied during production of a document may contribute more than one feature and therefore also cover more than one category of each kind.

Special colors Colors that are not easily reproduced using CMYK colors.

Strong adhesion Bonding between top and personalization layer high enough to prevent access to variable elements for falsification purposes.

Taggants Special materials/chemicals hidden inside the card core (plastic, composite paper or synthetic material) which can only be detected and authenticated with special equipment.

Tagged inks Inks containing taggants.

Tamper evident card body Card showing evidence of destruction or modification caused by an attack. E.g., Security Bonding

Thermochromic ink

An ink which undergoes a reversible color change when exposed to heat (e.g. body heat).

NOTE: The color change is less reactive due to prolonged exposure to heat.

UV

Ultra violet.

UV-A

No response using a light source with a wavelength between 315 nm and 400 nm.

UV dull

Substrate material exhibiting no visibly detectable fluorescence when illuminated with UV light or with a controlled response to UV at 365 nm.

UV fluorescent ink

UV fluorescent ink can be either transparent or integrated to an ink visible to the naked eye; in addition, some UV fluorescent inks can respond to standard wavelength UV light with one color and with another color to a shorter wavelength UV light, called Bi-UV.

NOTE: The UV response of fluorescent dyes and pigments is prone to fading after prolonged exposure to daylight.

Variable laser element (CLI/MLI)

Element that generated by laser engraving or laser perforation displaying changing information dependent upon the viewing angle.

Variable opacity

comprising two or more grey levels visible against a light source.

Visible evidence

Confirmed real thing by watching.

Visible security device

Security feature protecting dynamic data.

Watermark

A recognizable image or pattern that appears as various shades of lightness/darkness when viewed against a light source.

NOTE: Watermarks can be created by thickness or density variations. There are two main ways of producing watermarks in core material of a card; rolling process, and the more complex cylinder mould process. Watermarks vary greatly in their visibility.

Window element

A type of look through element with a high level of transparency.

Annex B (informative) *Conformity Assessment*

Conformity assessment is the name given to the processes that is used to demonstrate that a product (DL/ID) meets specified requirements. These requirements are contained in standards and guides. The processes that need to be followed to be able to demonstrate that they meet the requirements are also contained in ISO/IEC standards and guides.

The use of ISO/IEC standards in conformity assessment procedures allows for harmonization throughout the world and this, in turn, not only facilitates international interoperability between countries but also gives the purchaser of the product confidence that it meets the requirements.

The Courtesy Verification Program (CVP) provides an effective way for AAMVA members to determine if their driver licenses and identification (DL/ID) cards conform to the applicable AAMVA standards and specifications. AAMVA strongly encourages its member jurisdictions to regularly take advantage of the CVP. Even though AAMVA has published best practices, standards and specifications covering DL/ID cards for years, inconsistencies in the implementation of those guidelines continue to occur. These inconsistencies adversely impact the security, uniformity, and interoperability that are the main goals of the AAMVA standard.

A primary objective of the CVP is improving the consistency of implementation across all jurisdictions. Information gained from the testing of jurisdictions DL/ID cards and other documents is not only used by jurisdictions to improve their issuance systems but also is used by AAMVA to make improvements to the standards it publishes. For more information on the CVP visit www.aamva.org.

Annex C (informative) *Main Threats to the Security of a DL/ID*

C.1 Introduction

This section looks at the main threats to DL/ID security in terms of the ways in which a DL/ID, its issuance and its use may be fraudulently attacked. The purpose of this section is to provide a context for the recommendation of security features in the subsequent sections.

The threats are split into three primary categories according to characteristics of the underlying attacks: Counterfeiting, Falsification and Misuse.

C.2 Counterfeiting Threats

*A.1 Document design attacks

*A.1.1 Re-creating the basic document look and feel including such as the background pattern, flags and other fixed motives

- Copying and printing a valid document for physical manipulation
- Scanning a valid document for modification using computer software
- Re-creating of the document using computer software

*A.1.2 Adding personalization information

- Image and text editing with computer software (re-origination)

*A.2 Substitute Material/Personalization attacks

*A.2.1 Substitute Materials

- Using substitute materials to imitate original documents
  - Paper vs Teslin vs PVC vs PET vs PC
- Using original material that may be commercially available

*A.2.2 Substitute Printing Methods

- Reproduction of background and logos using alternative technologies
  - Screen printing vs offset printing vs dye sublimation vs laser
- Reproduction of text and images using alternative technologies
  - Inkjet vs dye sublimation vs laser vs laser engraving

*A.2.3 Alternative finishing

- Final lamination of the document using commercial laminates

C.3 Falsification Threats

*B.1 Falsification by physical Modification of Existing Valid Documents

- Printing directly on document, e.g. manipulation (erasing, modifying, adding) of data such as card holder

*B.1.2 Image attacks

- Complete substitution of the licence holder's portrait image
- Masking the original portrait by overlaying another photo
- Changing the original portrait to alter the appearance of the person

*B.1.3 Delaminating attacks

- Partly delaminating to remove genuine features and inserts forged ones (e.g. exchanging data by replacing the data carrying layers)
- Insert forged data or security features after adding, removing or damaging genuine ones during partial delaminating

*B.2 Falsification by Recycling

*B.2.1 Extraction of genuine security features

- Removal of security features from genuine cards (e.g. a hologram) for reuse in a falsified document

*B.2.2 Use of recycled genuine security features in a new falsification

- Applying original document parts including data storage elements into forged document

*B.3 Falsification of Logical Data

*B.3.1 Logical data denial of service attack

- Destruction of data storage elements to circumvent logical security features

*B.3.2 Logical data substitution attack

- Substitution of data storage elements such as IC's, magnetic stripes and laser recording

C.4 Misuse Attacks

*C.1 Misuse of genuine valid documents

*C.1.1 Identity Theft

- An unauthorized person using a valid genuine physical document of another similar looking person

*C.2 Misuse of Genuine Invalid Documents

*C.2.1 Invalid Documents

- Use of registered lost or stolen documents by look-alikes of the real document holder

*C.2.2 Cloned documents

- Cloning of logical data from a similar looking person

*C.3 Misuse by theft of original blank documents

This category of threats deals with the theft of original blank documents at some stage during the document life cycle up, until the point of personalization. This can be during the production of the document, during document transport, or during subsequent storage of the document at the personalization location.

*C.3.1. Theft of blank cards at the card production site

- Misappropriated during the production process
- Cards removed for quality assurance purposes
- Reject blank cards
- Taken from the intermediate production storage

*C.3.2 Theft of blank cards during the transportation process

- During card packaging
- During card transportation
- During intermediate storage

*C.3.3 Blank cards are removed from the personalization site

- From where they are stored
- During the stock issuance process
- During the personalization process
- Reject/Lost cards
- Intermediate storage

*C.3.4 Stolen blank documents personalized using alternative personalization methods that are available to the attacker

*C.3.5 Stolen documents personalized using the official equipment or using test personalization equipment

*C.4 Misuse Through the Fraudulent Issue of Genuine Documents

*C.4.1 An attacker makes a fraudulent application for an DL/ID document

- Identity theft using genuine breeder documents
- Fraudulent breeder documents

*C.4.2 Employee at the issuing authority makes unauthorized requests for DL/ID documents

- Employee bribed by an attacker

Bibliography

- AAMVA DL/ID Card Design Standard
- AAMVA DL/ID Security Framework
- ANSI/NASPO SA-2013 Security Assurance Standard
- Document Security Alliance White Paper: How to select a security feature
- ISO 14000 and ISO 9000
- ISO 14298

American Association of Motor Vehicle Administrators
4301 Wilson Boulevard, Suite 400
Arlington, Virginia 22203
703.522.4200 | **aamva.org**