Driver Licence Identification Document Security

Ian Williams - February 2001

Often in cost per card deployments a primary goal is to reduce the cost of the finished document. This is sometimes achieved at the expense of card security features. This is unfortunate today since a digitized driver licence card has become the defacto piece of identification for most people. It is commonly used for boarding an aircraft, opening a bank account, cashing cheques and a multitude of other applications where photo ID is required. Most often a holder, to provide proof of their entitlement, produces a driver licence card. Although sometimes accompanied by other forms of identification, it is the driver licence that is used most frequently, and that we rely upon.

We would strongly urge the (DMV) to fully consider the possible impact and subsequent consequential damage that a poorly designed or easily duplicated driver licence can cause. Easily duplicated licences from jurisdictions become targets for organized crime elements within North America and often from abroad, and can effect the stability of banking, economical and even political arenas. Certain security features included in the card should remain in the knowledge of the (DMV) only and not be publicly available. These are called covert security features and are discussed later in depth.

We have included the following information, which describes various security features available for identification cards.

The Documents

The evolution of security features in card documents has seen them develop into two primary categories. These categories are Overt and Covert. An example of an overt security feature is the holographic overlay currently in use by many Canadian driver licence issuers. It requires no specialized tools to observe and immediately provides a measure of security on a cursory examination. An example of a covert security feature used in card documents is Ultraviolet printing. This process applies a text or graphic to the document that is not readily visible but becomes acutely visible with the aid of an authentication device.

The (DMV) will be aware that certain security devices must be embedded in the blank card stock prior to the personalization process. Additional security features are also available for inclusion during the personalization of the DL/ID document, which will be discussed further below.

Driver License General Security Features
The following are generally accepted methods of applying data to a driver's licence or document to identify the recipient. Although not considered security features by themselves, when applied in specific manners and combined, they provide the basis for the majority of verification transactions today. Certain machine-readable technologies can assist in providing security against primitive counterfeiting. Organized counterfeiting will almost certainly have access to these technologies; thus further security features discussed later would need to be compounded.
Key to utilization of these technologies is how they are applied to the card. Overlapping, redundant data and color contrasting these fields, in addition to the card design format can allow for a certain basic level of security:

> **ID Photo** — An ID photo is the most widely used method of cardholder verification (particularly in state driver licence programs). A color picture can easily identify the cardholder as being genuine, either by visual or machine-readable verification

Printed Text — This is the easiest method of cardholder verification. The operator looks at the card and compares the printed information (a) to another ID provided by the cardholder or (b) to data stored in the card memory media, such as magnetic stripe, bar code, smart card, etc. In this case, the appropriate card reader would be required with the verification workstation.

Signature — The signature is another way that visually printed information can be verified on a card. Signature fraud is common, however, because inspectors are not professionally trained in identifying the nuances of signatures.

One-Dimensional (1D) Bar code — A 1D bar code can be used to store a unique cardholder number. The bar code can be read at a workstation, and the operator can request that the cardholder provide his or her number for verification. With this type of bar code, it is only practical to store from 10 to 15 characters, so it usually serves as a "pointer" to a record in the database if the *(DMV)* wished to query the *(DMV)* Host or central image database.

Magnetic Stripe — Magnetic stripes on cards can store more data than a bar code (up to roughly 200 bytes). The cardholder's unique number, name, and address can be encoded into the magnetic stripe and read at a remote verification workstation by using a magnetic stripe reader. The cardholder would then be asked by the operator to provide the same information (the cardholder's number, name, and address) for verification.

Two-Dimensional (2D) Bar code — A two-dimensional bar code, such as the PDF-417, can hold more information than a standard bar code or magnetic stripe. This significant amount of data can easily be used for cardholder verification. In some sample cards the bar code can store the minutiae of a single fingerprint along with textual information, such as the SSN, name, and address. For verification, the bar code on the card is read using a reader, and a fingerprint scanner scans the cardholder's fingerprint. The stored and live capture fingerprints are matched for verification. For additional verification, the cardholder would then be asked to provide other personal data that is stored in the bar code. Because of the uniqueness of fingerprints, fraud is easily detectable. (This is known as "one-to-one verification.")

Card Security -- Manufacturing and Materials

The use of plastic substrate in the production of high-security human or machine-readable documents offers, along with added durability, a level of security comparable to, and potentially greater than, the level of security inherent in traditional paper products. It is important to recognize that merely applying secure features to plastic will not in itself make a product secure. The design of usage patterns must be a key element in creating the document. A plastic card has multiple layers for embedding security features that are both machine-readable and visually detectable. Most security printing processes are consistent between the two (paper and plastic), although the application/curing of inks on plastic requires specialized knowledge and techniques. This specialized knowledge is not as easily accessible as the paper printing expertise available in today's marketplace. In itself, this offers a certain measure of protection to the issuer.

In any document, the level of security achieved is a function not of any single feature but rather of a combination of processes and features. For example, physical security and audit security at the place of manufacture and the issuance facility are both important. The following sections discuss issues of physical and audit security as well as the technical elements that combine to ensure a secure plastic card.

Card Manufacturing

A standard plastic card for the *(DMV)* should be manufactured to meet or exceed ISO Standard 7810 (*Identification Cards – Physical Characteristics*) and ISO Standards 7816-1 and 7816-2 (*Identification Cards – Integrated Circuit [s] Cards with Contacts*).

All cards should be manufactured within a high-security facility licenced for the production of secure credit cards. The requirement imposed by credit card issuers ensures that a licenced facility meets very stringent security requirements. Throughout the facility, there should be regulated and monitored procedures for both quality control and audit. Every department, from graphic preparation to shipping, has documented quality, audit, and security checks. Silkscreen and offset lithography are both used as printing processes in the manufacture of plastic cards. In addition, the lamination process that gives the card its distinctive finish is an exacting operation wherein the card is exposed to a degree of heat and pressure designed to bond together all of the elements of construction.

Card Security – The Three lines of Defense

Card security is most often divided into three categories. The first category being the most frequent verification of the document such as when cashing a check or verifying age for liquor purchases. The second category is becoming more common for patrol officers and licenced establishments where an additional verification of card authenticity is required without expensive equipment. A good example of this is occurring in taverns that have installed a small inexpensive Ultraviolet lamp next to the POS terminal or cash register. The lamp can illuminate hidden Ultraviolet inks that are printed on the card or licence, which may contain data such as date of birth. The third category is normally reserved for law enforcement forensic labs that require special equipment. Secure documents should be verifiable as original through complementary security features included for three levels of inspection:

> **First Line —** Cursory examination without tools or aids involves easily identifiable visual or tactile features for rapid inspection at point of usage
>
> **Second Line —** Examination by trained inspectors with simple equipment (magnifying glass, Ultraviolet light, machine reading equipment, etc.)
>
> **Third Line —** Inspection by forensic specialists conducting detailed examination allows for more in-depth evaluation and may require special equipment to provide true certification.
>
> The security options presented next, all allow for security to be incorporated in both the manufacturing of the pre-printed card and at the point of issuance or personalization.

In this next section more sophisticated methods of applying security features to an id document will be discussed and the relevant line of defense.

First Line Inspection

> **Laser Engraving —** Laser engraving has been used in Europe for several years on high-security plastic cards. Data is burned (or "engraved") into the inner core of the card. The information cannot be mechanically or chemically removed without damaging the surface of the card, thereby providing an extremely effective tamper-resistant barrier. It is also possible to engrave data in such a way that the outer surface of the card is "disturbed," creating a tactile effect to printing. This security feature provides another level of

verification similar to intaglio printing. However, it is extremely difficult to determine with the unaided eye if an image was laser engraved, particularly for an untrained inspector.

Laser Engraving allows personalized data, using an intense laser beam, to be engraved deep into the core of the card with the surface remaining level. Laser engraving can be performed with alphanumeric characters, digitized images (such as photos or signatures), or bar codes and OCR characters. As a result, data on the card cannot be removed via chemicals or abrasion without destroying the document. Additionally, laser engraving can print in resolutions up two 1700 dpi which far exceeds the current credit card standard of 600 dpi. This allows for micro printing of personalized data in a virtually unalterable manner. Laser engraving can also produce tactile printing which raises the text printing above the surface of the card without causing stress to the card allowing for a "Braille" type feel of the text printing. This tactile printing also penetrates into the core of the card; thus abrasion to the tactile printing would not eliminate the data.

Metallic and Pearlescent Inks — The typical appearance of metallic or pearl luster inks cannot be mimicked by color copiers or reproduced by scanning and reprinting. Although widely used for bank gold cards, the wide availability of these inks limits the security value of this feature.

Optically Variable Inks — Optically variable inks (OVI) can be incorporated into designs to create a striking color shift (for example, green to purple, gold to green, etc.) depending on the angle of light used in viewing the card. This material consists of transparent colorless ink containing microscopic, advanced multi-layer interference structures. OVI is precious, and production is available to secure printers only. Since the availability of these inks is highly restricted, true counterfeiting is unlikely. However, it is possible to create crude facsimiles that could be accepted by inexperienced examiners. For that reason, it is important to have reference standards available for training.

Rainbow Printing — Sometimes called "iris printing," this is a feature used only by selected manufacturers within the plastic card environment. Rainbow printing involves a very subtle shift in color across the document. Widely perceived in Europe and Asia as an element of a secure document design, it is commonly used in conjunction with a fine line or medallion pattern in the background of the document. Well-designed patterns cannot be accurately reproduced on color copiers or through the use of document scanners.

Fine Line Background — Commonly called "guilloche patterns," this detailing prevents accurate reproduction by copiers or standard document scanners, especially when used in conjunction with Rainbow Printing. A fine line background is constructed by using two or more intricately overlapping bands that repeat a lacy, web-like curve pattern on fine unbroken lines. Guilloche patterns are frequently printed on currency or valuable documents to raise a threshold against copying or the engraving of counterfeit plates.

Optically Variable Devices —

– **Holograms** - The metallized reflective hologram has been a security feature for Visa and MasterCard cards for more than 10 years. The intrinsic security of the hologram results from a moveable image when viewed from different angles. It is not receptive to photography, photocopying, or scanning, and it requires highly specialized equipment to replicate designs. Counterfeit holograms that have been produced for credit cards are generally poorly made and do not provide true holographic effects.

However, even poor facsimiles have often been sufficient to pass cursory inspection by an untrained inspector.

- **Transparent Holograms** -- It is also possible to incorporate holographic effects in a clear, transparent topcoat that can be applied over variable printing. Through careful design and physical registration, the clear holographic topcoat can serve as a deterrent to alteration in addition to its counterfeit protection features. If an attempt is made to remove or alter the topcoat, tampering will be detectable without the need of special equipment. Although it is possible to remove the holographic topcoat by mechanical or chemical means, once removed it cannot be recreated or replaced.
- **Kinegrams** - Kinegrams, like holograms, can be produced on a reflective or transparent material. However, unlike holograms, kinegrams only have two-dimensional effects, and effects are observable under a wider variety of lighting conditions. Also, kinegrams can incorporate asymmetric optical effects – that is, different optical variable effects are viewable, as the kinegram is completely rotated (360 degrees). Moreover, as a "controlled product," one company produces the kinegram; numerous companies produce the reflective hologram, on the other hand.

Opacity Mark — The opacity mark, which is similar to a watermark, is a plastic that contains a unique translucent opacity mark available only from a few European manufacturers. It is similar in principle and effect to a watermark found in paper documents and enjoys a high level of familiarity as a security feature.

Embossed Characters — Embossing is the impressing of raised characters to render a tactile pattern. The raised characters will also render the card uneven/not flat, thereby making the card more difficult to reprint. It is possible to develop unique embossing characters or logos that would not be included in commercially available embossers. The embossed characters can also be a repeat of the Social Security number (or some other reference tying the card to the numberholder).

Security Code — It is possible for high-resolution color printing systems to print a security code within the body of the color-printed photograph. For example, a security code can be printed in a non-proportional 2-point font that can imbed up to 20 characters on the edge or the bottom of the printed picture. The text can be printed on the image in colors that are complementary to the image or in black. This security code can be a repetition of the issued document number, an algorithm of the demographic data, or some other reference tying the document to the document holder.

Screen Traps or Moiré Patterns — Computer-generated designs can be incorporated that create variations in line frequency or modulation and reveal hidden images when copied or scanned (for example, "Void" or "Copy" will appear on photocopies, or "Original" will **not** appear on a copy). The sampling frequency of a color copying machine or scanner is "trapped" by the modified line pattern so that any attempt to copy the original will reveal the hidden image. Using highly sophisticated design software (which, in some cases, is patented) that allows for varying either dot size or the spatial frequency of lines or dots produces these patterns. Applications of this technology are referred to as "screen traps," "screen angle modulation," "sample band image coding," etc.

Redundant Data — Data can be displayed in more that one location on the ID, thereby raising the resistance to alteration. A simple visual inspection is required to determine if all data fields match. Redundant data can also be displayed in differing colors or fonts.

Overlapping Data — Variable data, such as a digitized signature or text, can be "overlapped" with another field, such as a photo image. This technique makes it necessary to alter both fields if either one of them is changed, thereby increasing the tamper resistance of the card by making it more difficult to alter.

"Ghost Printing" — Digital printing technology has made possible the printing of a "ghost" image, a half tone reproduction of the original image, which is typically printed in the same area as the personal data. The second image appears as a light background to text data, significantly increasing the difficulty of altering the photo image or the data. Any attempt at photo substitution would require alteration of the printed data as well as the ghost image. This technique is currently in use in several states as added security on driver licences.

Core Inclusion — It is possible to manufacture a plastic document with several different layers of core stock. A colored core material can be added to the card construction to create a colored edge along the card. This technique is currently used in the new INS Work Permit Card as a means of identifying a genuine document. Although possible to counterfeit, the equipment required to construct this type of card, which represents significant investment, will deter most attempts at counterfeiting.

Second Line Inspection

Machine-Readable Technologies — The card design can incorporate inclusion of many machine-readable technologies such as magnetic stripe, integrated circuit, 1D or 2D bar codes, OCR, machine-readable holograms, etc. Verification of the authenticity of the document, the data, and/or the person presenting the document can be accomplished with a card reader, depending on the technology employed. Common techniques to ensure data integrity include:

- Check digits and data encryption (presumably with public key encryption)
- For IC cards, tamper detection and chip disabling, and digital signatures for all data written to the chip.

Ultraviolet (Ultraviolet) Printing — Ultraviolet ink, which can be applied either through offset or silkscreen techniques, has long been accepted as a security feature for plastic cards. This invisible printing can be produced with the availability of a color shift when viewed under long-wave Ultraviolet light sources. Ultraviolet radiation is not visible to the human eye, but becomes visible when irradiated with an Ultraviolet light. Custom Ultraviolet fluorescing colors can be formulated that are not normally available commercially, thereby increasing resistance to counterfeiting.

Microprint — Miniature lettering, which is discernible under magnifying readers, can be incorporated into the fine line background or can be placed to appear as bold lines. Visa, MasterCard, and American Express include microprint as a standard security feature. Microprint was also added to U. S. currency in 1990. Accurate reproduction of microprint cannot be accomplished today by photocopying or by commercially available color photography or color scanners. However, the resolution of commercially available scanners and laser printers is continuously being improved. Certain techniques should be incorporated to protect against improved future reprographic devices. Such techniques include use of variable point sizes, printing on angles and on curved pattern, and using lithographic inks that are difficult to approximate with laser printer toners or inkjet inks

Directional Metamerism — Directional metamerism refers to the use of colors that differ in spectral composition but match one another under certain lighting conditions. With this technique, designs can be created that will show colors that appear to be identical under incandescent light but, under colored light, appear as different colors and patterns. For

example, a red filter could be used to identify a pattern created with metameric ink. This technique is effective against color copies and scanners.

Third Line Inspection

Specialized Inks — Special inks have been formulated with specific elements called "taggants." These elements react to electromagnetic energy sources from a remote reader. By using these inks and measuring their reflection, it is possible to identify designated card groupings or types. These taggant-carrying products are known as "smart" (or "intelligent") inks.

At the request of the (DMV), Datacard would be willing to discuss other security techniques as well as security issues or factors that may be of interest to the (DMV).

Additional Covert Security Features

There are several vendors working on developing highly secure technologies to incorporate into plastic cards. Some of these technologies are generally not known in the public domain, and should not be discussed in a public forum.

Examples of these technologies include:

- **Irregular Shape** - This can be achieved through a specialized die cut, similar to many types of secure paper documents. The die cut must be isolated to the top of the document in order to be compatible with issuance equipment. For example, a trained inspector could easily verify a slightly convex or concave shape along the top edge. If not disclosed as a security feature, the irregular shape is generally perceived to be a printing defect.

- **Deliberate errors** -- A design enhancement such as deliberate misspelling of words or reversed letters could be used as a checkpoint for verification. This is a common security feature in security documents, which is not made know to the general public, and provides a simple tool for law enforcement to check for document authenticity.

  Another variation would be a deliberate flaw in a font used for printing variable text data. A unique font could be developed for the sole use of a government agency that would have a consistently repeated flaw. Adding or deleting several pixels in a character or design could accomplish this. The flaw can be created so that it is generally unnoticed by the public, or at most would appear as a printing error.

- **Substrate Modification** -- PVC plastic manufacturers are now able to add elements to the substrate that allows identification of both the plastic supplier and card manufacturer. This is useful for forensic analysis of suspect cards, and is not a deterrent to counterfeiting.

  It is also possible to add "taggants" to one or more layers of the card construction. These taggants react with electromagnetic radiation in ways that can be readily detected. Depending how the material is incorporated, classes of cards or individual cards can be identified.

- **Covert inks** -- specialized inks have been developed which have non-visible, yet machine-readable reactions to specific light sources or frequencies.

- **Tactile Features** - A feature similar to intaglio printing can be accomplished with a plastic card. This provides a visual but transparent feature as well as a tactile feature suitable for field evaluation. This technique has been proposed for a high security card application but has not yet been adopted.

- **Core Inclusion** - It is possible to manufacture a plastic document with several different layers of core stock. Certain layers could include material that contains optical brighteners, which are available in a variety of color options. The result would be a fluorescing effect around the edges of the card when subjected to an Ultraviolet light source.

- **Ultraviolet printing for variable data** -- Ultraviolet thermal ribbon that allows printing of variable information on the front or rear of the document that will only be visible with an Ultraviolet light source. Examples of the type of data that could be printed in Ultraviolet include digitized signature, ID number, ghost image produced from the same data as the color image, etc.

  The use of Ultraviolet printing has, until now, been the in arena of the original document manufacturer. The manufacturer prints a hidden pattern or design into the document that will be invisible unless irradiated with an Ultraviolet light source. The advance possible with the Ultraviolet thermal ribbon is that the information may now be varied with each card, and therefore adds to the security of the document. Experiments have been made to produce Ultraviolet thermal ribbons in a range or fluorescing colors, although they have not been adopted for a major secure card program.

- **Specialized inks** – Special covert inks can be formulated which have unique "signatures." Normally such inks are reserved for third level examination. Portable readers have been built for some inks which would permit usage as "second level" inspection devices.

  Infrared Inks and pigments are one variety of such materials. Two classes of such inks are available. The first class of inks absorbs infrared radiation. Since the polymers used in plastic cards are transparent in the near infrared frequencies, different covert optical effects can be achieved.

  The second class are inks, which absorb infrared energy and emit visible light. These inks are extremely rare, and are only available from one U.S. manufacturer. Because these of the unique properties of these inks, they can be specifically designed to provide various levels of security.

  Prototype thermal ribbons have also been developed which incorporate these pigments. With such ribbons, critical information can be "over printed" with the card personalization equipment. This covert approach would provide an extremely high level of counterfeit and alteration protection, as the information on each card would be unique.

Card Design Considerations

Few security designs last more than a few years. Technology is moving quickly, and criminals quickly gain access to commercial products, which can produce reasonable facsimiles. The security features selected should incorporate *anticipated* threats as well as the current threats from counterfeiting and alteration.

Some security features should be included for each level of examination. Several features, by their nature, provide multiple levels of protection or deterrence. Training tools and reference aids need to be provided to the general public and to first level examiners. It must be assumed that they will be compromised. Similar tools need to be provided to second level examiners. It would be prudent to assume that these will eventually be compromised.

Third level features are typically used for investigative purposes. By the time the card gets to the lab, the crime has been done. As such their primary value comes from confirmation of excellent counterfeits, forensic analysis and the resulting link analysis. Third level features can also be "demoted" to second level, as better third level features become available.

Features should support each other. Some simple examples include:

- If Ultraviolet sensitive ink is used, there should be a visible reference point i.e., the symbol, which becomes visible under Ultraviolet light should match some other visible artwork on the card. Ideally the information printed in Ultraviolet sensitive material should be variable and reference some other variable and/or fixed information.

- Fine line, micro printing and covert material should overlap sensitive data areas to make alteration difficult. Optical variable and other tamper evident topcoats should be designed to protect critical data elements.

- If the card contains some unique characteristics, the uniqueness should be incorporated into data elements.

Some features should be held in reserve. As initial features are compromised the backup features can be announced. Meanwhile the next generation can be under development. At the same time it is useful if the card design includes some "red herrings", or features which are not actually used in examination of the card. Hopefully the criminal will spend time and effort attempting to replicate these features, increasing the barriers to fraud. By attempting to overcome these features, the criminal will likely leave a forensic trail.