Welcome to the 2003 Future Technology session of the American Association of Motor Vehicle (AAMVA) annual international conference, here in Philadelphia Pa.

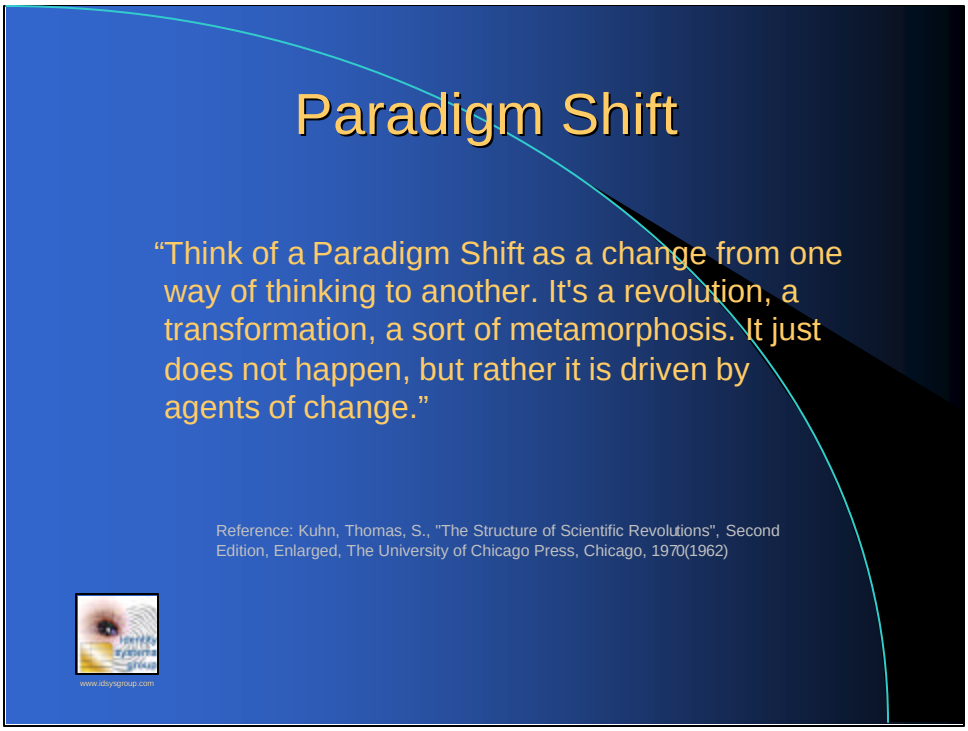
When I first spoke of Laser Engraving in Anchorage at the 1998 International, it was of an emerging technology.

Laser engraving has emerged, and in a BIG way. It is now deployed extensively in Europe and Asia. The technology is being equally applied to passport and identity card applications. As you can see from the collage, the technology is being applied in areas that require the highest level of security such as passport, national ID and driver licensing.

There are many reasons for this acceptance, but the elimination of concern regarding document fraud has been the driving force.

In the next few slides I will explain a little about the technology and how it will impact in the area of credential acceptance, and improve the overall identification process.

Laser engraving is initiating a **Paradigm Shift** in the document security world. We are realizing that if it is too **easy for us to personalize a credential**, it's equally as **easy for the bad guys to do the same**.



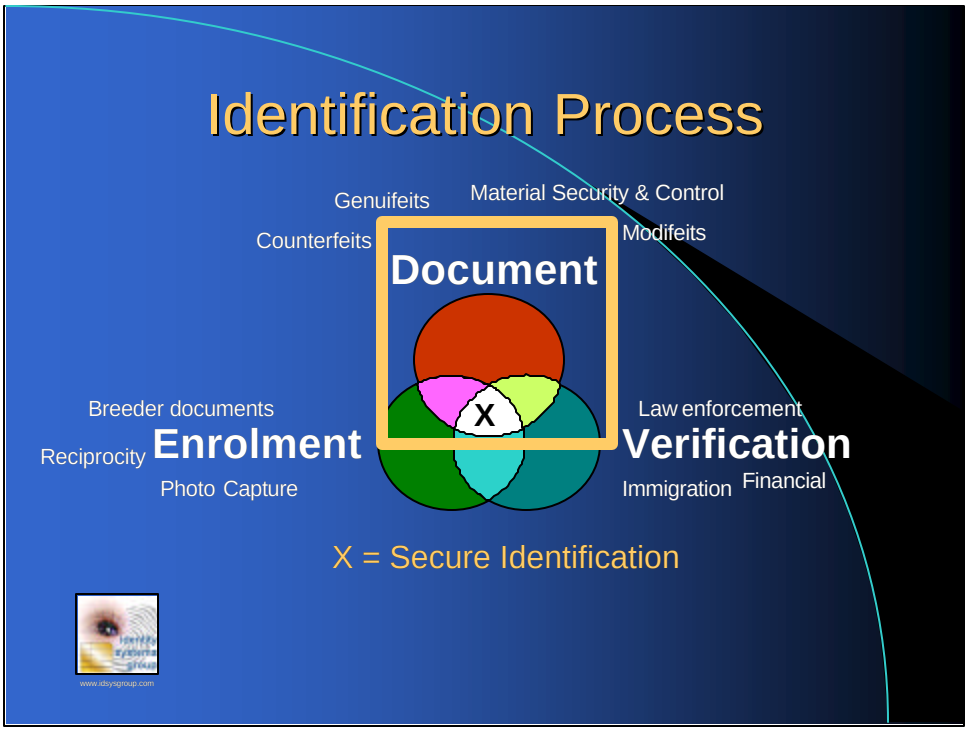
Personalization Security – some would call it a contradiction. We are familiar with the ongoing debate of centrally versus over-the-counter issuance methods. A legitimate argument, however the concern is not only regarding additional time to validate the breeder documents, it also relates to the ability to produce " documents of value" at multiple locations, with many people handling security supplies, holograms and laminates.

In both central and over-the-counter issuance better controls over card components is required, either by reducing the amount of components or the numbers of people having access to them. Document security can be enhanced by improving the auditing of card stock and access control.

However document fraud can be better defeated by eliminating the ability to perform unauthorized personalization, creation, modification or generation of cards, using widely available compatible technology, such as thermal printers, photocopiers, laminators, scanners and color ink jet technology.

"Off-the-shelf", a favorite term of the past decade in many RFP's. This term should not be applied when procuring mission critical identification card solutions.

We incurred an "agent of change" on September 11th. Prior, we spent a decade looking for easier, cheaper, faster ways to produce documents. Now we are not. This concept is a Paradigm Shift in the Driver License Document industry.



Identification is a process, not a technology. There are 3 aspects to this process:

Enrolment (validation)

Document (portable recognition of validation)

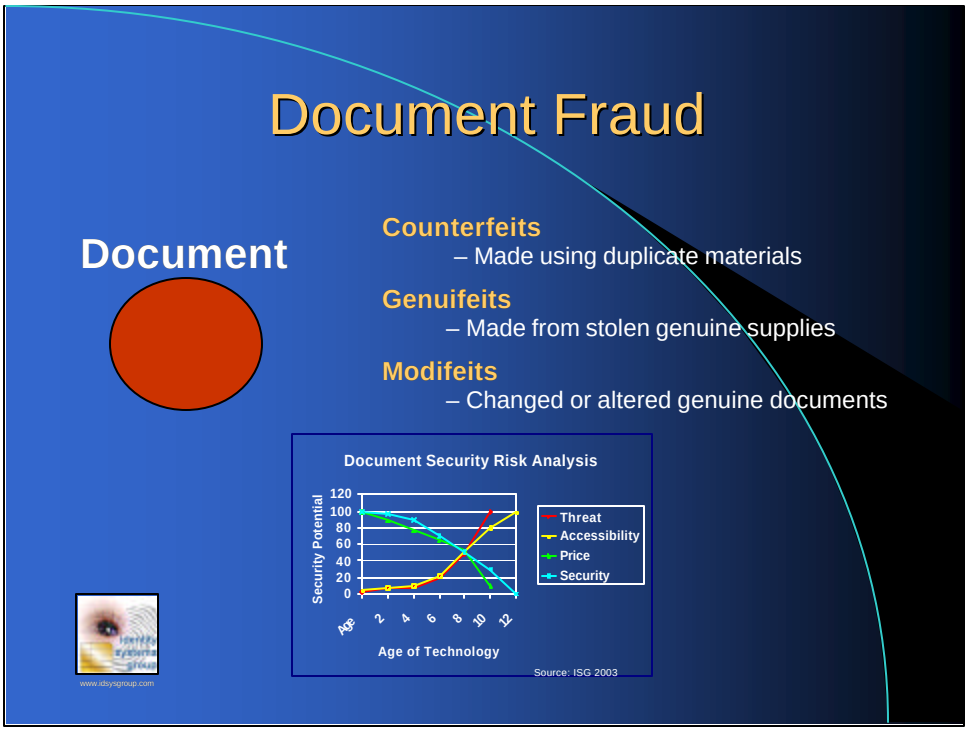
Verification (ensuring identity & document are related and valid)

A balanced approach to all three aspects is the only sure method for developing a highly secure identification application such as that required for driver licensing.

Issues surrounding the Enrolment aspect are extensive. We are aware of AAMVA's attempts to address these through the Fraudulent Document workshops and training. The third aspect, verification is also under significant debate, particularly in regard to the use of biometrics to improve this ability.

For today, we will discuss the 2nd aspect, the document. We will review some of the major concerns regarding document issuance and how laser engraving has addressed those concerns for many governments.

I will discuss the terms you see, such as Genuifeit & Modifeit in the next slide.



Document Fraud falls into three categories:

Counterfeits – these are originally produced documents from other than an Issuing Authority, generated to appear to be similar or identical to the real thing.

Genuifeits – these are very difficult to detect since they are created from misappropriated genuine supplies. They can either be personalized on the Issuing Authorities own equipment, or on similar equipment obtained by fraudsters.

Modifeits – these documents have been altered from their original appearance when provided by the Issuing Authority. The most common examples of Modifeits are altered DL's. Usually the birth date is changed to allow for the purchase or consumption of alcohol.

Document Security Risk Analysis

These factors affect the security of your document and it's resistance to fraud.. Multiple market technology increases competition which deceases it's price. This increases availability which increases your threat potential. Therefore, availability, deceasing prices and age will decease your security potential while escalating your risk or threat potential.

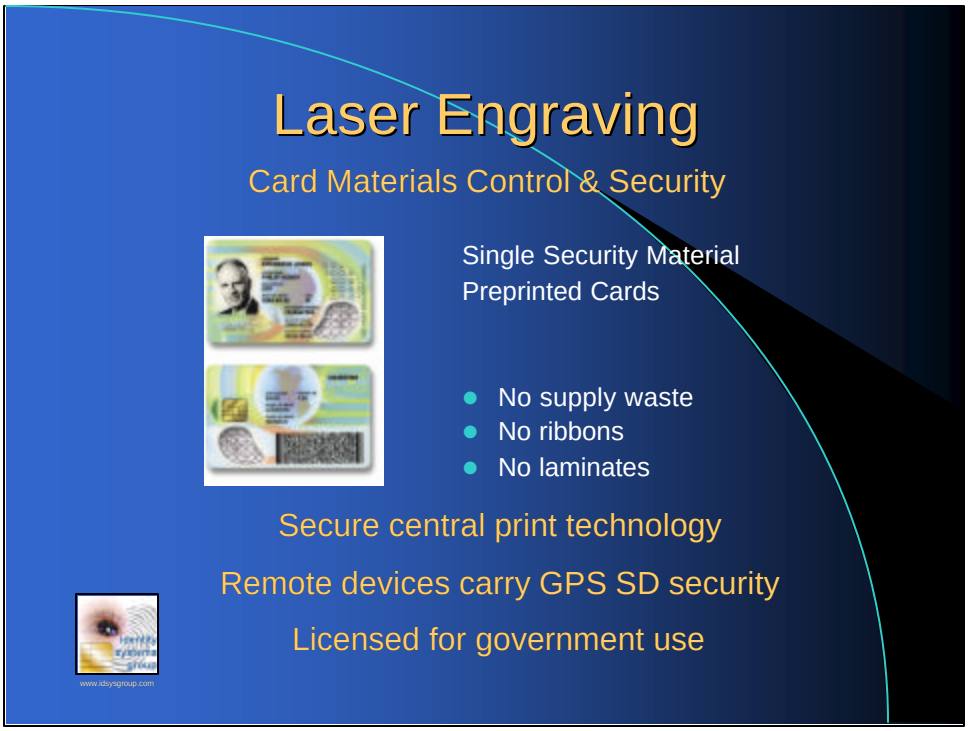
Oddly, we're here in Philadelphia for this conference. PennDOT were pioneers in Dye Sub, being the first jurisdiction to move from the old photo laminate cut 'n paste card, to a credit card type DL back in 1993. I recall this well, as I worked for the company that invented the technology and process of using color ribbons to print photos on plastic cards. Originally invented to put a photo on a credit card it was quickly adopted by the AAMVA community. Shortly after Pennsylvania implemented their Dye Sub technology, Alberta procured the same to become the second jurisdiction using "state-of-the-art technology for that era.

That was 11 years ago. This time around Alberta won't be playing second fiddle, They made sure they were the first AAMVA jurisdiction to implement laser engraving and began issuing laser engraved driver licenses last month.

There are many components involved in a dye sub application. The cards, the color ribbons, the holographic material, the durability laminates and the cleaning supplies also required. It is a process that mandates the handling of security materials often as they are depleted. Another real threat comes from the waste material. Serious security and privacy breaches have occurred as a result of the used supplies getting into the wrong hands.

An incidence of stolen DMV printers, complete with used supply on the take up reel, afforded an organized crime outfit in Canada all the data they required to issue their own licenses with legitimate information on the documents. Mind you they replaced the real photo with the members of the gang. Unfortunately lack of online image retrieval and reciprocity arrangements contributed to the security compromise.

Even if you can't swipe the printer you can buy your own, complete with supplies. You can check these out on Ebay. Lots of used DL personalization equipment is available from expired contracts. Additionally new equipment used in other markets such as college ID are available with complete sets of supplies.



With laser engraving there is one supply item. That is the secure pre-printed card.

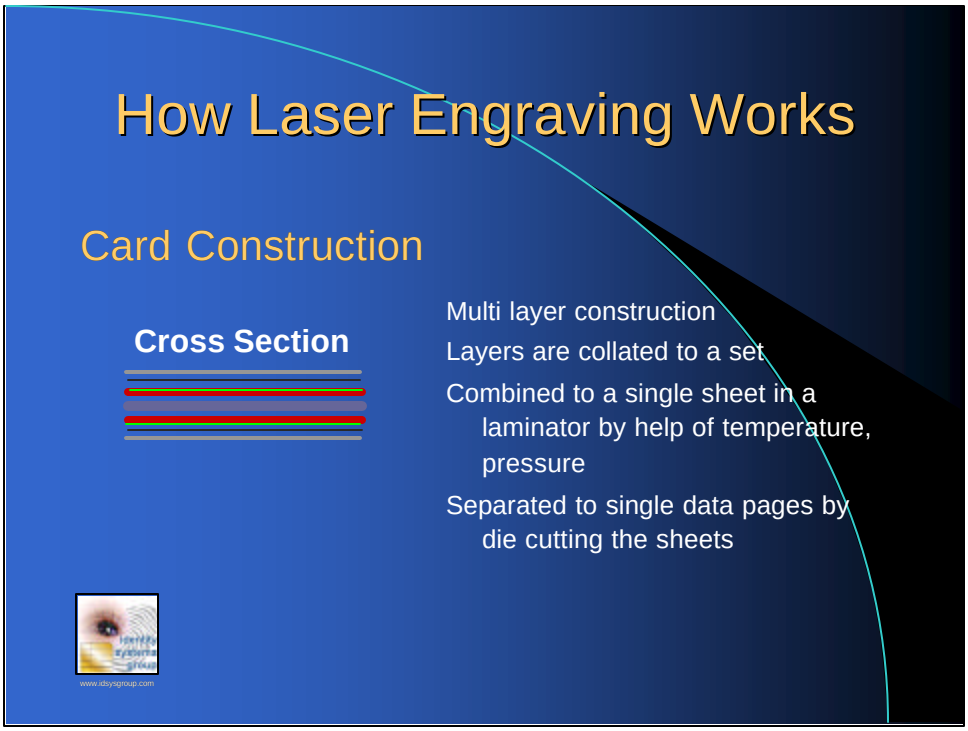
There are no waste ribbons, laminates etc. only the card. Although, some laser systems have a replaceable filter, changed periodically as part of routine maintenance.

Laser systems are typically deployed in central issuance applications. There are significant benefits to this form of issuance that will not be discussed in detail here.

However, there are over-the-counter versions of laser engraving that are available in restricted form for government use. These systems are a currently in use at sovereign embassies to allow for remote issuance of passports identical to the documents issued centrally from the same nation.

These devices carry a GPS SD (Global Positioning Satellite Self Destruct). If for example, a printer was moved beyond it's designated area (I.e. 200 metres) the satellite system tracks the printer and can immediately render the printer inoperable. Other features include biometric operator login. Attempts to disable any security feature also immediately renders the printer useless.

Many of the systems available require licensing, and are designed specifically for government use ONLY.



The laser engravable card:

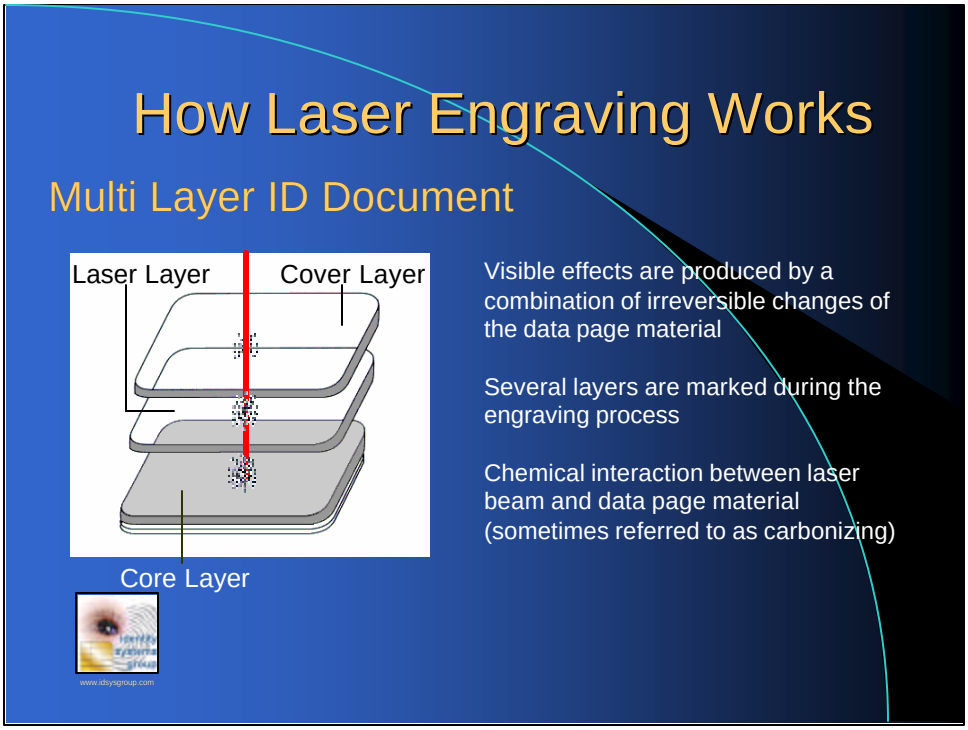
For those who aren't familiar with multi layer card construction, I just want to explain simply how a laser engravable card is manufactured.

As the cross section indicates, multiple layers are sandwiched together to create the card. This is typical of other construction methods used in the formation of highly durable cards.

In the middle you have one or multiple opaque core material layers depending on the thickness of the final product, normally 30 mil. The core layer is covered on the front - and the back side with pre-printed sheets. This pre-print includes security elements required for the card stock.

Do not try this at home folks. The process is complex due to the security elements and the special security ink. The preprinted layers are protected with a clear layer.

Between the outer and the preprinted layer we have special laser receptive layer. The laser receptive layer is required to achieve superior engraving results, including detail and mega resolution. Formed in sheets and optionally serialized individually, a die cutting process separates the single data pages.



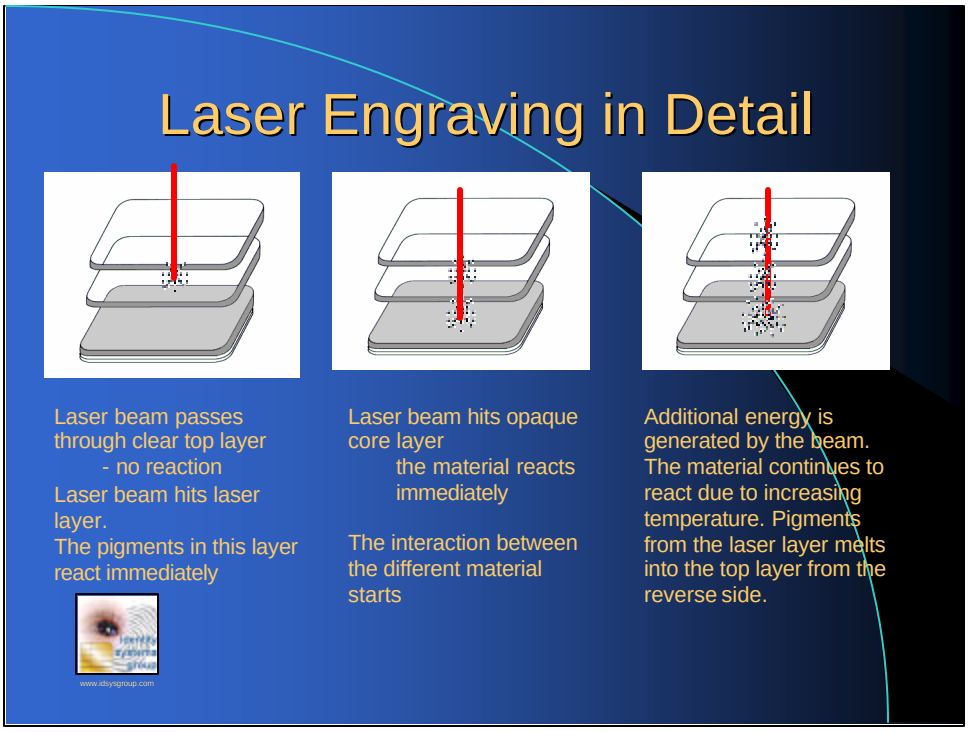
Adding text & graphics:

The laser beam penetrates through the layers to the laser receptive layer. When the molecules in the receptive layer are hit by a laser beam they change to tiny carbon bubbles. These form the black color.

All personal information including a photograph, signature, alphanumeric data and machine readable lines are laser engraved simultaneously.

Unlike dye sub or ink jet which apply inks only to the surface of a card, laser engraving data permeates from the inner core of the card to the surface and is therefore unalterable. It does not fade nor is subject to deterioration from UV light, moisture nor surface abrasion.

Laser engraving technology can print text, barcodes, images and add additional new security elements in a manner previously unavailable during the personalization process, including micro printing variable data.

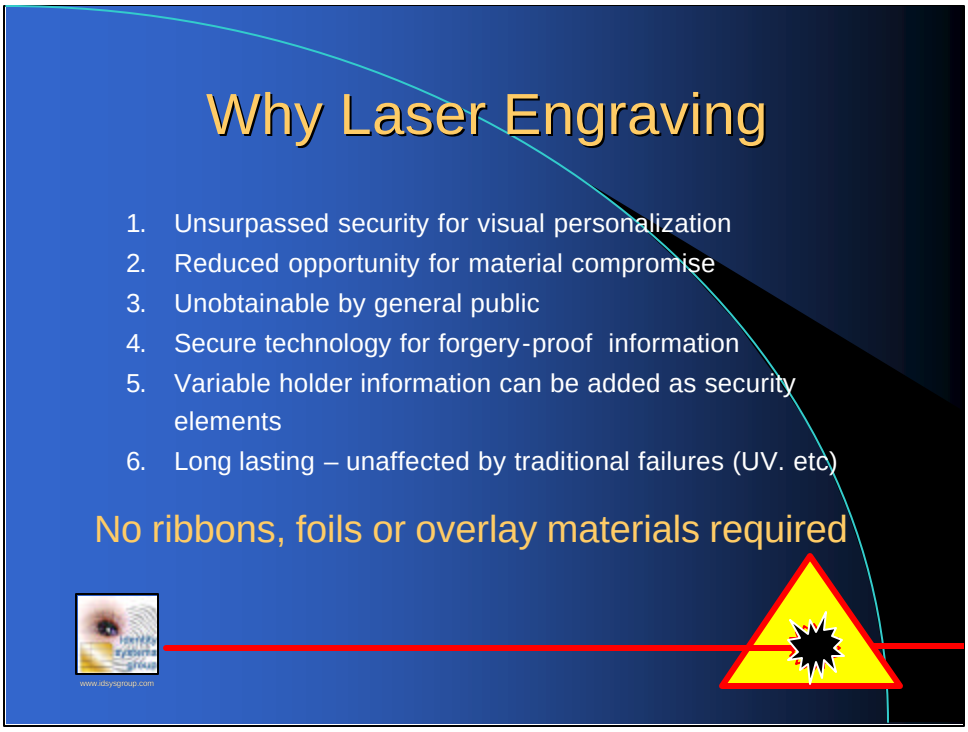


Step 1
Laser beam passes through clear top layer
-no reaction
Laser beam hits laser layer.
The pigments in this layer react immediately

Step 2
Laser beam hits opaque core layer
the material reacts immediately
The interaction between the different material starts

Step 3
Additional energy is generated by the beam. The material continues to react due to increasing temperature. Pigments from the laser layer melts into the top layer from the reverse side.

Varying the energy levels of the beam can add different security features such as tactile (raised textured) printing. The accuracy of the laser beam is measured in microns thereby resolutions for personalization, previously unattainable are now available.



Laser engraving can add all 3 levels of security to ID documents

The traditional 1st level or Cursory level can be achieved through visualization.

The second level is achieved through the tactile and high resolution security features.

The third level of security including the card authenticity is obtained forensically and can be penetrated deep into the core of the card.

The combination of polycarbonate plastic, laser engraving and the inherent security of this technology offers the maximum protection against data manipulation and forgery.

Additionally, weaknesses such as multiple supplies and sensitive data reproduction are eliminated.

I've discussed micro lettering and tactile. Let me mention Tilted laser image and others:

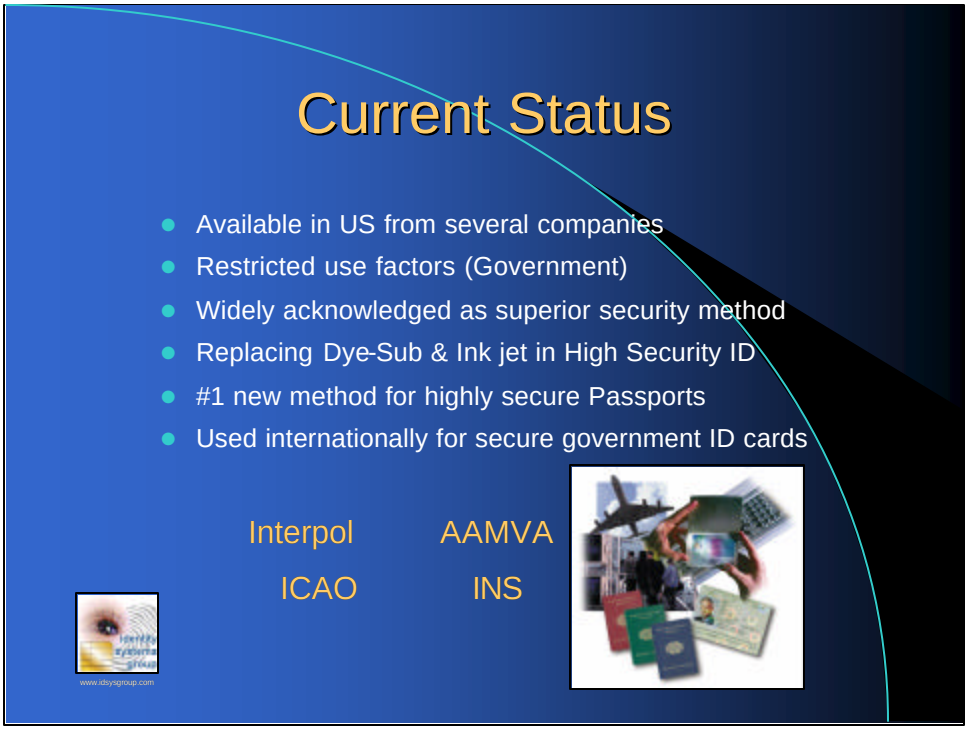
TLI or tilted laser image is achieved by burning patters into the card at an angle. This security feature allows for additional images and text to appear when the card is held at varying angles. This is useful for redundant data typically used in ID cards such as birthdate or a ghost image.

Perforated image is really neat. Tiny minute holes are burned completely through the card at varying diameters, in very close proximity. When held up to a light source, the light appearing through these holes forms an image with astonishing clarity. Typically the image is representative of the card holder. I have never seen this feature modifeited, genuifeited or counterfeited.

Again the high resolution allows for crisp clear images. Identifying marks (SMT;s) are not subjected to variances caused by color images. The DOJ mug shot image standard calls for gray-scale images. Grayscale is the preferred method of image identification in law enforcement.

I have always said that nothing is tamper proof, only tamper evi dent. I have not yet seen a successful tampering of a well designed laser engraved card. However, the technology must continually develop new features to stay ahead of future attempts to compromise it's security.

.



Laser engraving is available in the US through several companies.

Giesecke & Devrient,, Datacard and ISI -A few companies those in the AAMVA community might recognize.

Much of the products and technologies mentioned regarding laser engraving are available or licensed only to bonifide government bodies.

Laser engraving is not for the college ID or bus pass. It is a technology applied to only the most critical identification applications that meet the criteria established in your risk assessment, that approach national security.

The deployment of laser engraving is occurring at the expense of dye sublimation and ink jet. It is replacing those systems previously regarded as high security at a growing pace worldwide.

There is a noticeable gap worldwide, in government document quality. For those countries or government bodies that place significant value on sovereign security, laser engraving and other high security technologies are no longer desirable, they have become mandatory. The risk of not having the most secure document possible is just too high.

Thank you

Copies of this presentation in electronic format are available at:

www.idsysgroup.com

Contact the author Ian Williams:

ianw@idsysgroup.com

Copyright © 2003 Identity Systems Group Inc.