DOCUMENT SECURITY ISSUES

Part of a Series of Datacard Group White Papers for the Secure Document Issuer

DESIGNING AN ID DOCUMENT FOR ENHANCED SECURITY

Overview

Governments today are being driven to increase resources allocated for the design and production of secure ID documents. Advances in reproduction and printing technology have moved ID fraud into the realm of tech-savvy fraudsters, expanding the threats to secure document programs around the world. To improve security and reduce fraud, many planners today are developing sophisticated IDs with security features that are cross-linked at the time of personalization. This paper is intended as a reference for government officials considering how best to issue secure IDs. Because there are trade-offs with each model and different requirements for each issuing agency, there is no "best" method.

MARCH 2007

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

DESIGNING AN ID DOCUMENT FOR ENHANCED SECURITY

Keep it simple

Spending more on ID security does not necessarily yield better security. An ID overloaded with security features may end up being just as vulnerable as one with insufficient protection. There are numerous examples of expensive IDs which were compromised, as well as distinctive designs which issuers favored and were easily compromised.

Most experts agree that at most two or three security elements in a design can be communicated and recalled by all but the well-trained document examiner. In today's documents much of the design work is oriented toward conveying a sense of security. Some features must be included to confirm the authenticity of the document itself, complemented by other features that protect the data from alteration or substitution. The end result should provide clear, unambiguous evidence that both the document and the data it carries are genuine.

One strong security feature is not enough

A high level of security provided by one specific technology may be mistakenly viewed as sufficient to protect an ID – and in fact some vendors may promote one security element without acknowledging its limitations. An effective ID must be treated as a system, and as with any mission-critical system, includes a level of redundancy to maintain security if one element fails or is compromised.

For example, the early version of the US DoD Common Access Card relied on one visible security feature to authenticate the card. Although useful for validating the card, the security element provided no protection against alteration of the photo or personal data. Similarly, one US Government program relied entirely on the security of an IC chip embedded in the card, but provided no back-up in the event that the chip failed – either unintentionally, or because of deliberate abuse. If a primary verification feature fails, there must still be strong security features that can be used to allow an inspector to reasonably confirm the document's authenticity.

Engage Security Professionals

Developing a secure document should start with a threat analysis, evaluating the risks associated with varying levels of compromise. Unless skilled design professionals are available in-house, use of an independent security design professional is a critical step in developing a secure document. A skilled designer can incorporate a balance of overt and covert security features to minimize the likelihood of counterfeiting or alteration during the life of the document. Although many vendors are familiar with elements of a secure design, the best outcomes will likely result from recommendations by an experienced and independent design service.

Include features for each level of inspection

Some security features should be included for each level of examination. Some features are designed to provide multiple levels of protection or deterrence. Educational tools and reference aids need to be provided to the public or user organization as first level examiners. Special tools need to be provided to second level examiners, ranging from simple magnifiers to card or document readers (e.g. magnetic stripe, barcode, or IC chip readers).

Depending upon fraud threats associated with a document, designs should include features which provide counterfeit resistance to assure that an inspector can reasonably determine that the document is genuine. Traditional security printing – as used for currency – is still generally effective for 2nd level inspection. Application of an Optically Variable Device (OVD) is another important method for 1st level examination.

Assuring that the data is genuine – i.e. has not been altered or forged – may require entirely separate techniques depending on how the document is produced. For example, laser engraving or indent printing permanently alters the document substrate, reducing the threat of tampering or data substitution. Laser engraving can also be used to "disturb" the surface, creating a tactile effect useful for document authentication.

For many ID documents, transparent DOVDs (diffractive OVDs) are applied over the personal data to provide tamper evidence in the event that someone tries to alter a photo, birth date, expiry number, etc. Some transparent DOVDs are combined with laminates or overlays to also provide tamper resistance against alteration. Photos and personal data in the U.S. passport, for example, are protected by a transparent DOVD that is tamper-resistant because the overlay is so thin and fragile, and tamper-evident because an attempt at alteration destroys the OVD effect.

Figure 1
Levels of inspection

> **Level 1** - apparent to the casual observer

> **Level 2** – checked by a trained inspector with simple tools

> **Level 3** – analyzed by a forensic specialist using lab equipment

The Datacard® Optigram® laminate, and the Kinegram foil sheeting made by OVD Kinegram AG are two examples of secure, restricted-use DOVDs that can be incorporated in a document design to add resistance to counterfeiting and alteration.

Third level features are typically used for investigative purposes. Their primary value comes from forensic analysis of counterfeiting or forgery methods and the resulting link analysis. Third level features can also be "demoted" to second level as more advanced third level features become available, or in the event that second level features become compromised.

Cross-link security elements for a multi-layered approach

An emerging strategy for security is to cross-link document features at the time of personalization. The outcome is a document that has unique features that are not present in the pre-printed document, and are not generated by the personalization equipment without presence of an original document. For example, new data can be derived and embedded into a document based on the pre-numbering of that card (or data page) and personal data from the cardholder.

The Datacard® PB6500™ Passport Issuance System and Datacard® MX6000™ Card Issuance System are examples of high-security personalization systems which can add cross-linked features to a passport or ID card. The Datacard® Laser Engraving module or the Datacard® Artista® VHD Retransfer Color Printing Module can produce microtext data linked to other fields or properties of the document, yielding a cross-linked element unavailable using commercial off-the-shelf printers. The flexibility of those systems allows a new range of advanced personalization technology that can permanently link the document to the variable data on the ID. Figure 2 below is an example of a high security ID card with multiple layers of security and cross-linked data.

Protect all components of your ID "System"

Effective security for an ID document requires protecting system components. Blank documents and any custom security elements (e.g. security laminates, optically variable ink, etc.) must be produced in a

secure facility, controlled in their storage and accessibility, and transferred via secure carriers. Strong authentication methods should also be in place to control access to the system to assure that only legitimate documents are issued, and protect against data corruption or substitution during processing.

Anticipate change

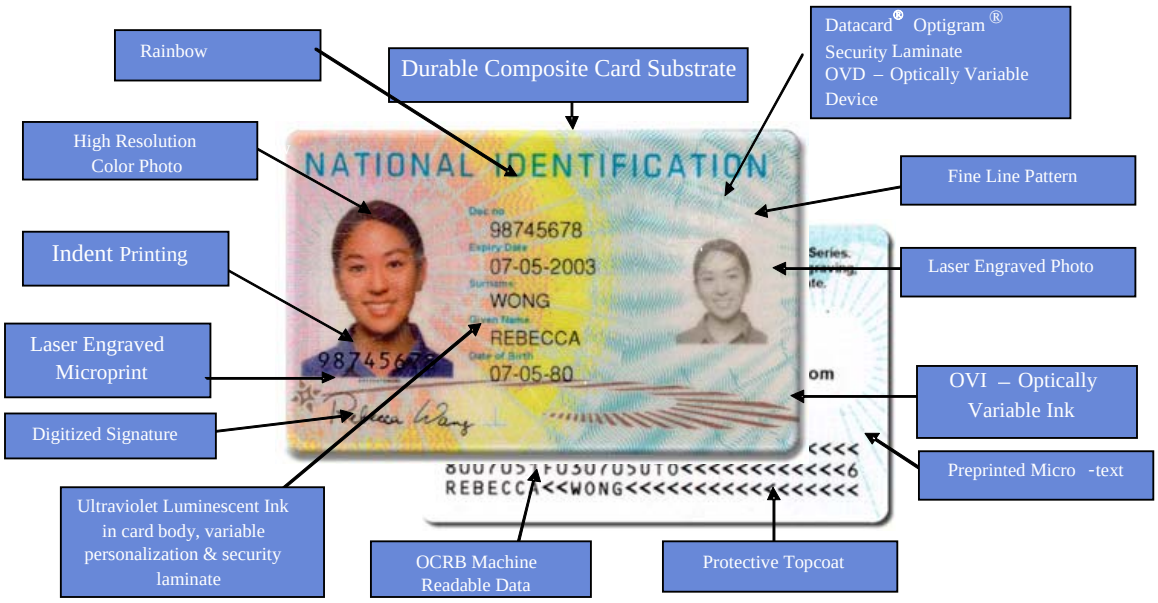
The effectiveness of security designs is now measured in a few years. For example, most currency designers expect to replace designs within 5-7 years. Technology is moving quickly, and criminals can readily gain access to the latest commercial products to produce reasonable facsimiles. The security features selected for an ID should incorporate *anticipated* threats as well as current threats from counterfeiting and alteration, recognizing that the best programs will stay only slightly ahead of the determined and well-funded criminal.

Conclusion

Recognizing that *tamper-proof* technology cannot be made, most government programs require strong *tamper-resistant* features in an ID card. Making the document difficult to alter or counterfeit is the first step in defending the integrity of an ID program. If someone is motivated to attack the ID, there must be some *tamper-evident* feature to make the alteration attempt apparent – visually or electronically. Optically variable topcoats are widely used because they are permanently damaged if alterations are made, yielding strong tamper-evidence. Ideally the OVD should be physically registered so that it protects specific data elements and provides the consistent and predictable appearance that supports document inspection.

The choice of security technologies to protect a document will always involve trade-offs between cost and security. The highest security will generally be obtained with restricted or limited use technologies, which by their nature will be more expensive. The more widely available any technology becomes, the higher the likelihood that it can be fraudulently used. Many planners today require systems that anticipate introduction of new or enhanced security features on a routine basis during the life cycle of an ID document.

Figure 2. High Security ID Card Example



Additional Resources

For additional information about security features used for secure ID documents visit:

- AAMVA – American Association of Motor Vehicle Administrators – website contains extensive information about standards, including extensive listing of available security elements http://www.aamva.org/KnowledgeCenter/Standards/
- European Union – EUR-Lex – website containing Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents http://eur-lex.europa.eu/en/index.htm
- Other standards documents are available for a fee from ISO and ICAO