

White Paper

ID DOCUMENT SECURITY

It's NOT Just "IN The Cards"

DigiOn24 team members are well experienced and have each worked in the auto identification industry and printer manufacturing for over 15 years. Larry Bowne, Vice President of Sales & Marketing, co-founder of the Document Security Alliance and a previous member of the Industry Advisory Board of the American Association of Motor Vehicle Administrators (AAMVA) provides his valuable insight and personal view on the importance of securing the ID card materials supply chain.

The information contained in this document represents the current view of DigiOn24, Inc. on the issues discussed as of the date of publication. Our hope is to create a higher level of awareness of the need to protect ID card production materials and supplies through every phase of the transportation, storage and cards production process, especially as use of finished ID card documents may impact not only America's homeland security, but the financial and personal well-being of its individual citizens.

This document is for informational purposes only. DigiOn24, Inc. makes no warranties, expressed or implied, in this document. Product and company names mentioned herein maybe the trademarks of their respective owners.

ID card security - the common practice

For many companies, large and small, and government agencies at all levels, most of the focus on minimizing ID card fraud has historically been on adding custom security features, both overt and covert, into the finished card document.

These security features, such as holograms, micro-print, and UV-visible inks, are either custom made with the blank card stock itself or applied during the card personalization printing and lamination process.

All of these security features are designed to make copying or counterfeiting of the original ID card difficult, if not impossible, and also to allow for the ready verification of authenticity of a legitimate document. To the extent that these unique security features can't be replicated by unauthorized parties, the "security" purpose is largely served.

ID card security – a security gap still exists

A significant security gap still often exists, a gap that, if not closed, exposes the issuing organization to the same risks as if the card security features were essentially non-existent: ***the failure of the organization to tightly monitor, record, and account for the legitimate materials themselves that are used in the finished ID card production process.***

As painful as it may be to contemplate the possible diversion of security materials from within an organization, it is all too often a sad fact in today's environment.

Whether the diversion is the equivalent of a single card's worth of material or hundreds, the potential risk to the organization, and possibly to the public at large, is significant.

This risk of internal diversion is in addition to the relatively infrequent, but not unknown, theft of card production materials and even card printers by parties not employed by, or known to, staff members.

ID card security – driver license issuers attack the security gap

To address this problem in large-volume, decentralized ID card applications such as State Driver License issuance, elaborate security processes and procedures are often built in to the transportation, receipt, storage, and distribution of the various components of the finished ID document.

These processes and procedures involve a combination of physical security (controlled access storage facilities such as safes or vaults) and detailed, automated record keeping of material movement and disbursement.

This material tracking is enabled by complex software, which is included in the overall issuance system utilized by the State jurisdiction. In some applications, not only are the

new, raw material components such as blank card stock, printer ribbons and laminate rolls monitored, but also items such as fully or partially used ribbon and lamination rolls and any non-issued cards (miss-prints, incorrect information, etc) are tracked and returned to a designated area for proper destruction and disposal.

The return of all used card printer ribbons for destruction is of critical importance, since all of the variable information on the finished card is retained on the ribbon panels, allowing for easy duplication by “dumpster divers”.

ID card security – business & organizational risk reduction when issuing ID cards

ID cards issued by organizations, both private and civil, often allow user access to physical areas and to property, property both tangible and "intellectual".

In addition, ID cards may also contain sensitive personal data that could be used in identity theft or other criminal activity.

It is incumbent upon the issuing organization to recognize its risks and responsibilities in creating and distributing ID documents, and to take the appropriate steps to install adequate safeguards that insure such risks are minimized.

Security issues to consider when evaluating your organization’s ID card issuance process and procedures:

1. Is the inbound and outbound transportation, receipt, and disbursement process clearly defined and documented? How? Who is responsible?
2. Is the material movement through the receipt, storage and issuance process recorded by date, time and quantity, as well as being directly linked to the requesting/receiving user?
3. Are all sensitive materials kept secure and limited to authorized access?
4. How are inventory levels of key materials monitored to determine re-order points for long lead time/custom materials (i.e. special hologram laminates)?
5. Are used/partially used materials (ribbons, laminates) tracked against new inventory & card production to identify possible diversion?
6. Are used or defective supplies, as well as rejected "finished" cards, properly destroyed? How?
7. Is record keeping and accounting adequate to record unique lot or item serial number data where appropriate?

ID card security - summary

Unless and until satisfactory answers can be provided to the above questions, the security and integrity of your entire ID card issuance process cannot be assured.

ID card document security... It's NOT Just "IN The Cards"

About DigiOn24

Based in Simi Valley, California, USA, DigiOn24 develops and manufactures contactless proximity encoders for card printers as well as secure inventory printer cabinets and software that protect sensitive supplies and track user access and inventory transactions.

For more information please visit our web site at www.digion24.com or contact us at 805-584-9884.