CARD MANUFACTURING™
The Official Publication of the International Card Manufacturers Association
August 2021 Volume 31 • No. 4

ADVANCED TECHNOLOGIES

DRIVE CARD DEVELOPMENT INTO THE FUTURE

Biometric Cardholder Authentication

Pioneering the Way with Security

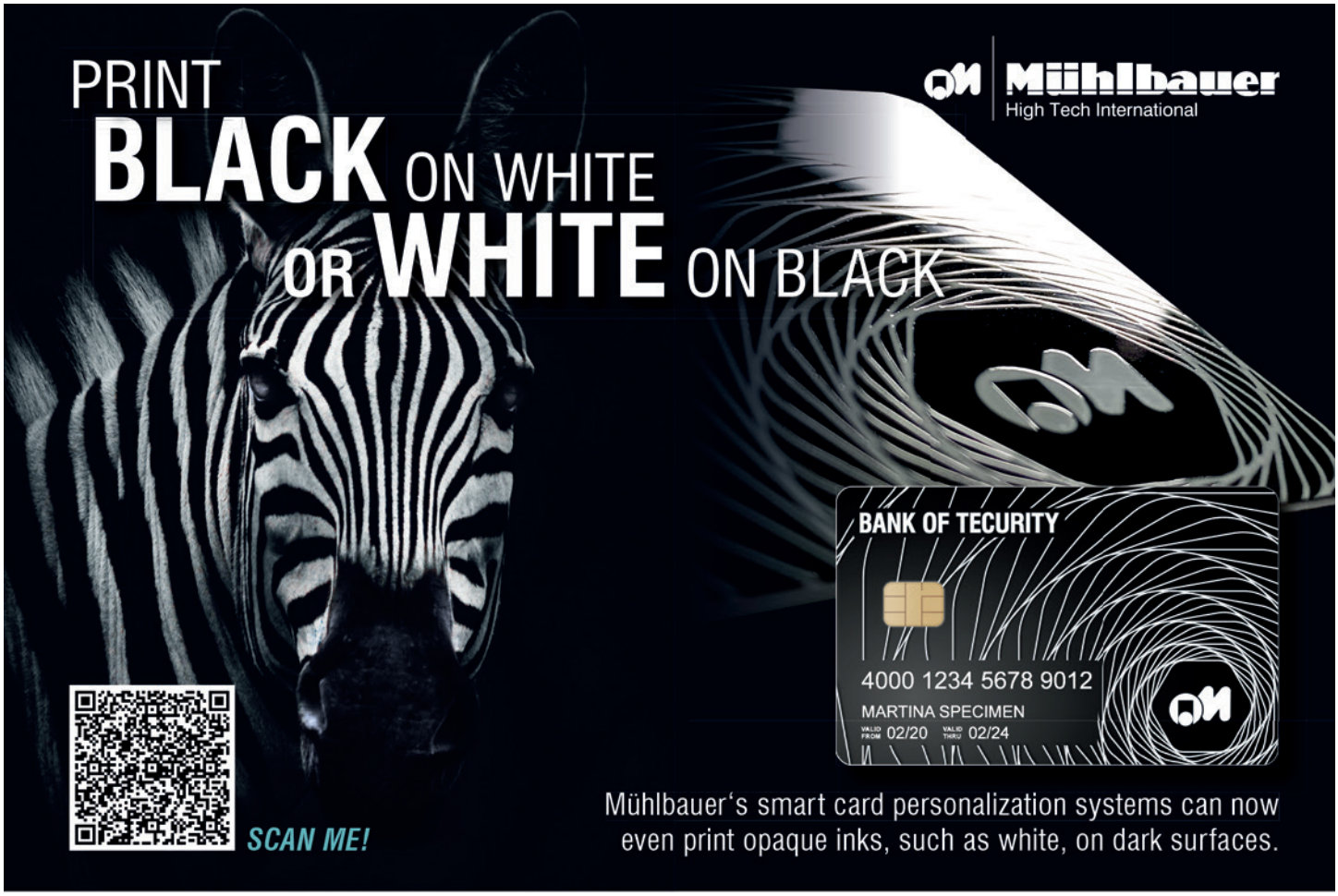
Why Digital IDs Won't Replace Physical Identity Cards Any Time Soon

Selecting the Right Ink Technology for ID Card Printing

Bringing Security to Contactless Biometric Payment Cards

PRINT BLACK ON WHITE OR WHITE ON BLACK

Mühlbauer
High Tech International



SCAN ME!

Mühlbauer's smart card personalization systems can now even print opaque inks, such as white, on dark surfaces.

MÜHLBAUER SCP 2000

CARD PERSONALIZATION TAKEN TO A NEW LEVEL

- Personalize up to 2,000 cards/hour - horizontal or vertical
- Suitable for ID and Banking Card applications
- MB Alfresco® printing technology combines inkjet printing and laser personalization for higher security card personalization
- Print vibrant colors on many different surfaces - drop-on-demand

MB Alfresco®
winner of Elan Awards 2020

Élan AWARDS

www.muehlbauer.com

CARD MANUFACTURING

is published by CMA for ICMA. Please submit all articles, news releases and advertising to:

CARD MANUFACTURING™
C/O: CMA
191 Clarksville Road
Princeton Junction,
New Jersey 08550 USA

Founder/Executive Director
Jeffrey E. Barnhart
jbarnhart@icma.com

Operations and Member Experience Manager
Michael Canino
mcanino@icma.com

Association Manager
Lynn McCullough
lmccullough@icma.com

Managing Editor
Jennifer Kohlhepp
jkohlhepp@icma.com

Membership Coordinator
Nicole Lauzon
nlauzon@icma.com

Project/Advertising Sales Manager
Diane Webster-Sweeney
dwebster@icma.com

Public Relations Director
Ken Hitchner

Marketing Manager
Kelsey Tweedly

Social Media Specialist
Natalie Spangenberg

Creative Director
Dave Sherwood

Founder Emeritus/Industry Advisor
Albert J. Vrancart
avrancart@icma.com

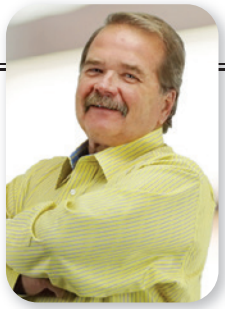
TELEPHONE
1-609-799-4900

WEBSITE
ICMA.com

E-MAIL
info@icma.com

International Card Manufacturers Association
icma

Card Manufacturing™ publishes information for the benefit of its members and readers. The sponsor, International Card Manufacturers Association (ICMA), the publisher and the editors of *Card Manufacturing*™ cannot be held liable for changes, revisions or inaccuracies contained in the material published. For more detailed information on the products, programs, services or policies covered in *Card Manufacturing*™, it is recommended readers contact the appropriate person, company, agency or industry group.



Enter the 2021 Élan Awards of Excellence!

By Jeffrey E. Barnhart

With hundreds of entries from around the globe each year, the Élan Awards of Excellence celebrate the world's most impressive cards and card technologies.

The competition, which was designed to drive innovation within the card industry, recognizes winners in three categories—card manufacturing, personalization & fulfillment and card suppliers. Judging is based on a quantifiable scoring system with criteria in nine categories. Winners will be announced during a special ceremony at the 2021 ICMA Card Manufacturing and Personalization EXPO from November 7-10 in Orlando, Florida.

Open to ICMA members only, entries for the 2021 Élan Awards of Excellence are due by September 1. The competition honors world-class achievements in the following categories: Secure Payments Cards; Loyalty, Promotional and Gift Cards; ID and Access Control Cards; Personalization & Fulfillment Product, Service or Project; Unique Innovation and Best Supplier/Vendor New Product, Service or Innovation.

New in 2021: The judges will select an award winner for each segment in the new Feature Cards category—biometric cards, environmentally friendly cards and metal cards.

An Élan Award is a status symbol, showcasing a company's expertise in the card manufacturing industry. Winning can also lead a company down multiple paths to success, including new business opportunities and high-profile visibility.

Experience the prestige of winning an Élan Award. Visit ICMA.com to enter the competition.

from the ICMA staff

Register Now to Attend Our 2021 EXPO

By Michael Canino

Network and get the essential education you need to excel in the global card industry by attending our 2021 Card Manufacturing and Personalization EXPO.

This in-person event, scheduled for November 7-10 at the Renaissance Orlando at SeaWorld in Orlando, Florida, will offer an abundance of networking opportunities, including the chance to meet top card suppliers, personalizers and manufacturers in the exhibit hall.

The EXPO also features a comprehensive conference program including expert presentations on card design, card manufacturing equipment, advanced technologies driving the industry into the future as well as environmentally friendly materials and sustainable plant operations.

ICMA members who register to attend the event prior to September 10 will receive a discounted rate of $995. Non-members who register to attend prior to September 10 will receive a discounted rate of $1,595. After September 10, the member rate is $1,195 and the non-member rate is $1,695.

Register to attend now at ICMAEXPO.com.

CARD MANUFACTURING

contents

VOLUME 31 • NUMBER 4
AUGUST 2021
ICMA.com

RECURRING SECTIONS

3 Founder/Executive Director's Message

28 EXPO News

30 Member & Product News

33 Industry News

36 ACE News

37 Association News

FEATURES

6 Biometric Cardholder Authentication

A card employing biometric technology would be able to both conduct a contactless transaction with the point of service and a contactless authentication of the cardholder.

| By David Tushie, Magellen Consulting, ICMA Standards and Technical Representative

8 Pioneering the Way with Security

René Stoerk, sales director card systems at Atlantic Zeiser, reports on why drop-on-demand inkjet technology has become so widely accepted and why demand for this type of government ID card is growing today.

| By René Stoerk, Sales Director, Atlantic Zeiser

12 Why Digital IDs Won't Replace Physical Identity Cards Any Time Soon

Around the globe, governments and national ID issuers continue to use physical ID documents and cards for a variety of applications and services.

| By Jennifer Kohlhepp, Managing Editor, ICMA

16 Selecting the Right Ink Technology for ID Card Printing

Understanding that not all print technologies are equal—and the basics of how they work—is essential to selecting the right solution.

| By Jim Meier, Senior Director of Product Marketing, HID Global

THE SPOTLIGHT IS ON ICMA'S PLATINUM AND GOLD MEMBERS

These suppliers have committed to the highest level of support to ICMA activities in 2021.

Platinum Level

D&K Group, Inc. Laminating Films and Equipment

kp klöckner pentaplast

Mühlbauer High Tech International

Gold Level

apollo colours

Atlantic ZEISER a coesia company

GTUS

SICPA

VFP Ink Technologies

COVER STORY

20 Bringing Security to Contactless Biometric Payment Cards

A contactless payment card with on-card biometric authentication offers an opportunity to replace forgettable and insecure PINs with a solution that not only offers a superior user experience but enhances security and reduces fraud.

| By Henrik Nilsson, Director of Product Management Payments & Access, Fingerprint Cards

New eZ-Inkjets Card Systems

Industrial Inkjet Print: Solutions I Software I Systems I Components I Supplies I Service

eZ-Inkjet Family of Printers

eZ 33mm — Low Cost DOD UV Printer
eZ 54–108mm — Hundreds Sold
eZ 65mm — Extra Speed (up to 1,000 ft/min)
eZ 120mm — New Epson Based Printer
eZ Colorjet 100mm — 4-Color Process

New Systems: TransitRunner, EMV-Duplex and EMV Runner.

Windows 10 SUPERTRACKER Controller

Upgrade to Windows 10 For PCI DSS Compliance
eZ Upgrade - Same Hardware and Software Interface
No Need to Re-train Staff - Even Runs Same Jobs

EMV-eL RFID Perso Line

Low Cost and Great Versatility
ID1 / CR80 product size
Includes Feeder, 8 Foot Stepper Transport
8 RFID Antennas, eZ-Inkjet, Camera, Conveyor
Base price starting at $150,000

Check Out Our New Website
www.graphtech.us

Easy Upgrades of Atlantic Zeiser, Datacard, Profold and CPST lines

2021 Trade Shows: PACK EXPO • PRINTING UNITED • ICMA EXPO
Printers and Systems Are Proudly Manufactured in the U.S.A

Made 100% in America

Call for a live Demo:
772-569-0066
or email
sales@graphtech.us

We'd love to hear from you!

Card Manufacturing **contains feature articles, listings, events, company news, industry announcements, association updates and other information that will influence and grow your business.** ***Card Manufacturing*** **also includes messages from key industry executives as well as news and tips from the heart of the association—YOU.**

- **Interested in submitting a bylined feature for an upcoming issue?**
- **Do you have company information or accomplishments you want to share?**

Please forward all news submissions, including press releases announcing new products or services, new hires, promotions, major contracts and acquisitions, milestones, community activities, case studies and any other industry news to Managing Editor Jennifer Kohlhepp at jkohlhepp@icma.com.

BIOMETRIC CARDHOLDER AUTHENTICATION

David Tushie – Magellan Consulting, Inc.,
ICMA Standards and Technical Representative

Like all things with cards, especially technology on cards, cardholder authentication has seen long evolutionary change. When cards were in a rapid growth phase in the 1970s and 1980s, authentication was largely by signature. Most secure cards had a signature panel on the card, most transactions were "attended" by a merchant or service provider employee and signature on a receipt could be compared visually with the signature on the card. With the introduction of unattended, card-operated transactions, like those at ATMs, another automated means of cardholder authentication was needed.

The introduction of PINs at ATMs was the first attempt at fulfilling this need. Typically, the card issuer would generate a PIN for the cardholder and require them to memorize this (four-digit) number. Frequently, as was/is common with passwords today, the cardholder would write the PIN number on the card signature panel, defeating the security of the card if it was lost or stolen. Most cardholders had several cards, each with a different PIN, and found it difficult to memorize each specific card's PIN. Thus, the customer-selected PIN became a common feature for card issuers to offer.

Many non-secure cards, particularly gift and loyalty cards, were issued with no cardholder authentication required. Such customers were often warned to treat their cards as "cash" since anyone in possession of the card would be able to transact with it. However, with the introduction of PINs and specifically, customer-selected PINs, these card issuers were now able to offer this option of a higher level of fraud deterrence.

Most recently, we see the COVID-19 pandemic driving the demand for contactless interaction at the point of sale (POS) or points of service. Financial transaction cards at the POS with "tap and go" functionality are in high demand. Will we be seeing similar uptake in demand for gift cards as consumers prefer contactless transactions? Similarly, the same question exists for secure ID cards at the points of service or admittance. Likewise for access control cards used at unattended points of entrance like buildings, rooms or doors. Will contactless demand drive the technology on these cards and the resultant means of cardholder authentication?

It appears as though biometrics on cards are the next technology advance to address this need. With an embedded sensor in the card body, a stored cardholder biometric like a fingerprint or signature/voice recognition characteristic can be compared to the actual person using the card. If the comparison matches, the transaction is allowed to be completed. No central database of biometric data, only a direct match of the physical cardholder with a biometric that is stored only in the secure memory of that specific card.

A card employing this technology would be able to both conduct a contactless transaction with the POS terminal or point of service reader and a contactless authentication of the cardholder. The cardholder, for example, would hold their thumb over the fingerprint sensor on the card while tapping the card reader. When the

card determines that the cardholder is authenticated, it passes that information to the reader as part of the data necessary to successfully complete the transaction.

For many years, the card industry has developed sophisticated chip technology that processes cryptographic functionality and secure protection of data. These are all low-powered chips that are able to operate from the radio frequency (RF) energy supplied by the reader devices. Biometric sensors have evolved to this same level of sophistication whereby the RF field is able to power them as well. No battery is required on the card to accommodate these capabilities.

Cost is always a factor in card manufacturing and the cost of biometric sensors is not trivial. However, consumer devices like mobile devices and laptop computers commonly use biometric authentication for access to their use. The sheer volume of these devices will drive the cost of these sensors to an affordable level in cards, particularly as card production adds to that volume. We only need to look at recent history with EMV card volume and its impact on the price of chip cards to see evidence of this effect.

A bigger factor for card manufacturers to consider is the effect these developments could have on card production. The implications may be most acute for some non-secure manufacturers who have not had much experience with chips, antenna or inlay components. Production equipment, employee technical skills, inventory management and new supply chains will all need to be evaluated and addressed as this trend comes further into focus.

About the Author: *David Tushie, ICMA standards and technical representative, has had a long and continuing career in the card industry, working for international companies such as DataCard, UbiQ and NBS Technologies. He has master's degrees in engineering and business, holds U.S. and international patents in measurement and card issuance systems and has had several years of involvement with the ANSI, INCITS and ISO Standards process. ICMA is represented at six ISO and ANSI Standards Meetings through Tushie's standards role within the association.*

PIONEERING
THE WAY WITH SECURITY

René Stoerk – Sales Director, Atlantic Zeiser

Ten years ago, drop-on-demand (DoD) inkjet technology began to be used in the personalization of government ID cards, voter IDs, driver's licenses, etc., opening entirely new prospects. Two arguments in favor of DoD were particularly persuasive at the time.

René Stoerk, sales director card systems at Atlantic Zeiser, who has been with the company since the very beginning, reports on why the technology has become so widely accepted and why demand for this type of government ID card is growing today.

What was Atlantic Zeiser's role in introducing DoD technology for ID cards?

We were one of the first to use this technology to print and personalize ID cards of all types, starting in 2011. This was very much a revolution in this area. No other provider on the market has since commissioned as many DoD technology systems for government ID cards as we have.

Did people immediately recognize the potential of this technology?

Oh, yes. They saw it right away. But in this area, you often deal with agencies and organizations that perform sovereign tasks, so to speak. They are always interested in new technologies but are often a bit hesitant to actually use them. But we were able to quickly overcome this tendency and convince them finally.

What specific advantages were especially important to potential customers?

We had (and still have) two convincing arguments on our side: One is that thermal transfer print, which dominated the area, is not very resistant to abrasion and is also susceptible to tampering. The other is that we could prove that costs per card are far lower for DoD technology than for thermal transfer or ribbon print.

Can you be more precise?

The costs for consumable materials for DoD printing are more than 70% less than those for thermal transfer print, which is, of course, an impressive argument. That is why DoD technology pays for itself several times over in a very short time. Another important factor is that abrasion resistance is four times as high for UV-cured DoD ink than it is for thermal transfer printed cards. DoD technology makes it easy to have a service life of 10 years or more that is required for ID cards.

What role does print quality play for ID cards?

That was another decisive factor. DoD technology's advantage is especially pronounced when it comes to integrating color photos into ID cards. This is because of its extremely high resolution and the brilliant quality of its color printing.

But you could also use a laser to print in color.

That is true. But using a color laser is very, very expensive, and one of the reasons for that is that it often requires a special card material. And color laser throughput is relatively low. We use laser technology in our systems where needed—primarily as an additional security feature. We laser the black parts of an image into the card material and then DoD-print the color. Even if someone were able to remove the ink, the card would remain practically unusable for a new overprint. DoD and laser are thus a strong and especially secure combination—it gives us the best of both worlds.

There are lots of ID applications. Are DoD technology systems limited to a particular segment?

On the contrary: one of the biggest advantages of these systems is that they are particularly flexible and can be used in a number of ways. ID cards, driver's licenses, health insurance cards, voter cards with or without chip programming: it can all be done on the same system, job changes

continued on page 10

Pioneering the Way with Security, continued from page 9

are easy, and the only requirement is the addition of new modules or software. And in some countries, the systems are used in a wide variety of ways for various applications. For instance, they are currently being used for "COVID cards"—for government services during the pandemic.

How can a company distinguish itself in the DoD technology arena?

You have to be able to do more than completely master the actual DoD inkjet printing process and pretreatment and curing processes. Ideally, you would also be able to develop and adapt inks for specific materials, surfaces and applications. Then there are workflow technologies that support full "rainbow deck" capability.

And by that you mean the function that allows customization of each individual card on the fly without setting up the system for a new job?

That's right. To use that function, you need additional inspection systems that uses the "rainbow deck" data stream to allow inline inspection without any additional set up. It is also important to have a secure data management environment that supports "security printing" levels of data protection and traceability.

Where do you see challenges in the future?

There is no question that security feature requirements will become more stringent. In this area, we are pursuing various approaches, such as special varnish or invisible ink, both of which we are able to apply inline. At the same time, the need for ID cards is growing very quickly worldwide. One reason for this is that many countries are just starting to provide their populations with counterfeit-proof ID cards of all types. Another is that many countries require replacements when existing cards need to be switched out for cards with chip personalization (in the area of health care, for instance). These developments are increasing the demand for solutions that can handle large orders quickly and reliably and can also deliver small batches at reasonable prices.

About the Author: *René Stoerk is the sales director at Atlantic Zeiser for the card printing, personalization and mailing systems that the company has been offering since 1998. He has initialized the development of a global strategic network aligning with digital personalization pioneering DoD ink jet technology in the card industry for many card applications since then. René Stoerk stands for more than 40 years of experience with global government organization offices for passport, ID and health card projects.*

ENDURA Overlams™

SECURE

ATTRACTIVE

DURABLE

TURNKEY

Get a Platen Press Look With Roll Lamination

5+ year Card Validation

NEW ENDURA Overlams Are:

- Waterproof
- Chemical Resistant
- Impossible to Delam
- Affordable

Patent Pending

Contact D&K for Samples and More Information

www.EnduraOverlams.com

D&K Group, Inc.
Laminating Films and Equipment

800-632-2314
info@dkgroup.net

Jennifer Kohlhepp – Managing Editor, ICMA

WHY DIGITAL IDs

WON'T REPLACE PHYSICAL IDENTITY CARDS ANY TIME SOON

As civilization moves toward more digital interactions and the verification associated with them, coordinating physical and virtual world credentials becomes increasingly important. Both physical and digital credentials must verify that you are who you say you are. They also have to be validly issued from an authenticated authority.

Physical ID documents and cards still play a major role in identity authentication—and in many ways will be closely tied to virtual credentials as the rollout of digital IDs continues throughout the world. Rather than simply being replaced by new digital formats, they continue to be the pre-requisite for the overall success of many schemes, according to a recent report from the Secure Identity Alliance.

Around the globe, governments and national ID issuers continue to use physical ID documents and cards for a variety of applications and services. Here's why:

Smartphones Aren't Ubiquitous

Portable and easy to present and validate by authorities without having to rely on mobile network connectivity or coverage, physical ID documents and cards continue to offer the ideal solution for citizens who can't or won't carry a smartphone or who live in locations where mobile coverage is limited.

"There will always be a need for a physical identification method and physical credentials must be considered a part of the citizen identity ecosystem," said Martin Hoff, product marketing manager, Instant ID Issuance at Entrust. "While mobile devices can be used to effectively store and present digital credentials, not everyone has a smartphone. Physical smartcards should work hand-in-hand with digital credentials to ensure a wide range of use cases and smooth interactions for citizens around the globe."

Trusted Digital IDs Rely on Physical IDs

Digital identity is one of the most significant technology trends on the planet and, for a growing number of public stakeholders and citizens, it's already a day-to-day reality. With specific credentials (i.e., a unique ID number in India, a mobile ID in Finland or Estonia or an eID card in Germany, Italy, Spain or Portugal), it can be used to authenticate its owner.

"The value in digital IDs is the ability to provide more citizens greater access to public services like health care, education and government benefit programs in a convenient, seamless and secure way," Hoff said.

A trusted digital ID is created by conducting three general steps: capture, verify and digitalize. The subscriber's ID information is captured from a physical identity document like a passport or card, such as a driver's license or national ID. After it has been captured, the system verifies the authenticity of the ID document or card with dedicated software. A digital ID may be created after a match is established between the biometric data and the identity document or card.

Multi-Layered Security Provides More Security

The combination of a physical card with a digital identity is powerful and provides multi-layered security. The two form factors together present a highly secure, highly personalized ID that cannot be easily counterfeited, providing significant cost savings to the governments that deploy them.

An example of physical and mobile ID co-existence is the Irish Passport Card, a highly controlled, highly

continued on page 14

Digital IDs, continued from page 13

secure document that allows travel across borders in the European Union. Irish citizens can apply and pay for their passport card using their mobile phone. Speeding up the enrollment process dramatically reduces the issuing agency's overhead and administrative costs while improving citizen convenience without compromising their privacy. In the end, a physical card is still issued, although the security protocols including authentication of a citizen's credentials was done online in advance, ensuring that the card issued is a "genuine" ID.

When it comes to highly secure government applications, physical cards and mobile IDs can work together as part of a total multi-factor authentication of what a person knows, such as a password or phrase, what a person has (i.e., a physical card) and something they are (e.g., a registered fingerprint that can be read by a biometric scanner). As demand for multi-factor authentication continues to rise in the interest of increased security, so too will a hybrid approach to credential deployment.

This year promises to be another big one for digital IDs—and secure physical credentials and cards will certainly play a role in that. Look no further than Estonia, which has by far the most highly developed national ID-card system in the world and still deems the physical credential necessary. Much more than a legal photo ID, the mandatory national card also provides digital access to all of Estonia's secure e-services. The chip on the card carries embedded files and, using 384-bit ECC public key encryption, it can be used as definitive proof of ID in an electronic environment.

HID

CARDS AND PRELAMINATES FOR EVERY APPLICATION

Part of ASSA ABLOY

HID cards and prelaminates combine innovative radio frequency identification (RFID) technology with industry-leading knowledge in the production of secure credentials. Proven processes and automated manufacturing ensure efficient and cost-effective production. We will make standard and custom configurations to fit any specification.

Powering **Trusted Identities** | Learn more at **https://hid.gl/ICMA** or scan the QR code.

©2021 HID Global Corporation/ASSA ABLOY AB. All rights reserved. Part of ASSA ABLOY

SELECTING THE RIGHT INK TECHNOLOGY FOR ID CARD PRINTING

Jim Meier – Senior Director of Product Marketing, HID Global

Organizations producing high-resolution identification cards have an array of card printers from which to choose. Understanding that not all print technologies are equal—and the basics of how they work—is essential to selecting the right solution.

Most identification cards produced today are still personalized using direct-to-card or reverse transfer color resin printing technology. Over the past decade, however, dye sublimation printing has become the leading color application technology of choice. It is a far superior application method than that of color resin and when paired with reverse transfer printing technology instead of direct-to-card printing, produces the highest quality images on the most durable cards. This is especially true for cards containing embedded technology such as proximity circuits, contact chips, or contactless integrated circuit chips.

Superior Image Quality

Dye sublimation printing creates various continuous tone colors within one individual dot or pixel of an image. It achieves this through a diffusion process that melds colors together into a smooth, continuous tone, and is capable of producing more than 16.7 million colors. Color resin printing, however, requires groupings of ink dots to signify one single color, lowering the resolution of the image. Illustration 1 below compares the resolution of dye sublimation printing to the resolution of color resin printing. Dye sublimation produces continuous tones that truly achieve the stated printhead resolution of the printer, either 300 or 600 dots-per-inch (dpi).

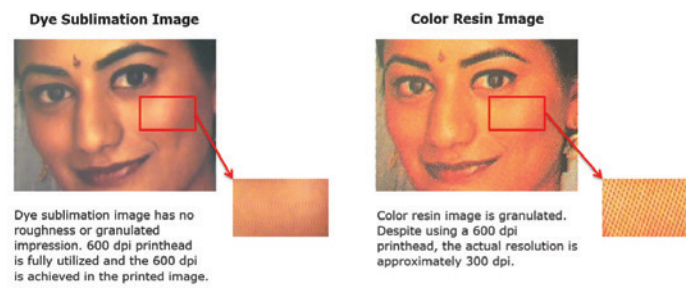


Illustration 1. Dye sublimation printing results in superior resolution

Color resin printing uses yellow, magenta and cyan to create only a limited range of colors as compared to dye sublimation. A single color is represented by a grouping of individual colored dots placed adjacent to one another. Even though resin printing may use a 600 dpi printhead, the actual quality of a color resin printed image remains only 300 dpi.

Images produced by dye sublimation technology are crisp and of realistic photographic quality. They achieve 600 dpi resolution by fully utilizing printhead capability. The dye sublimation process diffuses the dye, eliminating granulation while producing much greater image clarity. Dye sublimation printing diffuses the dyes together into a single dot on the card surface, producing higher levels of resolution than is possible with resin printers.

Color Comparisons

Color resin printing uses pigment-based colors while dye sublimation uses dye-based colors. As shown in Illustration 2 below, pigment inks do not accept light in the same way as dye inks. Dye inks focus light, while pigment inks reflect light. The larger size of pigment particles means they tend to scatter the light they reflect, which leads to less vibrant color. Small dye ink particles reflect light evenly for more vibrant color.

Because of this, dye-based inks provide superior image color, and consequently, better quality images.

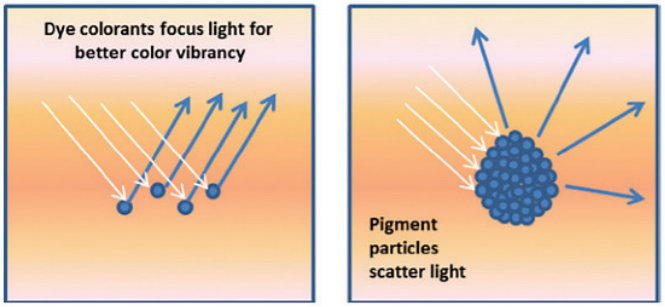


Illustration 2. Dye-based colors are used in dye sublimation printing. Pigment-based colors are used in color resin printing. Dye colorants reflect light evenly, while pigment particles scatter light.

Some colors are not reproducible by color resin technology. Certain graphics, logos and precisely reproducible Pantone® colors are not available using color resin printing technologies. Specifically, Kodak Corporation stated that pigmented inks are less suitable for the simulation of Pantone® and specialized spot colors, which are especially popular in today's corporate brand palettes. Better colors, plus the full gamut of actual colors, result in the highest quality print images.

Dye sublimation printing technology also utilizes color gradation more accurately. Therefore, images are clearer and better defined, allowing images with less contrast to be produced more accurately. This is important when creating small photographic images such as those typically printed onto identification cards.

Eye and Facial Recognition

Recognition of a person's eyes is a crucial part of photo identification. Fine detail is more accurately reproduced with dye sublimation printing which gives greater resolution to the eyes (see Illustration 3). This enables convenient and accurate visual identification.

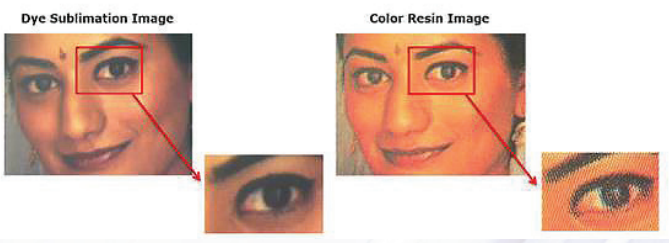


Illustration 3. The superior eye resolution of dye sublimation is crucial for facial recognition.

continued on page 18

Ink Technology, continued from page 17

Full color reproduction capability is even more significant when printing a wide range of skin tones. One of the key reasons for using a facial image on a card is easy recognition of that person. Dye sublimation's high color image quality is a crucial factor in getting the desired results of an identification card.

Printing Technology Methods

There are two primary methods of applying text and images to identification cards using dye sublimation technology—direct-to-card and reverse transfer.

In direct-to-card printing, images are printed directly to the surface of the card through heat and pressure. The printhead comes into direct contact with the card. This method is less than ideal when producing technology cards because the printhead is coming into direct contact with the uneven surface of the technology-embedded card.

In reverse transfer printing, images are first printed onto a clear film. Through heat and pressure, the film is then fused to the surface of the card. The printhead never comes into direct contact with the card surface. Technology card surface imperfections—such as smart chips that are not even with the card surface and ridges caused by internal RFID antennae—do not affect the print quality.

It should also be noted that cards produced with reverse transfer printing technology are innately more secure and durable than other types of cards because they are inherently tamper-evident—if a counterfeiter tries to peel apart the layers, the image essentially destroys itself. They also resist wear and tear by putting a durable layer of reverse transfer film between the card image and the outside world.

For enhanced card durability, protective overlaminates provide an ideal solution. For enhanced security, overlaminates can include holographic images and other Visual Security Elements (VSEs) resulting in credentials that are easy to verify but hard to duplicate.

Reducing Susceptibility to UV Fading

An overlaminate with holographic images can be adhered to a card using heat and pressure. Overlaminates are used to provide additional durability from abrasion, and add holograms and other security features, and protection against fading. Specifically, they effectively protect reverse transfer dye sublimation-printed cards whose dyes may fade over several years. Accelerated UV light testing of these laminated cards has shown fading is imperceptible to the human eye.

Another important consideration is the adhesion of the laminate to the card. Significant efforts have been made by overlaminate and reverse transfer dye sublimation manufacturers to ensure that the overlaminates remain securely fastened to the card. In a preliminary test on a limited number of color resin printing technology identification cards, the overlaminate did not remain securely fastened to the identification card.

In contrast, overlaminates that had been developed specifically to work with dye sublimation printed cards did remain securely adhered. With years of testing and field use, overlaminate failure on dye sublimation reverse image transfer cards has proven very unlikely (see Illustration 4).

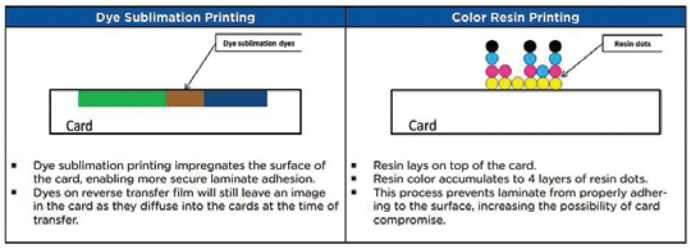


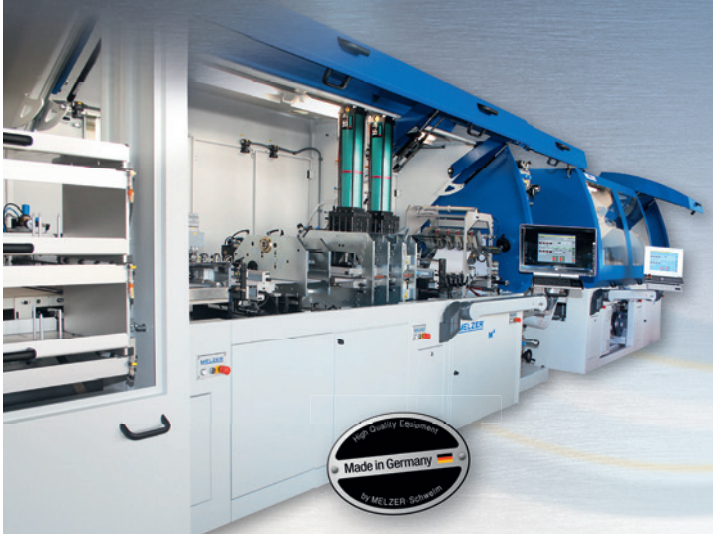
Illustration 4. Visual explanation of how dye sublimation enables more secure laminate adhesion.

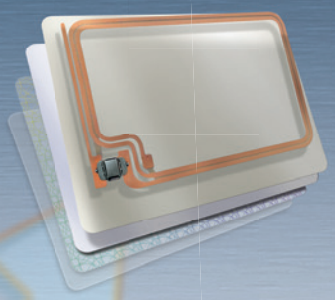
Quality, Durability and Security

Reverse transfer dye sublimation printing technology is superior to color resin printing technology and is the clear solution of choice for technology-based identification cards. Not only does reverse dye sublimation printing technology deliver the best photo and text print quality, it ensures that finished credentials are durable and highly secure.

About the Author: *Jim Meier is a senior director of product marketing with HID Global and manages the portfolio of desktop printer products. He has more than 25 years of experience working with printing technologies and has 20 patents related to these technologies.*

High Speed Inline Production of RFID Inlays





- All types of antennae
- Plated, wire embedded, printed, etched
- Up to 2,400 inlays/hour
- Including lamination and cover application

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

www.melzergmbh.com

BRINGING SECURITY TO CONTACTLESS BIOMETRIC PAYMENT CARDS

Henrik Nilsson – Director of Product Management Payments & Access, Fingerprint Cards

1. BIOMETRICS IN CONTACTLESS PAYMENT CARDS

1.1 IMPROVING THE USER EXPERIENCE OF CONTACTLESS

In the last decade, contactless cards have seen rapid adoption, especially across Europe, enabling users to simply 'tap' to pay without the need to enter their PIN code. In markets where contactless is highly used, 59% of consumers want to use their contactless card more but remain prohibited by the payment limit. However, fraud remains a significant consumer concern too. Without additional authentication, research shows that among users of contactless cards, 38% say contactless cards don't feel secure and over half (51%) are very or extremely concerned about fraud. The result is that 30% of all users with contactless cards don't use them[1].

In an effort to increase trust and reduce fraud, the EU launched Payment Services Directive 2 (PSD2), implementing new strong customer authentication (SCA) requirements. A user can be authenticated by three types of factors:

- **Ownership:** Something the user has, for example a payment card, physical keys, smartphone or security token.
- **Knowledge:** Something the user knows and remembers, such as a password or PIN code.
- **Inherence:** Something the user is or does, for example a fingerprint, signature, voice etc.

SCA requires two of these authentication factors, meaning when it comes to payments the user needs to present the card itself plus must provide either a knowledge or inherence factor. In action, this reduces the number of contactless payments, requiring PIN-entry more frequently as the default second factor of user verification. But the security of PIN is limited, and its user-experience is poor.

1.1.1 THE PIN PROBLEM

Consumers are overwhelmed and frustrated by the number of PINs and passwords to remember in today's digital age. And, if they forget their code, there is the added inconvenience of needing to issue a new card, which is a significant cost to banks, too. 20% of European users have the same PIN for more than one payment card, while 16% share their PIN with family and friends[1], heightening the PIN's vulnerability to fraud. The PIN is also susceptible to over the shoulder or "shoulder surfing" attacks, where an attacker gleams the PIN when it is being entered by the user.

In light of the COVID-19 pandemic, the PIN code also creates hygiene concerns. With the WHO encouraging contactless payments where possible[2], consumers are keen to avoid interaction with shared payment terminals wherever possible.

A contactless payment card with on-card biometric authentication offers an opportunity to replace forgettable and insecure PINs with a solution that not only offers a superior user experience, but enhances security and reduces fraud. With added trust to "tap" card payments, banks can also feel empowered to finally remove the contactless payment limit, increasing transaction numbers.

With biometrics, contactless cards can meet SCA requirements and alleviate consumer fraud fears, without impacting the seamless UX.

1.2 TECHNOLOGY FOR BIOMETRICS SYSTEM ON-CARD

Biometrics in its simplest sense is capturing unique physical features to identify the user, such as the iris, face, and fingerprint. It has been immensely successful in the mobile phone market with over 70% of all shipped smartphones now including biometrics[3], with fingerprint commonly replacing the PIN to unlock devices, making payments and secure applications.

The extensive R&D and market advancement during the smartphone world's mass adoption of the technology has readied the technology for integration into new form factors. Fingerprint sensors can now be manufactured in high volume at low cost, are compact and robust. Performance has been optimized too. This can be largely measured by the False Acceptance Rate (FAR)—that is, misidentifying a third party as a legitime user—which, in modern sensors for payment cards standards at a rate of misidentification of one in over 20,000.

The world of payment cards is complex, however. Bringing biometrics to cards requires careful consideration and

continued on page 22

Contactless Biometric Payment Cards, continued from page 21

innovation to integrate biometrics seamlessly, and with the highest levels of security, into the form factor.

1.2.1 BRINGING BIOMETRICS TO PAYMENT CARDS

A smartcard for payment is a standardized card with a payment application running on an on-card, highly secure processing platform called a Secure Element (SE), also known as the card's "chip." The card is inserted into a payment terminal or Point of Sale (POS) and the card and POS communicate via electrical connectors on the card.

A contactless payment card is both powered by and communicates with the payment terminal. The terminal generates a field (typically at 13,56 MHz), that the card then harvests the energy from to power the SE and other electronics on-card. The field is also used by both the terminal and the card to send commands and responses, the communication uses Secure Channel Protocol (SCP03). Typically, a PIN entered by the user on a terminal is sent via the field to the SE on-card to verify the user by comparing the received PIN with the PIN stored in the SE.

A BSoC, or biometric system on-card, is a contactless smartcard that also incorporates the fingerprint sensor needed to capture the user's biometric features, with the algorithms and processing power required for the matching process. It is worth noting that before a user can use a biometric system, they need to be enrolled. During enrollment, a biometric template that represents the user's biometric features is created and stored securely on the card. This template is then utilized to match against the user features captured during subsequent authentication attempts. The on-card data flow during a customer verification operation can be divided into four main steps:

1. Image capture
2. Image processing
3. Feature extraction
4. Biometric match against stored template

The image processing and feature extraction can be implemented either on a separate processor or the card's SE. The biometric match and storage of templates is always implemented on the SE, due to its robust security levels.

2. THREATS AND THREAT ACTORS

When developing any security solution, it is crucial to map the threats and threat actors. For payment cards, these are thieves looking to use the card either to make fraudulent payments or as an entry of attack on the payment system itself. An individual thief may have quite some experience, but normally lack the expertise and resources to develop advanced attacks. An organization however can have both the expertise and resources to develop advanced attacks which can then be performed by individuals.

The primary threat is to use cards that have been lost or stolen. The PIN protects against fraudulent payments for larger sums but as mentioned earlier, the PIN is vulnerable to "shoulder surfing" attacks, where a person is looking over the shoulder to see the PIN that is entered. This kind of physical attack is limited and not scalable however, as the thief must learn a new PIN for each card. Although such attacks are troublesome for the individual, what thieves really want are attacks that are general and can be applied directly to all cards or that do not even require a physical card. The potential monetary gain is much larger, and an organization is therefore more prepared to spend resources finding such attacks. Considering attacks on biometric systems, it's also a major security benefit that any spoof attempt is a "one shot" only—the thief only has one attempt to try and compromise a biometric system, unlike a traditional door lock that can be tried several times or attempting to guess a PIN code.

The threat actors are after monetary gain. And while biometrics offers an answer to some of the vulnerabilities of PIN, careful consideration is still needed to mitigate the vulnerabilities any new security solution has.

Nothing is ever 'un-hackable', but the goal of any security solution is to make attacks either too expensive or too complex to be feasible at any scale.

The attack vectors from one to seven are:

1. **Biometric spoofing.** This means something other than the user's finger is used on the sensor to try and trick the matching operation to accept the spoof as the correct finger, called presentation attack. The spoof could be a latent fingerprint on the sensor that is reactivated or an artificial fingerprint, for example.
2. **Replay or manipulation of sensor image data.** Replay or manipulation of sensor image data requires the ability to inject a sensor image instead of an image from the sensor. The image could have been captured from the same sensor at a time when the legitimate user used the card but is replayed later.
3. **Manipulation, disturbance of image processing and feature extraction.** The sensor image is processed, and biometric features are extracted. The attack attempts at disturbing the processing and extraction in such a way

that the biometric match accepts features it receives from the extracted image of the user's fingerprint.

4. **Replay or manipulation of biometric feature data.** If the attacker can gain entry to the interface between feature extraction and biometric match, a replay or manipulation attack is possible.
5. **Manipulation, disturbance of biometric match processing.** The attack tries to influence the biometric match processing to produce a positive match result even though the extracted features are not from the user's finger. This can even happen when no features have been extracted.
6. **Injection or manipulation of template in storage.** The biometric template, the asset created during user enrollment and used to match the features, is either modified or replaced to allow payments using the user's card.
7. **Replay or manipulation of biometric match result.** The final match result is modified or replayed to fool the rest of the payment system that the legitimate user was verified for a payment.

2.1 ATTACKS AND SCENARIOS

Looking at the on-card data flow again, there are several attack vectors that can be identified where a threat actor can try and influence the operation of a BSoC.

3. SECURITY FOR BIOMETRIC PAYMENT CARDS

3.1 MITIGATING THE THREATS

3.1.1 PROTECTION AGAINST SPOOFING

Spoofing involves the forgery of faces, voices, fingerprints etc. to try to authenticate fraudulently. Many advanced technologies have been developed to minimize the risk of spoofing. In fingerprint authentication, for example, spoofing risks have been significantly reduced by the introduction of active capacitive sensors. This meant conductive 3D prints would be needed that resembled the texture of a real finger to trick any system—a far trickier task to achieve.

Discriminating between the user's finger and someone else's—or indeed, a forged finger—directly relates to the quality of the sensor and the biometric algorithm. By increasing the image quality and using sophisticated matching algorithms, modern sensors now make creating a successful spoof require considerable time, money, skill, and care. A sophisticated biometric algorithm paired with a state-of-the-art sensor for payment cards is able to provide better than 1/ 20,000 FAR - far harder to achieve than guessing a PIN which, by comparison, has a rate of 1/10,000. Additional security can also be achieved by use of more than one biometric identifier to authenticate the user.

The opposite of FAR is FRR—False Rejection Rate, which means that the authorized user is misidentified as a non-authorized user. For the user, a false rejection is an inconvenience. The ideal biometric authentication system has minimal FAR and FRR, but in reality, biometric authentication systems are somewhere on a curve where you either have high convenience (low FRR) but lower security (high FAR), or vice versa. Striking a balance between these is crucial. A sophisticated biometric algorithm pushes the curve down and provides high convenience while at the same time maintaining high security levels. Modern matching algorithms also include detection and protection against different types of spoof attacks.

continued on page 24

Contactless Biometric Payment Cards, continued from page 23

3.1.2 PROTECTION AGAINST INJECTION AND REPLAY OF SENSOR IMAGE DATA

Injection and replay mean replacing the sensor itself with a device that provides an image instead of the sensor. The image provided can be the image of the user's finger captured at an earlier payment, and now replayed to trigger more payments.

Authentication of the sensor image allows the on-card host (the processor or SE) to verify that the image originates from the sensor, not another device. Replay protection allows the host to verify that the image received was captured in that moment and a response to an image request from the host, not a replayed image.

The inherent privacy of on-device biometric systems also provides protection against leakage of biometric information needed for a subsequent replay attack. All biometric data is stored and processed on the device in the case of personal authentication, and the biometric template that is created is entirely unique to that device.

As such, the same finger would create a different template when enrolled on another consumer device. This means attacks are considerably harder to scale and the ability to attack a secondary system that the user is enrolled on are considerably reduced. Better connection between the sensor and the SE is also fundamental to ensuring strong data protection, as it moves sensitive information and processing away from the vulnerabilities of the sensor to the robust protections of secure chip technology. Privacy is crucial to consumers—especially in the modern age of data protection. The consumer's data stays with them at all times on their device and is kept secure, never leaving the card.

3.1.3 PROTECTION AGAINST MANIPULATION OF BIOMETRIC PROCESSING AND TEMPLATE STORAGE

These types of attacks target the execution of the biometric software. Attacks can consist of fault injection attacks, or inversely measure effects such as variance in time, power consumption or in electromagnetic fields caused by the execution. These are types of side channel leakage that are then used to optimize fraudulent inputs. This process is known as a hill climbing attack.

The robustness of the processor execution and protection mechanisms against fault injections, as well as the protections against leakages, provides the necessary defenses against these types of attacks. Again, high quality biometric algorithms and how the algorithms are implemented also impacts how sensitive the biometric processing is to these attacks.

The perfect combination of hardware and software is key. A high-quality sensor combined with an advanced algorithm finds the sweet spot between security and convenience.

3.2 MEETING THE DEMANDS OF PAYMENT CARDS

The requirements on a security solution to be embedded in payment cards and launched commercially are plentiful and complex:

1. **Low cost.** The security solution cannot drive cost by requiring more memory, processing power in the sensor host etc.
2. **Ultra-low power consumption.** ISO 7816 Class C cards, the standard card utilized in the payment world has to power all electronics inside a card on the available magnetic field from the PoS, typically four to five mA. The power budget is very limited, any security functionality integrated in the sensor can therefore only draw a tiny fraction of the power budget.
3. **Real-time performance.** The time from the user holding up a contactless card against the reader until a match operation has completed and the user has been verified in less than a second. Any security solution cannot add latency that disrupts this convenient user experience and the less-than-one-second response time expected by consumers.
4. **Ease of production.** Smartcards are manufactured in the billions. The security solution cannot require complex, time consuming production steps to establish the on-card security.
5. **Attacks cannot be scalable.** Each card must be unique. No attack should work on multiple or all cards, nor should it be able to work with zero or minimal work effort for each new card. In effect, attacks must be too costly to scale.

3.3 FINGERPRINTS' SOLUTION

Fingerprints™, the leader in biometrics for contactless smartcards, provides a solution that can be totally integrated into the card itself. This means that all steps in the biometric verification, from sensor image capture to final match, are performed on-card and in real-time. This allows the system to be used with any payment terminal that accepts contactless cards. This also means that all sensitive information is contained in the card and not accumulated in the terminals or in the cloud. For the user, the experience remains just as convenient, only with added security.

Fingerprints FPC SafeTouch® feature is a collection of functions designed to maximize the security. Fingerprints' updated version of this feature is integrated into a selection of its latest sensors to offer a flexible and cost-efficient security solution. It provides two security modes. The MAC mode provides sensor image origin authentication, as well as integrity and replay protection. Additionally, the ISO compliant[4] EtM mode provides sensor image confidentiality.

The security solution uses separate keys for encryption (ENC_KEY) and authentication (MAC_KEY). The ENC_KEY can be either 128 or 256 bits. The MAC_KEY is 128 bits. Sensors with support for the latest FPC SafeTouch work exactly as sensors without earlier SafeTouch functionality, improving the efficiency of testing during card manufacturing and assembly. Only when pre-shared keys have been established, and the desirable security mode has been selected is the security functionality enabled. Once enabled however, the security mode is irreversible and cannot be disabled in any way. The pre-shared keys (PSK) ENC_KEY and MAC_KEY can be established during production, personalization or even during user enrollment, allowing for an ease of production and user experience.

The security solution is based on well-established trusted industry standards[5] and proven technology to ensure that the solution is compatible with existing components in the ecosystem and interoperates seamlessly. Authentication, integrity and replay protection are provided with AES-CMAC[6] in combination with a random challenge from the host when requesting a sensor image. If enabled, AES-CBC[7] provides confidentiality protection of the image data. AES is also used internally as part of the generation of initial vectors (IV) for AES-CBC.

The solution requires the host to use a single crypto primitive, AES[8]. This makes the solution easier to integrate and cost efficient. AES is commonly supported in MCUs (microcontrollers) and SEs, which further cuts the cost and power consumption required to support the solution. The solution can also be performed in streaming mode, further reducing memory requirements and minimizing latency. The Fingerprints' sensor provides image protection without any loss of bitrate performance or lagging.

continued on page 26

Contactless Biometric Payment Cards, continued from page 25

Replay protection is based on a 128bit random challenge (CR) provided by the host when requesting a new image. The challenge is used to initialize the CMAC tag for the image captured and sent to the host. This allows the host to verify that the image received is not a previous image being replayed but sent as a response to the request to the sensor with which it shares the authentication key.

The sensor data size only marginally expands when security has been enabled. With authentication and replay protection, the data expands by 16 bytes. If confidentiality has also been enabled, the data expands with 32 bytes in total. As such, for a sensor image of 10 kilobytes, the expansion is less than 5%.

4. CONCLUSION

Adding biometric authentication on-card is the natural evolution of contactless card payments. It offers an answer to fraud fears and security requirements, without impairing the convenience of paying with a "tap." By adding strong authentication to contactless, the financial world can also finally eradicate the need for PIN entry by removing contactless payment limits, enabling a consistent, simple and hygienic payment experience.

Compared to PINs and traditional contactless, cards with integrated, fingerprint-based biometric authentication offer a superior solution on multiple fronts. However, biometric solutions rely on the quality of the biometric processing itself, and how assets such as the sensor image and templates are protected.

Robust security and privacy protections are fundamental for the launch, and indeed mass adoption, of any new technology relating to sensitive financial data. Fingerprints' sensor and its image protection features meet these demands. With extensive and considered R&D, we have created a solution that delivers multiple attack mitigation functions that can be layered and

implemented throughout the manufacturing and personalization process. Our solution has been carefully developed to meet stringent technical, market and user requirements. Created in line with existing card standard requirements, the technology can enter the market seamlessly, with simple manufacturing processes and no update required to existing payment infrastructure.

The next generation of contactless cards is ready to roll. To learn more about Fingerprints' biometric payment card offering, visit fingerprints.com.

REFERENCES

[1] Fingerprint Cards. Biometrics – The missing piece of the payment card puzzle? 2018.
https://www.fingerprints.com/uploads/2018/05/fpc-smartcards-ebook-en.pdf

[2] The Telegraph. Dirty banknotes may be spreading the Coronavirus, WHO suggests. 2020.
https://www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirusworld-health

[3] Fingerprint Cards. Banking on Biometrics. 2019.
https://www.fingerprints.com/uploads/2019/08/fingerprints-banking-ebook-3.pdf

[4] ISO/IEC 7816-4:2013
https://www.iso.org/standard/54550.html

[5] ISO/IEC. Information technology -- Security techniques -- Authenticated encryption. 19772:2009
https://www.iso.org/standard/46345.html

[6] NIST. Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication. SP 800-38B. 2005.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[7] NIST. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. SP 800-38A. 2001.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[8] NIST. Advanced Encryption Standard (AES). FIPS-197. 2001.
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

About the Author: *Henrik Nilsson is director of product management at Fingerprints Cards AB, the world's leading biometrics company with its roots in Sweden. He is a key member of the team behind the innovative T-Shape® sensor module and software platform, bringing convenient touch authentication for smartcards used in contactless EMV payments, access control and identity applications.*

ICMA's 2021 IN-PERSON EXPO

Cards Reimagined

A smarter future for the card industry.

Join us for ICMA's

30th

Anniversary Celebration

More than Three Decades of Uniting The Card Industry

November 7-10
in the Renaissance Orlando at
SeaWorld in Orlando, Florida.

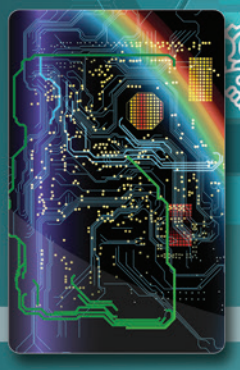
REGISTRATION IS OPEN!

The EXPO showcases the latest research, trends and strategies in the global card industry.

This premier event, **Cards Reimagined**, will feature expert presentations, valuable networking opportunities and an exhibition hall. For more details and to register, visit ICMAEXPO.com

To learn more go to
ICMAEXPO.com

International Card Manufacturers Association
icma



ICMA EXPO 2021 CELEBRATES CARD INDUSTRY

IN-PERSON EVENT SET FOR NOV. 7-10 IN ORLANDO, FLORIDA

ICMA will host its annual Card Manufacturing and Personalization EXPO on November 7-10 at the Renaissance Orlando at SeaWorld in Orlando, Florida.

The premier industry event—***Cards Reimagined***—will celebrate ICMA's more than three decades of uniting the global card industry during the event.

"As the leading global trade association for the card industry, it is critical for ICMA to continue to deliver the cutting-edge education and networking opportunities that our members depend on to advance their careers and businesses forward," said Jeffrey Barnhart, executive director and founder of ICMA. "We will also pay tribute to our association's rich past, honor our members' dedication, recognize more than 30 years of innovation and set the stage for what's to come in our ever-evolving industry at the 2021 EXPO."

ICMA's 2021 EXPO will include an exhibition of leading card industry suppliers showcasing equipment, materials, card components and services as well as diverse networking opportunities, including speed networking with exhibitors, golf, outdoor receptions and dining with card manufacturers, personalizers, issuers and consultants. Winners of the 2021 ICMA Élan Awards of Excellence, which celebrates the pinnacle of design innovation, security and technical achievements in the card industry, will also be announced at the EXPO.

David Burkus, a best-selling author who was named one of the world's top business thought leaders by Thinkers50 in 2017, will present the keynote speech. "Under New Management: Full Transparency, Less Email, No Cubicles and Where the Future of Work is Headed" challenges many of the long-established principles of management and leadership. Drawing on decades of research, Burkus has found that many fundamental management practices are wrong, misguided and downright counterproductive. His revolutionary insights convince companies to leave behind decades-old management practices and to implement new ways to enhance productivity and morale. He has earned invitations to speak to leaders at Microsoft, Google, Stryker and the U.S. Naval Academy and Naval Postgraduate School. His TED talk has been viewed more than 1.7 million times.

Contribute to the 2021 EXPO

ICMA's 2021 EXPO will showcase new and exciting ways to apply science, engineering, tools, methods and knowledge to the development of materials, equipment, products and services that will guide the transaction card industry into the future. Share your expertise and deliver a presentation at the event. Email an abstract to jkohlhepp@ICMA.com for consideration.

Strengthen your business by showcasing your product or service at the EXPO. Submit an exhibitor contract as soon as possible to ensure a premium location on the exhibition floor. Booth spaces are chosen in the order contracts are received and they are filling up fast. Contact Diane Webster-Sweeney at dwebster@ICMA.com to reserve your booth today.

Align your organization with this premier industry event while boosting brand awareness by sponsoring a key element of the EXPO. Sponsorships are available for a wide range of budgets and include, but are not limited to bags, lanyards, program advertising, the event app, educational sessions breaks and meals. Email dwebster@ICMA.com with sponsorship inquiries.

We look forward to having you contribute to our big 2021 event! Remember to stay tuned to ICMAEXPO.com for more EXPO details and early registration discounts.

SPONSORS

The following companies are sponsors of this year's event. We appreciate their support and encourage everyone to recognize their generous contribution to this event. The valuable support of our sponsors contributes greatly to the success of our events.

Monday Networking Reception & Élan Specialty Drink Sponsor

Regi-ception, Showcase Advertisiting & Full Page Program Book Ad

Anniversary Water Bottle Sponsor

Mobile App Sponsor

Badge Lanyard Sponsor

Pen Sponsor

Speed Networking Prize Sponsor

Hotel Keycard and Badge Sponsors

Meeting Room Seat Drop Sponsor

CloudCard Selects Arroweye Solutions as Card Fulfillment Partner

Arroweye Solutions has been selected as the card production and fulfillment provider for CloudCard, a next-gen issuer processing platform.

CloudCard's next-gen card issuance and digital banking platform enables API-driven integration offering instant program launch for fintechs and program managers needing smart payment solutions. Arroweye was selected for its on-demand contactless and EMV card fulfillment capabilities to support CloudCard's delivery of secure and configurable payment solutions.

Arroweye's technology-driven card marketing and fulfillment platform delivers low risk and customized card campaigns within days to launch EMV card programs faster to build customer affinity. Its EMV on-demand provides a no-inventory, highly flexible solution and the agility to launch a new program.

For more information, visit arroweye.com.

Earthwise™ High Content Payment Card Wins Award

CPI Card Group Inc. was named a Gold Stevie® Award winner in the 19th Annual American Business Awards®. The company's Earthwise™ High Content Card received the highest honors awarded in the Product & Service—Business-to-Business Products Category.

The American Business Awards are the United States' premier business awards program. All organizations operating in the United States are eligible to submit nominations.

Introduced in June 2020, the Earthwise™ High Content Card is the first card made with up to 98% upcycled plastic, depending on design, and is EMV® compliant and dual-interface capable. The Earthwise™ High Content Card is made with rPETG and was recognized for the manufacturing innovation and expertise behind it, as well as its overarching purpose: to reduce first-use PVC in payment cards by using plastic waste that might otherwise end up in a landfill. The card is part of Earth Elements™, CPI's portfolio of more eco-focused payment cards, which includes Second Wave®, the first to market, EMV® compliant, dual interface capable, payment card featuring a core made with recovered ocean-bound plastic, and the Earthwise™ Recycled PVC Card, which features up to 85 percent upcycled PVC, dependent on design. Second Wave® payment cards were honored with 2020's Gold Stevie® Award in the same category.

For more information, visit cpicardgroup.com.

Entrust Supports Strong Authentication for Government Employees

Entrust partnered with Yubico, the leading provider of hardware authentication security keys, allowing U.S. federal agencies to issue YubiKey 5 Series and YubiKey 5 FIPS Series with Entrust derived Personal Identity Verification (PIV) credentials to employees instantly, remotely and at scale.

Established on FIPs 201-2, the U.S. federal government's PIV program requires smart card-based authentication for employees to be able to access government computers and networks. However, PIV cards on their own present many operational inefficiencies, including requiring a specific card reader for mobile devices and many desktops and laptops. Additionally, PIV cards are difficult to issue and manage with today's distributed workforce.

Derived PIV credentials (PIV-D) on a YubiKey eliminate the need for a physical smart card to comply with this mandate. Entrust is an acknowledged leader in digital credentials for the U.S. federal market, issuing civilian agency credentials and data protection solutions that help secure the data, encryption keys and secrets of many U.S. agencies. Customers can take advantage of YubiKeys with derived PIV credentials, which are based on NIST 800-157 using the Entrust Managed PKI solution. Additionally, this functionality is included with Entrust Identity Enterprise, which joins Identity as a Service and Identity Essentials as part of the "Works with YubiKey" program.

For more information, visit entrust.com.

Fingerprint Cards Awarded Biometric Card Manufacturing Patent in U.S.

Fingerprint Cards has been granted a biometrics patent by the U.S. Patent and Trademark Office for the design and manufacturing of a capacitive fingerprint sensing module for integration in smart cards.

The patent document for the proposed "fingerprint sensing module and method for manufacturing the fingerprint sensing module" describes the use of a biometric sensing module with electric wire-bonds connecting pads to the external circuitry (to the module) of the device.

This technology can help deliver fingerprint biometrics at lower costs suitable to smart cards, FPC says. This is because it supports the "mill and drill" technique currently used in card production, with a conductive inlay laminated at the center of the card.

For more information, visit fingerprints.com.

Giesecke+Devrient Supplies Sustainable Cards

Giesecke+Devrient (G+D) is one of the suppliers selected by BBVA to manufacture the bank's new sustainable cards as part of its commitment to fight against climate change. With these cards G+D joins this commitment and provides BBVA with the first cards on the market made of 100% recycled PVC layers, thus becoming the first bank in its markets to have this type of card.

BBVA, which has already begun to send the new cards to its customers in Portugal last January is now offering them in Spain and plans to send them to its customers in Mexico as well starting next year.

With this card, G+D not only reinforces its own environmental strategy, which includes a 25% reduction in CO2 emissions by 2022, but it also helps its clients achieve their own sustainability and CO2 reduction goals. In the case of BBVA, G+D is supporting the bank's strategic commitment to only use cards produced with recycled materials by year 2023 and thus involve card users in promoting circular economy. The G+D Convego® Recycled Card body uses 100% recycled PVC layers, compared to many other "recycled" material cards in the market which often are composed of a lower share of recycled material, sometimes even mixed with various plastic types. The unique specifications of the Convego® Recycled card make it easier to be recycled after expiration and a very attractive payment solution for those concerned with the environment and the fight against climate change.

For more information, visit gi-de.com.

HID Global Launches Card Personalization Solution to Streamline Rewards Program

HID Global recently announced that maritime company Attica Group has selected its HID® FARGO® DTC4500e High-Capacity Card Printer & Encoder to optimize its loyalty program kiosks. The solution improves the user experience by instantly personalizing high-quality full-color membership cards and supports the continuous issuance needs of the loyalty program.

Attica Group is engaged in passenger shipping through SUPERFAST FERRIES, BLUE STAR FERRIES, HELLENIC SEAWAYS and AFRICA MOROCCO LINK. Its Seasmiles loyalty program offers an all-year discount ticket policy, a 3-tier card system and an "earn and burn" model which rewards an array of ticket purchases and transactions onboard in exchange for free tickets or meals and drinks when traveling. Previously, passengers had to submit handwritten applications that did not protect any personal data and had to wait more than six weeks to receive their cards. Members can now sign up at once and immediately receive the loyalty card to start enjoying the benefits on-board.

In partnership CubeIQ Limited, Attica Group installed user-friendly Seasmiles

continued on page 32

kiosks on 19 passenger ferries. The kiosks efficiently and securely capture new registrant data, process applications, and HID's FARGO® DTC4500e High-Capacity Plastic Card Printer & Encoders instantly issue membership cards.

In addition to enhancing the onboard experience, the integration of HID's FARGO DTC4500e printer and encoder into the kiosks has helped improve customer loyalty. Within the first 180 days of deployment, loyalty membership registrations increased to more than 15,000 and the kiosks personalized more than 40,000 cards.

For more information, visit hidglobal.com.

Mastercard Partners with Conservation International

Mastercard and Conservation International today announced the introduction of the Wildlife Impact Card program, which enables consumers to help protect wildlife habitats, including those that are home to many critically endangered species.

The Wildlife Impact Card program offers consumers an opportunity to contribute to Conservation International's efforts to conserve the habitats of many critically endangered species globally, including the Sunda Pangolin, African Forest Elephant, Peruvian Yellow-Tailed Woolly Monkey and the Black-and-White Ruffed Lemur.

The Wildlife Impact Card program is available to issuers globally. The first card offerings launch in the United States in partnership with Usio, with virtual prepaid cards available now that can be added to any mobile wallet. Physical cards made from 100% recycled materials will launch this summer.

For each card purchased, $1 will be donated to Conservation International to help protect and restore wildlife habitats, including priority areas equal to 40 million hectares of landscape and 4.5 million square kilometers of seascape globally by 2030. Consumers are also offered the opportunity to further support the cause by contributing to Conservation International through the Mastercard Donate platform.

Additionally, Mastercard has pledged to reach net zero emissions by 2050, building on existing commitments to reduce greenhouse gas emissions aligned with a 1.5-degrees Celsius climate trajectory. Mastercard also issued a $600 million sustainability bond and recently announced changes to its executive compensation model to help accelerate progress around three global ESG goals: carbon neutrality, financial inclusion and gender pay parity. This is all part of its goal of building a more inclusive and sustainable digital economy—where both people and the planet can thrive.

For more information, visit mastercard.com.

SecureID Brings Nigeria to Fore of Global Competitiveness

Vice President, Professor Yemi Osinbajo, has lauded Africa's leading smart card manufacturing and digital solutions company, **SecureID Limited**, for its manufacturing operations in Nigeria while creating copious job opportunities and bringing Nigeria to the fore of global competitiveness with its world-class smart card manufacturing plant in Lagos.

The company recently bagged the esteemed Global System of Mobile Applications (GSMA) making it the first in Nigeria and third in Africa; adding to its other global certifications including Visa International, MasterCard Incorporated, Verve, Card Quality Management (CQM), and ISO 9001/2015 for Smart Card Manufacturing and Personalization of credit and debit cards for all banks in Nigeria and clients in 21 countries across Africa. SecureID also manufactures sim cards for telecom companies, loyalty cards for retail, and security documents for public sector: driving license, national identity cards, international passports, and more.

Osinbajo expressed confidence in the company to bolster local content and contribute to the growth of the economy, stating that the recent GSMA certificate and other global certificates bears glowing testimony to the level of high standards demonstrated in its production of first-rate smart cards in the country.

For more information, visit securid.com.

Visa Partners with Goldman Sachs to Modernize Global Money Movement

Visa recently announced a global strategic partnership with Goldman Sachs Transaction Banking to help businesses—large to small—move money effortlessly around the world.

Through its implementation of Visa B2B Connect and Visa Direct Payouts solutions, Goldman Sachs will help its commercial and corporate banking clients simplify complexities and costs associated with existing systems and inefficient processes. These solutions will enhance Goldman's cross-border business-to-business (B2B) and business-to-consumer (B2C) payments program for high and low value payments. Goldman Sachs's corporate clients can move funds quickly and securely, have near real-time visibility into their payment status, obtain necessary reconciliation and compliance data, ultimately helping improve organizations' cash flow.

For more information, visit visa.com.

BOC Introduces Improved Multi-Currency Travel Card

The Bank of Ceylon (BOC) Multi-Currency Travel Card (MCTC) is now upgraded with benefits that add more security and convenience with near-field communication and 3D secure authentication service for e-commerce transactions.

The bank is offering the BOC MCTC under a special approval obtained through the Central Bank of Sri Lanka. The BOC MCTC is produced jointly with Mastercard International and is accepted around the world to assist travelers to conduct their transactions seamlessly.

This card can be used at ATMs, points of sale and for online transactions where the Mastercard acceptance mark is present. Cardholders can enjoy dining, shopping and travelling while abroad and can use the card at duty-free shopping outlets in Sri Lanka. This card also replaces currency notes, which may be exchanged at a loss when travelling across different countries.

The BOC MCTC provides users with a solution to manage exchange rate fluctuation and keeps travelers informed about transactions via SMS or email.

Canterbury to Get National Public Transport Card

The metrocard, which replaced concession cards in England in 2003, may be replaced with a national public transport card in the near future.

The national smart card for payment for all public transport, dubbed Project NEXT, has been in development at Waka Kotahi NZ Transport Agency in various forms since 2009. Environment Canterbury (ECan) is now proposed to be the first region to launch the card in 2022, followed by Wellington towards the end of 2022 or early 2023. Councils throughout the country would progressively join the program over

continued on page 34

Most Secure and Economic Personalization of ID Cards

Combining laser marking with DoD color inkjet technology

PERSOMASTER

ID Card Personalization System

- High security laser marking with brilliant and fast color DoD printing
- High resolution graphic personalization in black, white and color
- Lowest personalization cost
- Superior durability compared to legacy solutions
- Processes up to 4,200 cards/hr

Atlantic Zeiser GmbH
78576 Emmingen-Liptingen
Germany
www.atlanticzeiser.com

Atlantic ZEISER
a coesia company

several years. A full national roll-out would not be possible until 2026, when Auckland's AT HOP contract expired.

OmniCard Aimed at Youths

Eroute Technologies, a fintech in the payments space, has launched OmniCard— a prepaid card aimed at youths between the ages of 15 and 24 years old—in Mumbai.

This is the first prepaid instrument to be launched after the central bank allowed more features to be built into prepaid cards, bringing them on a par with payment banks. Eroute had received authorization as a prepaid instrument issuer in May. The only other company to have received the prepaid authorization after the guidelines is Bajaj Finance.

OmniCard, which is issued in physical form with tap-and-pay option included, can be used both offline and online. The card is issued on the RuPay network and comes with a mobile application. It can also be used for mobility payments like in Metro trains.

Russia's 'Mir' Available in South Korea

BC Card, the biggest payment processing company in South Korea, has partnered with NSPK to process the Russian national payment system "Mir" among its 3.2 million domestic merchants. As a result of the partnership, Russian visitors can use their own Mir cards in South Korea much more conveniently.

Mir has 158 issuers and 265 acquirers and is accepted in more than 11 countries. According to NSPK, 98.7 million cards had been issued in Russia as of May 1.

In advance, BC Card cooperated with NSPK to establish its cross-border payment infrastructure and discard an extra exchange fee for international payment. BC Card will continuously advance its domestic ATM and point-of-sale terminal network to accept Mir cards.

Translink Promises Ticket System Revolution

Translink has promised a ticket revolution over the next year that will link all of its transport with a contactless card system. The new system means people will be able to use bank card or smart card contactless taps that will cover all Metro and Ulsterbus, glider and rail in an integrated way, with the payment at the end of the journey.

The new Future Ticketing system cost of £42.7 million and will double the amount of ticket machines to more than 4,500.

Digital Payments Preferred at Vending Machines

Cantaloupe Inc. recently announced that a joint study with Michigan State University (MSU) found that the number of digital payment transactions per vending machine exceeded those made with cash in April 2020 (137 digital and 135 cash transactions per machine), with the monthly digital sales volume per machine 47% higher on average than with cash ($235 versus $160).

The study found the growth of digital payments increased steadily through 2020. The average number of cash payments decreased from 52% in November 2019 to 40% in November 2020. Meanwhile, contactless credit card use increased 57% from 14% in November 2019 to 22% that same month in 2020, with a 9% dip in magstripe credit cards during that same period (86% to 78% of total payments). The joint study evaluated sales and transaction data from approximately 122,000 vending machines connected to Cantaloupe's digital payment platform across the United States.

MTA Ends Cash Transactions at Subway Booths

Metropolitan Transportation Authority (MTA) officials recently announced that subway booth workers—who once handled thousands of cash and fare transactions each day—will no longer accept riders' cash or swap their damaged MetroCards.

Hand-to-hand transactions were banned at the booths in March 2020 as transit honchos feared they put workers at risk of catching COVID-19. Now officials say that shift will be made permanent.

The MTA's tap-and-pay fare system will fully replace MetroCards by the end of 2023, which means the authority will no longer need workers in booths to assist riders with cash transactions.

Riders can still use cash to pay for MetroCards at automated vending machines in subway stations. The vending machines will eventually be replaced with OMNY machines that also take cash.

MTA officials also said that riders with damaged MetroCards will have to mail them in or go to the agency's customer service center in lower Manhattan to get replacements.

Jennifer Kohlhepp – Managing Editor, ICMA

ICMA'S LATEST ACE-COMMERCIAL CLASS ANNOUNCED

ICMA would like to congratulate the following individuals who successfully completed the Advanced Card Education (ACE)-Commercial training program:

NAME	ORGANIZATION NAME	TITLE
Kathleen Angel	Perfect Plastic Printing Corp.	Customer Service Representative
Cindy Hill	Valid	Lead Client Service Representative
Kristina Hoch	Valid	Lead Client Service Representative
Nina Mager	Barnes International Limited	Sales Executive
Dominika Mazurova	Barnes International Limited	Commercial Manager
Eva Nye	Valid	Manager of Client Experience
Aaron Seiler	Q-Card Company	Laboratory Support Technician
Jalpa Shah	Valid	Client Services Manager
Morgan Strzok	GOEX Corporation	Inside Sales Representative

ICMA recently expanded its ACE program to include ACE-Commercial virtual training.

The purpose of ACE-Commercial training is to provide sales, marketing, customer service and other card industry professionals at your company with the opportunity to learn the fundamentals of card manufacturing. Others who may find this training beneficial include suppliers and consultants who want to have a deeper understanding of the card industry opportunities and challenges experienced by card providers.

Employees who participate in the training series:

- Receive a high-level overview of the major components of a card manufacturing business.
- Learn about the production of cards.
- Review customer service support and sales issues that arise in the sale and support of card products and projects.
- Review top-of-mind questions and topics that customers of card products may have.

Unlike ICMA's other ACE programs, which require students to pass an exam to achieve a corresponding certification, ACE-Commercial is designed to provide employees in customer-facing roles with high-level card industry education without the need to enroll in certification-level curriculum.

Conducted by David Tushie, ICMA's standards and technical representative, ACE-Commercial is taught virtually in two, 2-hour sessions on the same day. There are no pre-requisites, but the program is only available to current ICMA member companies. Employees who complete the training class will receive a certificate of completion.

The cost to attend the training is $249 per attendee or $210 per attendee for groups of five or more from the same organization. Private company training is also available at a reduced rate for groups of 10 or more.

For more information and to register, visit icma.com/ace-commercial-training/.

NEW BLOGS POSTED ON ICMA.COM

Have you read ICMA's latest blogs?

5 Reasons Why Paper Cards are Making Inroads into the Transaction Card Market delves into the reasons why paper cards are entering the equation, according to Greg Maze, director of product management, packaging, Neenah Inc.

5 Pro Tips for Powerful Card Packaging explains how card packaging is now seen as a meaningful introduction to impactful card products and features Burgopak Ltd. Creative Director Dane Whitehurst's professional tips for powerful card packaging.

Learn about ICMA marketing solutions that can help boost brand and product awareness, generate leads and grow business in ***ICMA Marketing Solutions: 6 Ways to Grow Business in the Card Industry.***

To read all of ICMA's latest blogs, visit the blog section of ICMA.com.

ICMA'S ECOLABEL PROGRAM:

A NEW OPPORTUNITY FOR CARD MANUFACTURERS

Take the next steps to become a licensed ICMA EcoLabel manufacturer. It's a great opportunity to demonstrate your sustainability initiatives.

ICMA's EcoLabel standard program is now available for member card manufacturers to be recognized for their commitment to sustainability and for their cards that meet program requirements.

ICMA's green card standard at a glance

In response to consumer and card issuer demand for green transaction and identification cards, the ICMA EcoLabel Standard Program establishes criteria for the environmental impact of a manufacturer's cards through a third-party ecolabeling program.

Manufacturers can become EcoLabel Program licensees. Licensees can showcase their support of sustainability initiatives.

Licensees can offer issuer clients a valuable EcoLabel opportunity for cards that meet established criteria in one of the following categories:

- **Reduced materials**
- **Recycled content**
- **Compostable**
- **Biobased content**

Sign up for the EcoLabel program today and demonstrate your commitment to green! Questions? **Visit ICMA.com or contact us at info@icma.com.**

2021

September

Money 20/20 Europe
21-23 September, 2021
Amsterdam

October

Money 20/20 USA
October 24-27, 2021
Las Vegas

November

ICMA Card Manufacturing & Personalization EXPO
November 7-10, 2021
Orlando, Florida

TRUSTECH
30 November-2 December, 2021
Paris, France

marketplace

Magellan Consulting, Inc.
Providing Professional Services to Payment and I.D. Card Markets

FULL RANGE OF PROFESSIONAL SERVICES

Magellan provides consulting services to all aspects of the card industry, specializing in large or complex projects:

- Research on product and market opportunities
- Productivity improvement programs in manufacturing and engineering
- Project management and product support
- Due diligence support for acquisitions or product development programs

CONSULTANTS TO THE CARD INDUSTRY

+1 612 747 6553 **info@Magellan-Consulting.com**
www.Magellan-Consulting.com

© 2021 ICMA. All rights reserved. Reproduction without permission is prohibited. Printed in U.S.A.

MIX
Paper from responsible sources
FSC
www.fsc.org
FSC® C012856

index of advertisers

Atlantic Zeiser....34
Buskro....18
D&K Group....11
Graph-Tech USA....5
HID Global....15
Magellan Consulting....38
Melzer Maschinenbau GmbH....19
Mühlbauer High Tech International....2
Rinas Gerätetechnik GmbH....35
SICPA Securink....33
VFP Ink Technologies....Back Cover
VTT GmbH....31

ICMA: The Premier Card Manufacturing & Personalization Organization

Access three decades of card industry data. Network with industry thought leaders and peers. Make an impact around the globe.

200+ companies recognized by prestigious Élan Awards of Excellence

The voice of the card manufacturing industry for over **30** years

Events have been held in over **15** countries

3 industry leading training & recognition programs

Global Card Market Statistics Reports covering **12** markets to support your business planning

200 members representing **43** countries

1,000+ industry articles provided through *Card Manufacturing* magazine, monthly *Inside ICMA* e-newsletter, and weekly *In-brief* e-newsletter

1,100+ exclusive online articles, reports, presentations & resources

Website – visited by **5,000**/month – drives traffic to member websites and offers on-demand member training

2 regional education events in North America and Europe

Nearly **50%** of members with the association for **10+** years

Global EXPO with **300+** attendees and over **50** exhibits

UNLIMITED opportunities for building business partnerships

For more info or to join, visit ICMA.com or call 1 609.799.4900

International Card Manufacturers Association

icma

L'INK

VFP
Ink Technologies

SMART inks for a
SMART connection