NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2017 | #21

The VAULT

HOW TO OPTIMIZE YOUR ID INVESTMENT

- Innovative packaging
- Smart printing
- Flexible software
- High quality, high automation

Reducing Total Cost of Ownership

HID®

BECAUSE PEOPLE ALREADY IDENTIFY WITH THEIR PHONES.

As demand grows for more intelligent and secure mobile identification solutions, HID Global is driving innovation through best-in-class technology and convenience. Our HID goID™ platform for government-issued mobile IDs is the most advanced solution of its kind — allowing control over how much personal information is shared — so a citizen's identity is always protected, whether online or off. And because it's powered by secure Seos® technology, you can invest with confidence.

You'll call it customizable convenience. We call it, "your security connected."

YOUR SECURITY. **CONNECTED** | Visit us at hidglobal.com

Contents

Saving cost with innovative packaging systems 4

By Helmut Strycek, Infineon Technologies

Flexibility and transparency are key 8

By Markus Hoffmeister, cryptovision

New partners for De La Rue 10

By Silicon Trust

"Quality is always the best investment" 12

A quick word with Dirk Melzer

Top 10 considerations on how to boost security while reducing Total Cost of Ownership 14

By Craig Sandness, HID Global

Reducing cost through ePassport and eID synergies 20

By Veronica Atkins, Silicon Trust

Biometrics - marrying security and convenience 24

By Isabelle Moeller, Biometrics Institute

Don’t get left behind by quickly changing PKI standards 28

By Tomas Gustavsson, PrimeKey

Protecting medical big data 30

By Daniela Previtali, Wibu-Systems

Innovation Council 32

Silicon Trust Directory 2018 35

Imprint

THE VAULT

PUBLISHED BI-ANNUALLY BY KROWNE COMMUNICATIONS GMBH, BERLIN.
PUBLISHER: KROWNE COMMUNICATIONS GMBH, SÄCHSISCHE STRASSE 6, 10707 BERLIN
EDITOR-IN-CHIEF: VERONICA ATKINS
ART DIRECTOR: LANA PETERSEN
EDITORIAL CONTRIBUTIONS: HELMUT STRYCEK, DIRK MELZER, DANIELA PREVITALI, MARKUS HOFFMEISTER, CRAIG SANDNESS, ULRICH WALTER, ISABELLE MOELLER, TOMAS GUSTAVSSON
PHOTOS: INFINEON, ISTOCKPHOTO, HID GLOBAL,

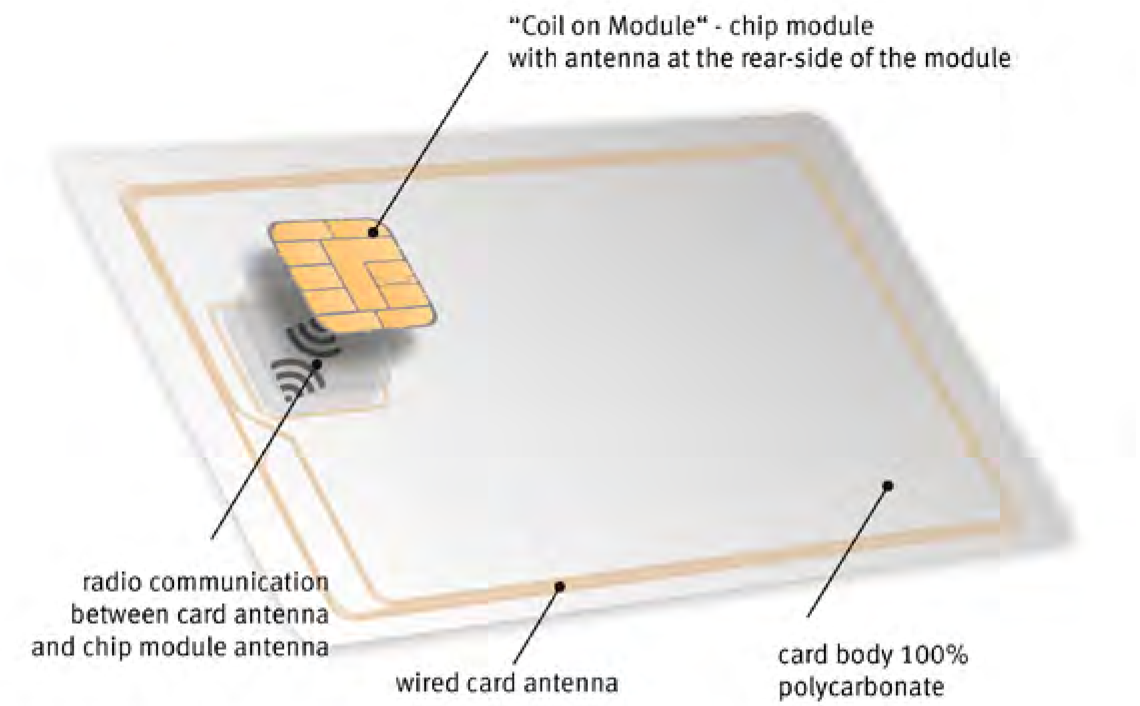
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE

EDITION: AUTUMN 2017

All product copyrights and trademarks are the property of their respective owners. All product names, specifications, prices and other information are correct at the time of going to press but are subject to change without notice. The publisher takes no responsibility for false or misleading information or omissions.

SAVING *COST* with INNOVATIVE PACKAGING *systems*

By Helmut Strycek, Infineon Technologies



Total Cost of Ownership is a key decision making point for governments throughout the world. With different national ID card lifetimes, public sector implementations have to be planned long-term: The investments taken at the start of a project may be higher than, for example, in a singular payment or transportation scheme, but so are the challenges and risks. Modern ID cards are required to stand up to many types of stress, ranging from attempts at physical alteration, to wear and tear, as well as inconsiderate handling in a variety of environments and weather conditions. With a lifecycle of up to ten years, national ID cards have always been designed and manufactured on the basis of the highest standards in the smart card industry. The international card industry, together with various standardization bodies and government agencies, has developed and defined standards and certification levels, which have been adhered to for decades.
Infineon's packaging innovations are designed to increase the durability and robustness of any kind of smart card, while at the same time reducing cost for the manufacturer.

□ *Dual interface technology - bridging between traditional and next generation use cases*

In terms of worldwide implementations, contactless schemes are on the rise. Driven by the payment sector and strongly invested in by industry giants such as Visa and Mastercard, the tap'n'pay convenience of contactless schemes is growing at a remarkable speed. Countries without a smart card legacy often leapfrog directly to full contactless governmental applications.

When it comes to multi-application government schemes, the challenges are of a different nature. Infineon believes that a dual interface model is the best solution to address the upcoming multi-application-on-card scenario. Dual interface cards have the benefit of supporting all existing standards and are therefore able to bridge contact-based infrastructures and modern contactless systems.

Complexity and cost of dual interface card manufacturing

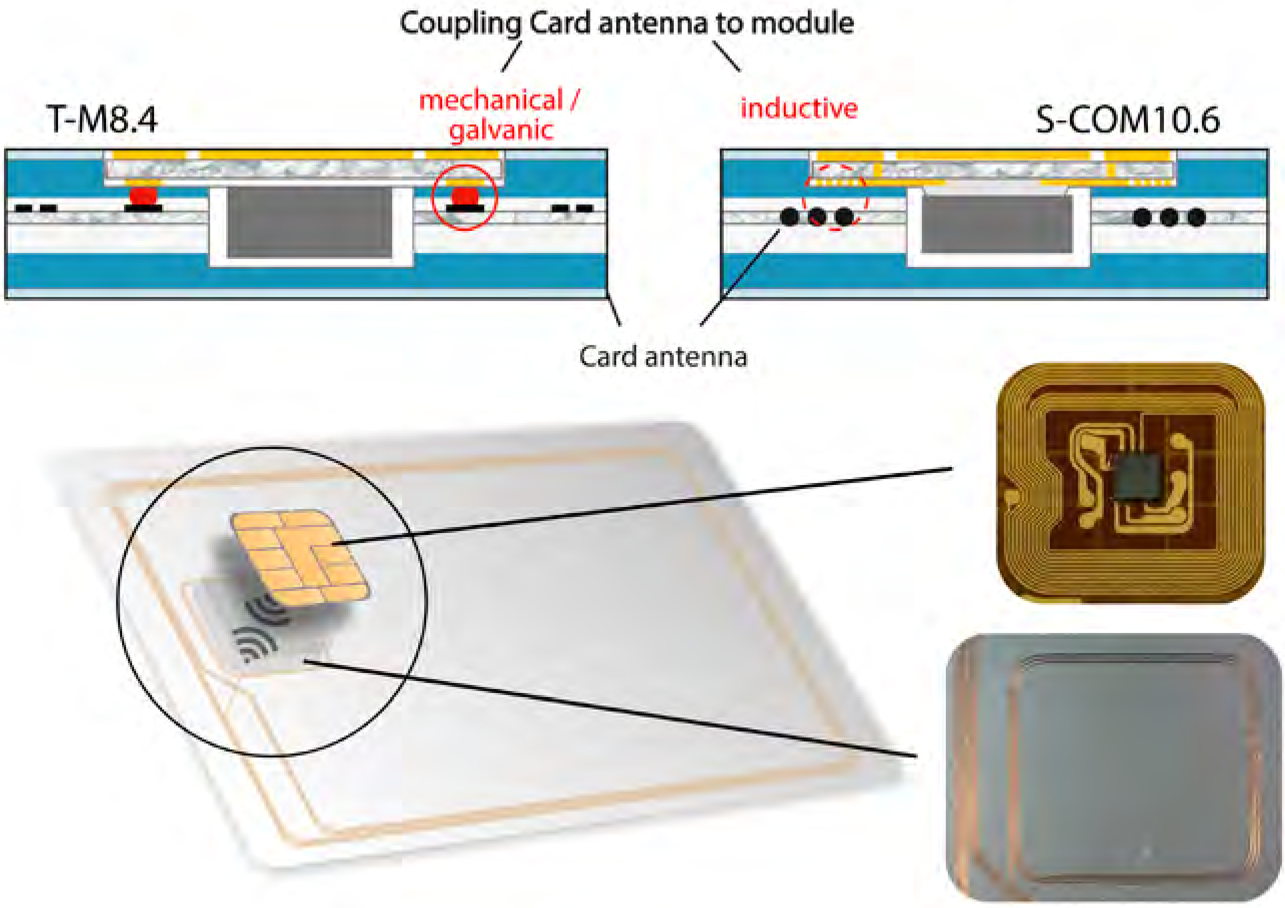
In general, when producing dual interface cards, new processes and production methods increase the complexity of card manufacturing which, in many cases, will lead to increased production costs and potential yield loss. A rough factored equation on cost associated with different card productions published by Eurosmart, showed that the complete cost of a dual interface card can be 50-70% higher than the cost of production of a contact-based card. The key contributors to this high cost are often investments in packaging technology, such as new connection machinery, consumables for the connection, yield loss during the dual interface process and the cost of the additional antenna. While some of this cost is mandatory, Infineon's innovative Coil-on-Module packaging technology helps to keep the overall investment much lower.

A standard card body production consists of the collating of various sheets of polycarbonate (e.g. 50µm and 100µm thick) which are laminated together resulting in a 760µm +/- 80µm (ISO 7810) thick sheet from which the individual cards will be punched out, before an optical inspection finalizes the card body production process.

When producing contact-based cards, the chip module needs to be implanted into the card body. Therefore a milling process forms a cavity in the card body to accommodate the module. The hot melt glue used to attach the module into the cavity is applied to the back surface of the module, before it is placed into the cavity itself. The hot melt glue is then activated using heat and pressure to ensure proper fixing.

When producing a dual interface card, first the additional card antenna needs to be on one of the polycarbonate sheets when they are collated - second a much more challenging aspect of dual interface card production is connecting the card antenna to the module. The connection needs to be done to the back surface of the module during the implanting process. Currently favored connection techniques known to be used for payment cards use a solder process, glue or flexible bumps.

Infineon has developed its Coil on Module system, based on inductive coupling, to reduce the cost of dual interface card production. Unlike other methods for incorporating dual interface, antenna connectivity uses electromagnetic waves for connection between the module and the antenna. Similar to the way a contactless card communicates with a terminal, a small antenna on the chip module connects to a coupling area on a standard size antenna in the card, using an electromagnetic field within the card body. This lack of mechanical galvanic connection with no soldered or welded connection ensures that



there is no chance of breakage between module and antenna – a huge advantage for a card with a ten-year lifecycle.

Infineon's Coil on Module packaging process allows the skipping of the complex connection process at dual interface card production, leading straight to the module being implanted into the card. Without this production process there is no need for further investments in machinery or consumables, nor are there any additional yield losses. For the card manufacturer this means considerable savings, bringing the additional cost of migrating from contact-based to dual interface from 50%-70% down to 30%-50%.

Packaging technology for polycarbonate cards

When looking at making a smart card tamper resistant, it is essential to look at the card body and what it is made of. Polycarbonate, due to its unique properties, has won the trust of governments as the material of choice for durability and tamper resistance. A so-called 'Polycarbonate Monoblock' consists of 'top to toe' polycarbonate, which connects to one block during the lamination without any chance of delamination. After the lamination process, the individual layers can no longer be identified, ensuring improved robustness and an increased tamper resistance.

During the production process, it is crucial to adhere to the element of a secure 100% 'Polycarbonate Monoblock', even when introducing additional items such as security features or antennas: Having a wired antenna on Polycarbonate continues to support the 100% Monoblock concept. It keeps the existing card construction, as only the wire is inserted onto one of the existing polycarbonate layers and ensures no change to the lamination process, as no new material is brought into the card itself.

Infineon offers copper wire antennas that can be integrated into any card material, thereby supporting companies who are pushing a solid Monoblock as an anti-tampering method.

Higher security with lean packaging technology

Increasingly, security designs for national ID cards use the card body and its layers as an enhanced security feature. With transparent layers on both sides of the card, the remaining thickness to hide the module cavity shrinks reasonably.

The module from Infineon is very lean at 420µm (30% less than the competition) and supports increased layers as a security feature, by enabling new card constructions that require shallow cavity milling that ends within the antenna sheet, rather than milling further down into the transparency layer that holds the offset print and hologram patch. Milling down into the final transparent layer would result in the module being visible from the outside of the card. Milling down to a depth of only 440µm will ensure that the module is not visible from the back of the card.

Under the currently used Lean test for card robustness e.g. ISO 10373 specifications, only 8 Newton are required for the 3 wheel test, or just 1,000 bending's and torsions, whereas the industry agrees on at least 4,000. However, up to 8,000 are much more representative for GOV applications.

There are other bodies providing robustness specifications like the Mastercard Card Quality Management (CQM) for contact-based and dual interface cards.

CQM recommends that in order to survive hard-use cases, the cards and modules should survive a pressure of 15 Newton at the 3 Wheel Test. This advanced, recommended specification is difficult to reach with current standard technologies. With Infineon's flip-chip technology used for the Coil-on-module, even the 15 Newton can now be achieved. This in itself goes some way to meeting the 10-year hard usage goals required by government bodies.

Preparing for a pure contactless future: Infineon's INLAM packaging portfolio

There are a variety of sources for standard contactless inlay solutions, like thermo compression welding, conductive paste and bare die flip chip – each having their advantages and disadvantages when taking into consideration the required ten-year lifetime of the card. Infineon's Coil-on-Module technology eliminates the galvanic mechanical connection between module and antenna, thereby eliminating a major weak point.

There are an increasing number of additional security features, such as advanced holograms, UV printed layers, metal stripes, watermarks and more. As all of them require to be placed into the card itself, while keeping the maximum card thickness of 840µm specified by the ISO, there is less available space for the chip module. For standard thermo compression welding, the copper wire is "guided" over a part of the chip module and herewith limits a minimum thickness. For the Inlam CL, the wire is laid around the module, which in combination with a module thickness clearly below 150µm, opens the way for a very thin version of Inlam CL.

While the standard thickness for an inlay is currently 320µm, with inductive coupling technology, Infineon now has a roadmap for contactless inlays to 250µm, giving the end card manufacturer much greater flexibility. This is an attractive argument for passport manufacturers, as they look to reduce the thickness of the data page that carries the chip. Current data pages are standard 800µm, some are at 650µm, with the goal of reducing the thickness to 600µm and below. With standard CL module technology as it stands today, any further reduction will require new solutions such as the Coil-on-Module approach.

Beyond the innovative technology, there are additional benefits with the process flow: Before, manufacturers had to purchase the modules from one supplier and then shipped them to another company for programming and finally ship to the inlay manufacturer. With Infineon holding the responsibility for the entire inlay supply cycle, it can now handle all these aspects of production resulting in a single customer supply point and shorter lead times for the card manufacturer.

Conclusion

The move from traditional ID to eID has meant the integration of one or more card technologies in the production process.

Assuming contactless is the last step in the smart card evolution thanks to its convenience, flexibility in design of the card surface and with no wearing out of contacts, the logical next step for today's contact-based national ID cards would be to migrate to a dual interface format, as a bridge between existing traditional infrastructures and future contactless systems.

With more applications being added to the functionality of an ID card, there is a greater urgency for industry innovation in addressing the physical durability issues that are required to future-proof the credential of tomorrow. Requirements for durability and flexibility in card design will increase, as greater customization of the card takes place alongside increased usage of the cards and documents.

The benefits demonstrated by inductive coupling technology, as well as Infineon's drive towards much leaner chip modules, will go a long way to delivering both an advanced ruggedness of the card and enhanced tamper resistance. With these functionalities in place, the ten-year lifetime requirement of the card becomes a reality. ☒

FLEXIBILITY and *TRANSPARENCY* are KEY

By Markus Hoffmeister, cryptovision

Implementing an ID project is an immense investment for any government or public sector institution. With lifetimes as long as ten years, identification schemes are all about return on investment. Whether it is a national ID project on the African continent or an educational ID project in South America, the total cost can make or break a successful implementation.

□ For governments throughout the world, planning to implement, to re-launch or to optimize ID schemes, Total Cost of Ownership will be one of the biggest considerations and influencing factors. It is unique to the public sector segment, that ID schemes are essentially designed to support physical ID cards with a lifetime of up to ten years. Therefore, it is important to make the overall requirements, service and follow-up costs as transparent as possible at the beginning of the procurement process.

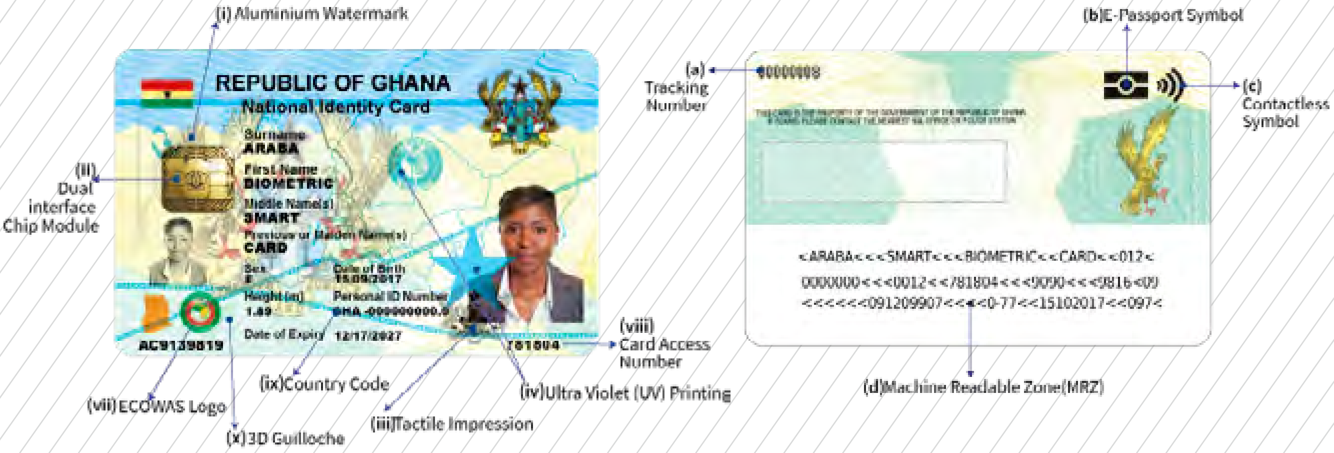
Cryptovision's portfolio covers all security relevant components for a complete solution for state-sponsored ID schemes and corporate ID systems: From the applications on the document, to the tools to create the profiles and personalization, and the middleware to connect to the document and terminal and the Public Key Infrastructure for the administration of keys and certificates. All products follow international, transparent specifications. This means that there is no supplier lock-in for customers and that know-how can be transferred if required. Cryptovision can deliver complete ID systems or components of such systems, depending on customer preferences. With this kind of flexibility, each country can build its own value chain locally, which is hugely beneficial in terms of Total Cost of Ownership.

In terms of components, when looking at cryptovision's flexible and secure smart card and token middleware, it supports all card profiles and operating systems and is designed to connect the smart card or token to virtually any PKI enabled application. It is a sophisticated universal middleware, with support for dozens of smart cards, security tokens of several different form factors and all major desktop operating systems. This allows the client to choose whatever desktop option is most cost effective, allowing the optimization of the overall investment.

The innovative ePasslet Suite is a modern Java Card applet suite, providing a complete set of common applications for electronic identity cards, electronic travel documents, electronic driving licenses, and other similar documents. It supports many international standards and enables international customers to transfer know-how to local suppliers. This, together with the unique feature of cryptovision's ePS that additional document applications can be instantiated after issuance without any impact on the already running apps and their certifications, improves long-term Total Cost of Ownership. ☒

Success Stories

GHANA



As a key vendor to the Ghanaian prime contractor Identity Management Systems (IMS), a subsidiary of Margins Group, cryptovision delivered critical components for the project, including the applications on the eID card, the backend certificate infrastructure, and middleware components used at the card issuance terminals.

The Ghanaian government has ambitious goals to issue a total of 16 million eIDs to its citizens within 12 months. The GhanaCard is a multi-application document. In addition to the primary function of identity verification, it also serves as a passport equivalent for travel within the ECOWAS sub region. Furthermore, it will enable strong two-factor authentication as a password replacement for eGovernment services online and can be used for digital signature of electronic documents. It is also suitable for financial transactions, as the plan is to enable citizens to activate the payment application after card issuance.

To ensure the security of the GhanaCard and its infrastructure, the Ghanaian government rely on technology provided by cryptovision: For the functions on the card and also the Public Key Infrastructure (PKI), as well as the token based access to the PKI. The GhanaCard PKI, which is designed for 16 million certificate holders, ranks among the most advanced certificate management systems worldwide – incorporating several certification authorities (CAs) and multiple certificates on each card.

NIGERIA

With 160 million citizens, Nigeria is Africa's most populous country. As part of an ambitious Presidential initiative, adult Nigerians and resident legal aliens are issued advanced multipurpose electronic identity cards. cryptovision plays a critical role in this mammoth project, as the majority of the applications on this eID card are based on ePasslet Suite. These include an ICAO compliant travel application, a national eID application, and a digital signature application, which include support for biometric Fingerprint Match-on-Card functionality provided by a cryptovision technology partner. The number of applications will grow in the future stages of the project thanks to the unique architecture of ePasslet Suite, which enables infield update and provides additional features.

New PARTNERS for *DE LA RUE*

By Silicon Trust

□ De La Rue and its local partner Pastoriza SRL, have been selected by the Direccion General de Pasaportes following a tender process, to develop a new design for the Dominican Republic's refreshed machine readable passport.

The new passport entails a complete redesign of the current document, placing it firmly at the forefront of passport innovation in Latin America and worldwide. With new cross page designs, which include the latest design-integrated security features, oriented to emphasize the natural beauty of the country, this passport book will help to deliver world-leading counterfeit resistance.

This machine-readable passport, with enhanced security features, is intended to be the precursor for an ePassport solution that the Dominican Republic Government plans to have implemented by the end of next year.

Speaking about the award to De La Rue, Mr. Ramon M. Rodriguez, Director of the DGP (General Affairs for Passports) commented “I am sure we have selected the best partners to design our new passport, which will position us in a more comfortable position to perform the transition to the ePassport”.

Martin Sutherland, De La Rue Chief Executive Officer said: “The award of this design contract is testament to our on-going relationship with Dominican Republic and the expertise of our in-house design team. This is also a great partnership for our growth strategy in the area of identity, and we look forward to working on more projects with Dominican Republic.”

In terms of partnership, De La Rue announced recently that it has entered into a strategic partnership with Opalux, a producer of premium first level security features. The partnership will incorporate joint product development and related sales execution on a global basis.

Commenting on the new partnership, Ulrich Walter, the Managing Product Director of De La Rue's Security Features and Identity Portfolio said: “As a security business, we spend every day staying ahead of the counterfeiter across currency, identity, tax stamps and brand protection. One of our core strategic priorities is to grow our security features portfolio by investing in research and development, as well as partnerships. Opalux has an exciting technology that we believe can play a significant role for our global customers, as part of an integrated portfolio and multiple solutions from De La Rue.”

> *“One of our core strategic priorities is to grow our security features portfolio by investing in research and development, as well as partnerships.*
>
> *— Ulrich Walter, Managing Product Director*
> *Security Features and Identity Portfolio —*

Opalux develops and manufactures tunable photonic crystals; smart materials that change colour in response to external stimuli. Based on this platform technology, Opalux has created a range of highly recognisable and secure features with distinct colour effects for government documents. Speaking about the partnership, Andrew Binkley, the Chief Executive Officer of Opalux said: “We are excited to combine our leading edge technology and security features with De La Rue's integrated portfolio and global reach. We look forward to working together to create a strong set of highly-differentiated solutions.” ☒

THE 4TH ANNUAL MEETING OF THE ID4AFRICA MOVEMENT

Harmonization of Identity Schemes

Be A Part of the World's Fastest Growing Identity Marketplace

Organized by

ID4AFRICA

Hosted by

National Identity Management Commission
Nimc

Platinum Sponsors

zetes
ALWAYS A GOOD ID

PWPW
POLISH SECURITY PRINTING WORKS

Premier Sponsor

IDEMIA
augmented identity

Gold Sponsor

HID

Silver Sponsors

gemalto
security to be free

GEN KEY
Identity for all

www.id4africa.com

Contact Veronica Ribeiro at
v.ribeiro@id4africa.com

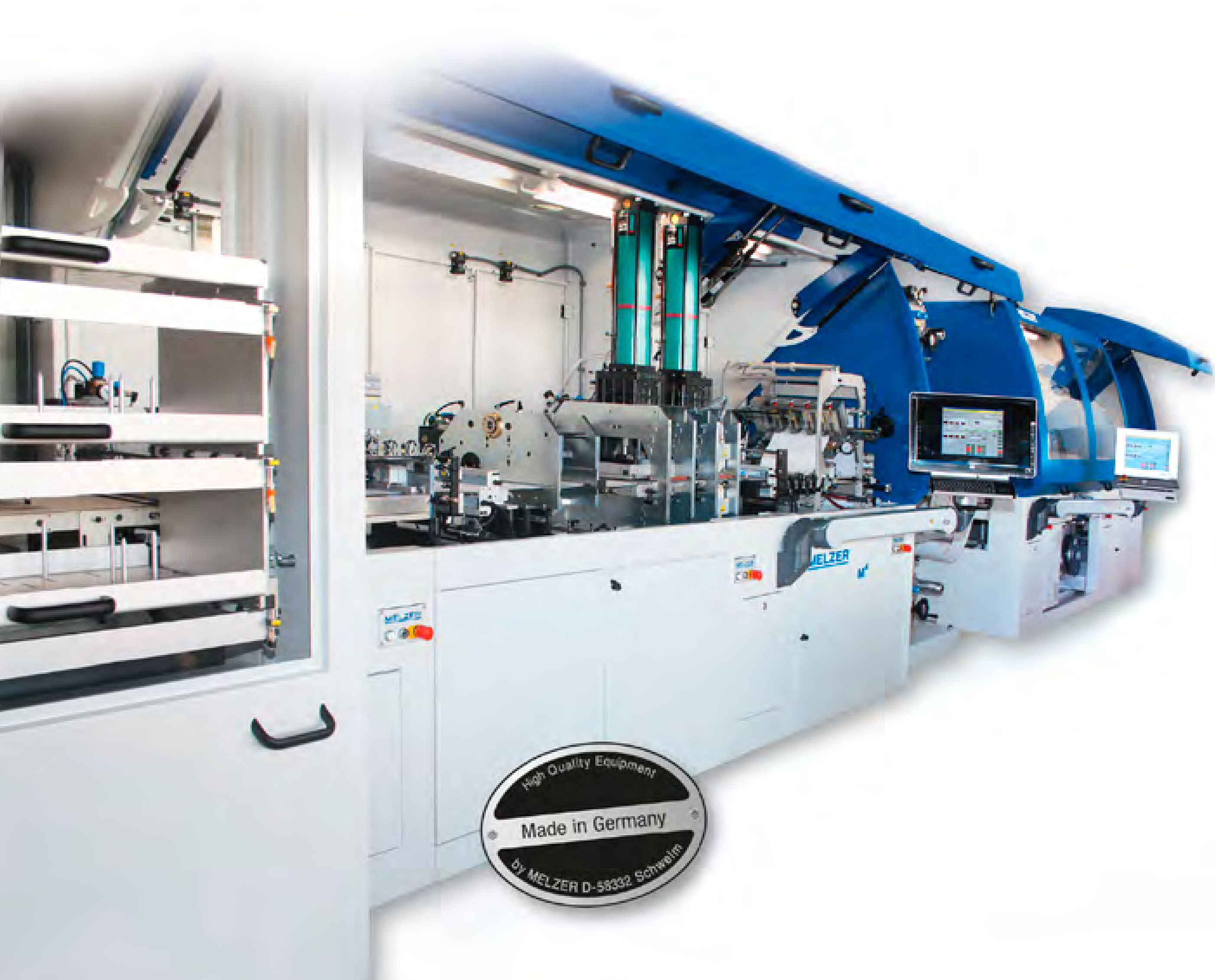
Sponsorship & Exhibiting Opportunities Available!

24-26
April 2018
Abuja International
Convention Center | Nigeria

"QUALITY is *ALWAYS* the BEST *INVESTMENT*"

A quick word with Dirk Melzer

Cost of ownership is an important topic throughout the ID value chain. Production equipment will make up for a substantial part of any new system, so we caught up with Dirk Melzer of the family-run business Melzer maschinenbau, to find out how to best address the topic of ensuring Return on Investment.



□ *When discussing the total cost of an ID project, how does Melzer argue the investment in the production line a customer has to calculate?*

DM: We pride ourselves in having a very close relationship with our clients. Melzer has been successful in this business for 60 years thanks to our customers all over the world. When it comes to Cost of Ownership, Melzer is very fast to react to the requirements of the market. After analyzing the needs of our customers, we can implement them to the highest standards. Most important for the Return on Investment (ROI) is a high yield rate: avoided waste pays back the investment into the machine after a very short period of time. Additionally, a low number of operators, low energy consumption and little space requirement further accelerate the ROI.

How important is the topic of maintenance for Melzer and how can you offer adequate service packages throughout the lifetime of a product, such as an ID card?

DM: Our clients benefit from lowest maintenance costs, thanks to our open design and mostly maintenance free components. Also, most of our clients have their own local maintenance team, which makes a lot of sense and keeps the costs for the system upkeep down. Our goal is that we enable our clients to do their own maintenance well, by offering intense training on site. As a result, almost no service packages are needed. Of course we offer instant support, should the customer need it!

Melzer is known for its quality and its modular design. In your experience, have these characteristics been the core differentiator when going into tender?

DM: In our experience, the main differentiator when it comes to our portfolio, is the degree of automation we can offer. This really helps to keep the costs down. Training, wages and supervising of operators is a major concern in high security document production and its environment. Nevertheless, the operators normally make the mistakes! So, automation is the key and overall, yes, we believe that quality is always the best investment!

How can you help your clients in the long term to keep the Total Cost of Ownership low?

DM: At Melzer we believe strongly in our design capabilities and really, our good track record and market position has reassured us that strong design, in the long run, breeds success. It also keeps cost down, just like our high quality, low maintenance components. It's not so different than with a lot of things we purchase privately: Cheap, most of the time, turns out to be expensive if you have to go back for repairs, parts or external maintenance. The best way we help our clients, is to always work to the highest standards and to share our knowledge with the local teams on site, so that the upkeep can take place there. ☒

TOP 10 *considerations* on while reducing TOTAL

By Craig Sandness, HID Global

With security concerns ever on the rise, today's enterprise corporations, healthcare facilities, educational campuses and government agencies are seeking reliable, scalable and cost-effective solutions for producing secure ID badges on-demand. These credentials come in many forms and can serve one or more purposes – from a simple photo identification (ID) card to badges that allow for physical access or even multi-functional smarts. Because the spectrum of available secure ID card printing solutions is quite broad, understanding your technology options and choosing the right solution can seem like an overwhelming task. The following overview aims to simplify this process, by providing the top ten things to consider as part of an evaluation process, before choosing the right ID card printing solution.

1 *Security*

□ Security should be paramount and its importance can never be overly stressed, for it is precisely the reason that you are seeking a secure ID card printing solution in the first place. Many printing solutions can support a full range of visual and technical security elements that can help ensure that your organization's identities are secure and tamper-proof. But which ones are right for you? How secure do you need your credentials to be and how much should you invest?

To determine the appropriate level of credential security to implement, it is often helpful to assess your risks. What would happen if credentials were compromised by counterfeiters and unauthorized parties gained access to the sensitive areas within your organization?

Beyond the obvious safeguarding of personnel, consider the impact if your organization's confidential data was accessed and compromised. Such sensitive information could include databases, financial systems, customer and/or patient records or classified documents. The most serious breaches can result in theft of proprietary information or financial fraud that can cause an organization to sustain irrecoverable losses that can cost into the millions. Given the potential for such losses, it is absolutely essential that those having access to your organization's buildings, personnel, and systems are known, vetted, and easily identifiable with robust credentials that cannot be easily duplicated.

As such, it is highly recommended that you evaluate solutions that support a variety of security technologies. These can range from standard or custom holographic overlaminates, to those that encompass more complex visual security features, such as morphing images and microtext, to those that support encoding for mag stripe or embedded smart chips.

Selecting an ID card printing solution that can support a broad range of credential security measures ensures that your investment is protected. As your security needs change or increase over time, you need only purchase new consumables or accessories – but your core printer investment remains intact.

Another often over-looked aspect of a secure ID card printing solution, is the security of the card printer itself. The first level of a secure card issuance system should limit operator access to its physical components. Mechanical locks should restrict access to printers, including card input and output. This will prevent cards printed with sensitive personal information and protected credentials encoded on the card being removed from the printer. Furthermore, physical locks should be placed on all access points

how to BOOST *SECURITY* COST of *OWNERSHIP*

to protect ribbon and film consumables, so that these materials are not accessible to would-be counterfeiters.

Electronic security is also critical. Ideally, operator access to each printer is controlled via personal identification numbers (PINs) and print job data packets should meet or exceed advanced encryption standards, such as (AES) 256 bit data encryption, to ensure system privacy, integrity and authentication to the final issuance endpoint.

Selecting only those ID card printing solutions that meet the aforementioned requirements will ensure that you make the best choice to bolster the security, not only of your card program, but also of your overall organization.

2 *Credential Durability*

Ultimately, the efficacy of any secure ID card printing system, comes down to how effectively the issued credentials meet the demands of use, over the desired life of the card. When considering card durability, think about the expected length of your card life and the environments or conditions to which cards will be exposed. Is the end credential an employee badge that will be worn outdoors and exposed to the elements? Or perhaps a magstripe card that may be swiped through card readers multiple times a day for access to secured locations? Knowing how the card will be used and for how long, can help you determine the level of durability you'll want to incorporate into your solution.

One option is simply to leverage high or re-transfer printing. HDP print technology can provide distinct advantages over direct-to-card printing (DTC®) if you are not planning to use overlaminates. The HDP film that is used in the re-transfer printing process inherently protects printed images, creating more durable credentials and providing clear visual evidence if tampering is attempted.

Of course, another option is to laminate your cards. Overlaminates are available in varied levels of thickness and will extend card life. Highly durable overlaminates can extend card life by as much as ten years.

For those organizations that may not require as much durability as is provided by lamination, or in situations where the use of overlaminates is cost-prohibitive, a third and viable option might be to use a high durable, on-card film with an HDP card printer. A high durable film is three times more durable than standard re-transfer films and can extend the life of a card by two to four years – all without requiring additional investments in separate lamination hardware and protective card overlaminates. By forgoing these additional products, organizations can reduce the cost of card personalization equipment by up to 45 percent and the cost of materials by 25 percent or more.

Whichever level of durability you need, it is recommended that you evaluate only those solutions that can offer all of the above as options. This will provide you with more flexible and cost-effective choices.

3 *Card Printing Volume*

How many cards will you be printing and at what intervals? Will you only need new cards printed intermittently throughout the year or will you be printing large batches of cards at a time, several times a year? These questions are important because not all printers are created equal. Some models are equipped to print larger volumes over time but only intermittently, whereas others were built to print significant volumes in single large batch runs. Still others were designed for smaller volume demands or even hand-fed, one-at-a-time print jobs. As such, you'll want to be sure that you select a printer that was actually designed with your needs in mind.

For larger overall volumes or significant batch runs, you'll also want a card printer that supports large yield consumables,

such as color ribbons or laminates. This will maximize productivity, as your operators won't constantly be changing out and replacing materials. When supporting higher volume demands, it is also recommended that you select models that have large capacity input and output hoppers, so that batches can run uninterrupted before card stock must be replenished.

4 Simultaneous functions and card throughput speed

Other critical factors you'll want to consider are whether or not you wish to employ multiple simultaneous applications to your cards, such as encoding and lamination, and at what rate finished cards must be disbursed.

With sophisticated microprocessors at their cores, many contemporary card printing and encoding systems are capable of performing multiple operations simultaneously, yielding card throughput efficiency and speed. Each individual station can work independently, yet simultaneously with other printer/encoder units, to seamlessly print visual personalization, encode data via one or multiple technologies – magnetic stripe, smart card, or proximity – and finally to apply layers of secure, protective lamination.

Multiple print mode settings introduce varied card throughput rates, based upon the organization's card design. Higher card personalization throughput for cards requiring graphics only may be alternated with higher definition, high-resolution image quality requirements and the flexibility to print at more traditional card throughput speeds.

Another feature that can enhance throughput is a dual input hopper. This is a particularly useful feature when you need to print more than one kind of card – with different kinds of credentials – at one time, such as in the case of printing IDs for government employees versus contractors or student IDs versus staff in an educational environment. In these instances, when one card type is being issued, the printer will pull blank cards from the full hopper, while the second hopper is being refilled, enabling continuous operation. If multiple card types are being issued, each printer can automatically select between two card blanks to produce the correct credentials for each card request, eliminating the need for manual hopper changes during multi-card-type production.

Only you can determine what options will best meet your needs, but if you have specific application or throughput requirements, you'll want to evaluate only those solutions that were designed to perform to those expectations.

5 Flexible interoperability

When thinking about your ideal secure ID card printing solution, think about it holistically. What other ways might an ID badge be used in your organization? What other systems / functionality do you need to keep in mind when selecting an ID card printing solution? Whether your organization seeks to migrate simple ID badges into multi-functional technology cards or to increase security by tying into a Physical Access Control System (PACS), it is highly recommended that you carefully consider providers that offer a full spectrum of interoperable secure identity solutions. Providers that only focus on stand-alone badge-printing products limit your ability to incorporate and take full advantage of newly available, complementary technologies.

Additionally, products that were not built with this kind of cross-system compatibility specifically in mind may not always operate as intended. This can potentially open gaps or expose weak points in your security infrastructure. By selecting a solution that at its core, supports interoperability, you ensure that your previous investments will still be relevant, that you can incorporate additional technologies into your infrastructure as needed, and that they will work together harmoniously to enhance your enterprise security and reduce risk.

6 Connectivity

Do you have a need for remote or wireless printing? Do you require solutions that allow you to do mobile, on-the-spot printing and encoding of secure IDs? If so, look for solutions that can support multiple connectivity options spanning USB for single PC connectivity, Ethernet for network printing, and Wi-Fi® for convenient wireless card printing. This will ensure you have the flexibility you need to print from any location and easily alter locations or connectivity methods as requirements change. Because many available products do not support all three connectivity types, be sure to check with your dealer or integrator to ensure your final selection will fit seamlessly into your computing environment.

7 Operational convenience

Today's ID card printing solutions are quite sophisticated and as such, they require routine maintenance to perform optimally, particularly when issuing potentially thousands of ID cards a day. Advanced printers are engineered to minimize operator time and effort required for maintenance, thus maximizing uptime and system throughput. But when repair is necessary, the more quickly a technician can identify the problem and implement a solution, the more quickly that printer gets back online – which in some instances can be mission-critical.

Best-of-breed printers and encoders are equipped with automated diagnostic systems that can alert even non-technical operators to issues that arise, making it easier and quicker to resolve any problems that may occur. Alert mechanisms like lights or graphic displays / touch screens, however, are not limited solely to indicating when repair is necessary. These features also alert your operators when materials are low or cleaning is required, which will help to lower the total cost of operation while reducing downtime.

8 Modularity and system scalability

You will also want to consider only fully modular, field-upgradable solutions that can support new card personalization and security needs as your requirements change over time.

Why is this important? Planning for the future of both the enterprise itself and chosen card printer technology is key for any organization. However, as the size of the business increases, this foresight becomes even more crucial. Solutions should be modular with the ability to add features that allow for technology migration or program expansion. For example, printers with built-in encoders that can assign permissions to your door or your data at the time of card printing combines what previously were multiple processes into a single, in-line card personalization step. Doing so significantly boosts issuance speed, reduces the chance of "human error" in encoding the wrong permissions on to a particular card, and increases the user's convenience and efficiency. Opting for field-upgradeable units enables organizations that already own a card printer, to add an encoder at any time, so they can leverage smart card benefits well into the future.

As with large businesses, the idea of versatility comes into play with the mid-size firms as well. Mid-size companies often require electronic personalization and encoding to support their technology migration needs. Printer and encoder solutions should be capable of accommodating the addition of a magnetic stripe to the card, as well as more robust card technologies, to support an organization's transition from one technology to another.

As your organization grows and your card issuance needs increase or require migration to more advanced card technologies, a field-upgradeable and truly scalable solution can

be expanded in defined increments to meet those demands as they are required, further reducing your total cost of ownership for years to come.

9 Quality

It goes without saying that when you're talking about security solutions, quality is paramount. Solutions worth considering are those that are produced out of ISO 9001-2008 certified facilities. An ISO 9001-2008 registration certifies that the provider's quality system governing the design, manufacture, sales and distribution of their products has been verified by objective third-party audits.

In addition to superior quality standards, it is recommended that you only consider those solutions that include full, multi-year warranties on printers and lifetime warranties on related critical accessories such as print heads. This will help you reduce your costs in both the near- and long-term, too.

10 Partnering with a leader and innovator

As you evaluate various solutions, it is important to consider the provider's longevity and innovation in the industry, as these are good indicators of what you can expect going forward. You should seek manufacturers with a long-time reputation as a trusted source for innovative solutions, technologies, and services, ideally with more than a 20-year history. These providers exemplify stability and customer trust. Ideal providers will also have been leaders in the industry since its infancy and thus, have had a hand in shaping what the industry has become, with technology innovations that other providers only duplicate.

So, how will you recognize such a provider? First and foremost, the provider's product developments will reflect a rich history of customer-inspired innovation, evidenced by its long list of inventions and issued patents. They will also have multiple industry firsts under their belt, such as bringing the industry's first re-transfer, high definition printer to the desktop. Or perhaps they were the first to develop a truly industrial desktop printer for increased security and streamlined, large-scale issuance. Innovations such as these that were developed with the consumer's needs in mind, demonstrate true thought leadership and dedication to the best interests of its customers – both of which are qualities that will prove beneficial to any enterprise that selects solutions from such a provider.

Conclusion

Although the spectrum of available secure ID card printing solutions can seem overwhelming at first glance, by understanding your technology options and taking the aforementioned ten factors into consideration, you will be able to effectively narrow your selections and confidently choose the right ID card printing solution to best meet your unique needs. ☒

mikron

Learn more at: **www.mikron.ru/en/**

Microelectronics production since 1964

- Secure microprocessors for smart cards and ID documents
- RFID chips, tags and inlays: brand protection, retail and library labeling, manufacturing and spare parts labeling, medical ID bracelets, event passes, etc.
- Transport applications: tickets and cards, tags, CAMs

MIKRON is an exclusive supplier of microchips and cards for Russia’s state infrastructure projects: e-passport program, national payment system (MIR), Moscow public transit system.

Headquaters
Mikron JSC
1-y Zapadny Proezd 12/1,
Zelenograd, Moscow,
124460, Russia
Phone: +7 495 229 74 89
E-mail: globalsales@mikron.ru

Representative offices:
USA
Germany
China
Hong Kong
Taiwan

REDUCING cost *through* ePASSPORT and *eID* *SYNERGIES*

By Veronica Atkins, Silicon Trust

□ The fast digitization of society continuously brings new challenges to the public sector, its offerings and its service infrastructure. Electronic identification (eID) allows citizens to access online services, using, for example, a secure token in the form of an ID card. During the last two decades, governments all over the globe have defined, specified and started the roll out of eID card schemes, in order to enable their citizens secured access to online services, as well as highly secured documents for personal verification.

Implementing an eID card scheme is a massive investment for any government, especially if eID cards and electronic passports are implemented as separate projects. Thankfully, standardization as well as technology and processes across the value chain, allow governments to consider implementing a family concept for both ID1 (card) and ID3 (passport booklet) formats.

ICAO Doc 9303 Machine Readable Travel Documents

ICAO's initiative to develop standard specifications for passports and other travel documents followed the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organisation. ICAO's mandate stems from the Convention on International Civil Aviation (the "Chicago Convention"), which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls.

ICAO Member States have recognized that standardization is a necessity and that the benefits of adopting the Doc 9303 standard formats for passports and other travel documents extend beyond the obvious advantages for states that have the machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer strong defense against alteration, forgery or counterfeit. The adoption of a standardized format for the visual zone of an MRTD (Machine Readable Travel Document) helps airline and government officials with the inspection process.

In terms of protection against tampering and fraud, the optional introduction of biometric data stored on a contactless security chip will provide greater protection and facilitate the use of automatic border control (ABC) systems.

The ICAO 9303 standard has been deployed for travel documents incorporating technology standards such as ISO/IEC 19794 for biometrics and ISO/IEC 14443 for the contactless interface, as well as application standards for travel documents, like passports (ID3 format), Residence Permit cards and Registered Traveller cards.

Also, since 2006, the ICAO standard has also been applied increasingly for national eID cards (ID1 format). This has political and legislative implications, some application effects as well as an impact on production and of course, it affects the electronic, contactless interface of the card.

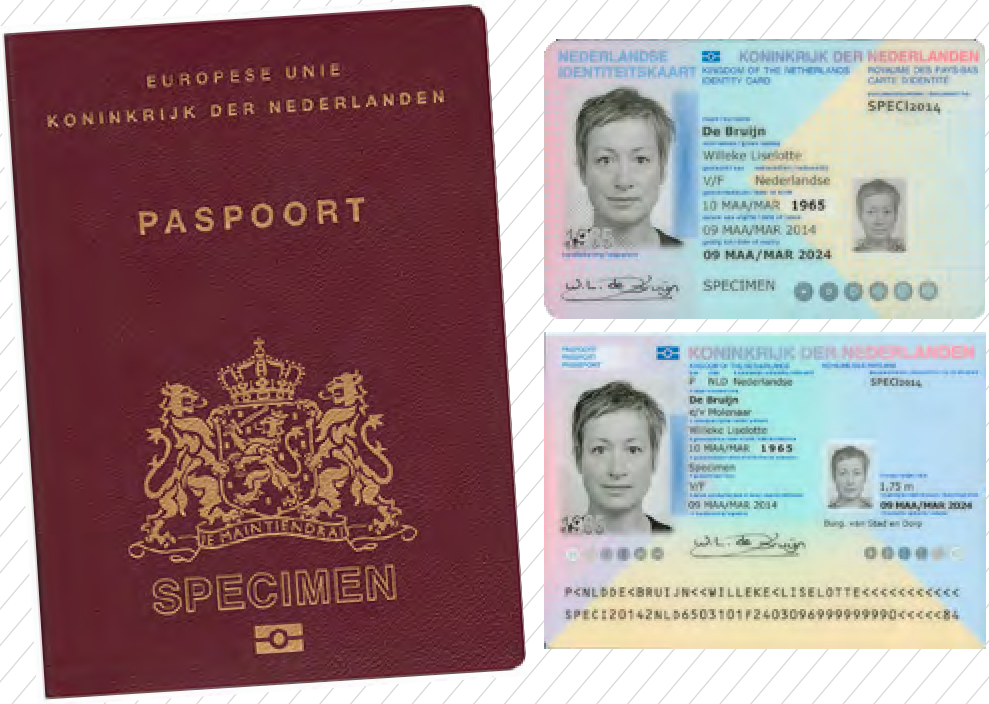
Synergies in production, infrastructure and document security

Synergies between the 2 formats can be found in document production, in equipment procurement, as well as in the process workflow. Both ID1 and ID3 polycarbonate lamination use equipment for both multiple printed panels, the process for lamination applies to both formats with the stacked layers.

When it comes to PC foil printing and finishes, such as hologram and transparent foil, the same equipment and workflow is applicable.

In terms of the key management infrastructure with the

Using the example of the Dutch ePassport datacard and ID card, one can recognize the similar optical design. Integrated within both documents are the same optical security elements (level 1, level 2 and level 3). Both documents carry the same electronic functionality (ICAO 9303 standard) and the same biometric data, stored in the chip (face, since 2006, plus 2 fingerprints since 2009)



purpose of creating and handling keys and certificates, a connected network is required for both formats. In the same way, equipment for capturing the biometric data, such as scanners or cameras, can be used by the registration office also for both document types. Equipment for optical and electronic personalization is available on the market, which can work with ID1 and ID3 documents in mixed mode.

A family concept for both ID cards and passports can be applied when it comes to the optical security concept for a country's documents. All security levels are applicable to both formats, such as rainbow pre-print, UV-mark and special holographic foils.

Synergy in teaching and training of authorized persons

The examples above give a good indication how a cross-format ID family concept can be utilized when it comes to document production and ID infrastructure. However, governments and institutions that opt for a family concept when implementing their national ID document strategy, can utilize synergies beyond the production process.

Take, for example, national ID registration and issuance centers: When rolling out an ePassport project, each center requires a complete solution set – hardware, software, maintenance – even though, on average, only about 30% of the population will ever apply for a passport. If a government decides to use the existing set up also for national ID cards, the efficiency and return on investment is much higher.

Once the documents are issued, also the training and teaching modules of the personnel in charge of border security and immigration, as well as for national eServices, could be offered for both formats: eID card in ID1 & passport holder page in ID3.

Use cases for ICAO data set, biometrics, electronic security and interface

Five different document types use the ICAO 9303 Standard:

1. Passport, ID3, eMRP in more than 120 countries worldwide
2. ID-Card, ID1, National eID-Card in more than 9 countries worldwide
3. Residence Permit, ID1 in more than 50 countries worldwide
4. Frequent Traveller Card, ID1, China & Macao; China & Hong Kong
5. Seafarer Card, ID1, Myanmar Pilot, start in 2017; based on the ILO recommendation.

Conclusion and outlook

The ICAO 9303 standard has been well defined since 2004. To date, more than 100 Mio documents, based on this standard, are issued every year. This standard captures a comprehensive data set (LDS1.7), document reading security (e.g. BAC), stored biometric data & quality (ISO/ IEC 19794) and the used interface (ISO/IEC 14443); The re-use of this standard into other documents besides ID3- booklets, such as ID1 card and Residence Permit card can reduce cost, effort and time for production, for infrastructure, for training and for the forensic lab. For the end customer, the benefits are in the application. For example, when entering and leaving states where an additional visa or entry/ exit stamp is not required, the citizen has a choice. He or she can leave the passport behind and use the eID card with the ICAO-standard for travelling and for ABC systems at the border. This means less hassle and more convenience with a standard wallet-friendly ID1 card format. ☒

Overview on booklets with ID3 format PC holder page – status in 03/2017

Albania, Antilles, Armenia, Azerbaijan, Brunei, Hong Kong, China, Macau, SAR, Colombia, Croatia, Czech Republic, Denmark, Finland, Germany, Hungary, Ireland ,Latvia, Lithuania, Luxembourg, Macedonia, Malaysia, Montenegro, Netherlands, New Zealand, Norway, Panama, Poland, Portugal, Romania, Russia, Serbia, Singapore, Slovakia, Slovenia, Republic South Africa, Sudan, Sweden, Switzerland, Tajikistan, Thailand, Turkmenistan, Ukraine, Venezuela

The following countries start soon:

Brazil, Egypt, Island, Indonesia, Italy, Myanmar, Saudi Arabia, Spain, USA

References on ICAO-MRTD data set in ID1 documents.

The following states use ICAO data sets, biometric, security and interface in ID1 documents in the public domain (alphabetic order):

Albania, 2007

Germany,* 2010

Hungary, 2016

Italy (2nd Gen), 2017

Lithuania, 2009

Monaco, 2008

Netherlands, 2006

Sweden, 2005

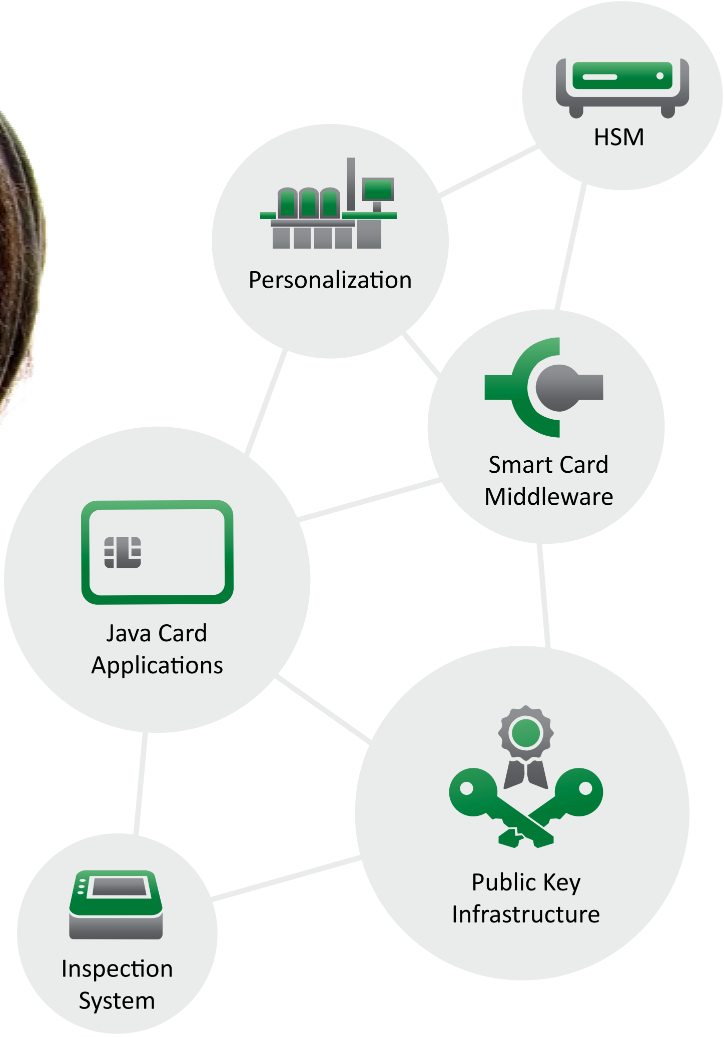
Turkey, 2016

Ukraine, 2016

* Note: Germany needs another authentication protocol than ICAO (TA authentication first, followed by CA authentication).

cryptovision

We create your eID Solution



HSM

Personalization

Smart Card Middleware

Java Card Applications

Public Key Infrastructure

Inspection System

Flexible eID solutions for enterprise and government

www.cryptovision.com

BIOMETRICS - *marrying* SECURITY and *CONVENIENCE*

By Isabelle Moeller, Biometrics Institute

Only biometrics can unify the age-old opposing forces of user-experience and digital security. When it happens, the effect will be remarkable. Thanks, in no small part, to the whims of Hollywood, biometrics have become something of a go-to metaphor for bleeding edge, bullet-proof security. It's easy to see why: iris scanners make great TV.

□ Sadly, reality is always different to the big screen. The last five years have lifted biometrics out of Mission Impossible and dropped them into the lives of everyday consumers, where they are fast assuming a central role in digital identity management. Popular engagement with voice recognition in telephone banking and smartphone fingerprint scans, are, thankfully, sobering perceptions. Security breaches, while unfortunate, have underlined that biometrics are far from infallible and most certainly are not an 'overnight solution' to the world's digital ID problems.

Neither are they toothless, however. On the contrary, in the right hands, biometrics, like chilli peppers, can be powerful ingredients that give real punch to the security mix. What's more, in the world of digital identity, particularly in user authentication, there is an urgent need to spice things up; the industry faces serious challenges.

> *“In the right hands, biometrics, like chilli peppers, can be powerful ingredients that give real punch to the security mix.*

The recent proliferation of digital services and cloud-based platforms, each requiring independent user verification, is making mincemeat of the username and password (UNP) model. Ubiquity compels even the diligent to reuse at least some of their UNP credentials, dramatically increasing the security implications of a hack. Indeed, many of the most popular cloud-based services already automate this practice, enabling users to apply their 'unique' UNP to a variety of other accounts (a process known as single sign-in, or social login). The risk posed by this kind of identity federation is obvious: a hacker needs only to crack one UNP to gain access to all the user's associated accounts. Various services exist to help mitigate UNP vulnerability (password 'vaults' and management applications) but few would disagree that these are at best sticking plaster solutions; the days of UNPs are numbered.

Two-factor or multifactor authentication solutions are far more impenetrable but, compared to UNPs, adoption rates remain comparatively low, largely because the multifactor approach fails to deliver a smooth and convenient user experience. Physical authentication tokens, often used in e-banking, are easily lost or stolen, but more importantly, the authentication process itself is laborious. Typically, receipt or generation of a random key or number sequence occurs on one device (a smartphone), which must be combined in some way with another unique piece of information known only to the user, before being inputted into a second device (laptop, tablet, PC etc.). Replacing all UNPs with this multi-step model is no solution at all; today we login to so many different platforms that interruption and end-user frustration would dominate the digital experience.

Enter biometrics. There is little doubt that the future of digital identity lies in using multiple factors to verify a user's authenticity. The key difference will be that one or more of those factors will be delivered biometrically, enabling the authentication process to be vastly simplified and greatly accelerated. Apple's Touch ID is an excellent example of how a biometric can make an authentication process fast and convenient, as well as secure. Indeed, with biometrics 'in play', a digital world in which the authentication process disappears entirely from the user's experience, could be right around the corner.

When appropriately deployed, behavioural biometrics such as typing styles, app navigation habits, or the pressure applied to touchscreens, leave a data trail almost as distinctive as a fingerprint or face. The identifying power of these behavioural factors can be harnessed by multifactor authentication solutions and, when combined with conventional biometric data, can be used to continually and automatically confirm and reconfirm the

> *“There is little doubt that the future of digital identity lies in using multiple factors to verify a user’s authenticity.*

user’s identity, without interrupting their user experience with off-putting ID challenges.

Adaptive and risk-based authentication solutions are also gathering momentum. These solutions monitor the user’s daily journey through their apps, platforms and devices and use this data to ensure an authentication challenge is only issued when the system deems it absolutely necessary, according to pre-determined policies set by the issuer.

When these fields are mastered, biometric-powered multifactor authentication will finally unify the age-old opposing forces of convenience and security, and a brilliant and incredibly secure end-user experience will be established.

Imagine almost never having to be challenged again when logging into a cloud service, a mobile app, social platform, collaborative workspace, email inbox, remote VPN…

We are not there yet. More work needs to be done to identify and increase the reliability of behavioural biometrics. Capture technologies are still developing and their integration into intelligent solutions must be handled with care, if we are to stay ahead of the hackers. Privacy issues also remain a key concern, as does the storage and sharing of biometric data once it has been captured. This is the space inhabited by the Biometrics Institute Digital Services Working Group, which is one of the few places globally where the boundaries of these solutions are being explored in an open, collaborative and commercially neutral forum. Crucially, it encompasses the full spectrum of stakeholders too, including academics, vendors, end-users and privacy advocates.

The importance of this work cannot be overstated. Collaborative efforts are essential to ensure the true enabling power of biometrics can be realised in the digital space without putting the individual’s biometric data at risk. Cross-industry collaboration at the Institute also accelerates the evolution of these technologies, shortening the lead-time before full deployments are possible and end users benefit. In this instance, this can’t come soon enough. The world of digital services is evolving at a tremendous pace and the threats to personal data security are increasing as a result. Only when biometrics have been successfully integrated will multifactor authentication solutions be able to deliver the user experience demanded by today’s digital consumer. Mass adoption will then follow and all that inhabit the digital world will be safer for it.

While the legal framework and policy creation for biometric data privacy remains a matter for lawmakers, commercially independent guiding principles for the design, deployment and operation of biometric technologies already exist. They are the product of international collaboration between academics, governments, vendors and other key stakeholders at the Biometrics Institute.

Only by sharing live deployment experiences, establishing guiding principles, creating best practice guidelines and promoting the responsible use of biometrics globally, can the industry truly claim to be representing the interests of end-users. Biometrics may be perfect, but our use of them is not. As the adoption of biometric technologies continues to accelerate, it is our collective responsibility to ensure we strike the right balance between delivering a great user-experience and mitigating security risks along the way. ☒

DON’T get *left behind* by QUICKLY CHANGING *PKI STANDARDS*

By Tomas Gustavsson, PrimeKey

As cybersecurity gets more complex and the threat landscape evolves, PKI is there as always, as one of the underpinnings of a robust security infrastructure. As technology evolves faster, so does the PKI, and your teams that are responsible for operations must be on their toes to keep up. Running a PKI is requiring more from your team for a number of reasons.

□ *Technical standards change fast*

Technical standards evolve fast with new protocols and algorithms taken in use, and old ones being phased out as insecure and insufficient. New products in your environment use new protocols to communicate and new algorithms for protecting their communication. On the PKI side, we see new protocols such as EST and extended use of REST APIs, as well as changes in how older protocols are used such as OCSP with the introduction of OCSP stapling. New algorithms such as ECDSA and RSA-PSS are quickly coming to the mainstream. Neither your old PKI, nor your old systems, were equipped to handle this 5-10 years ago and a transition and continuous evolution is needed to keep systems secure.

Audit requirements become stricter

If you are in a larger enterprise or in a regulated industry, chances are high that you will be affected, one way or the other, by audit standards like WebTrust, eIDAS or industry specific requirements such as CAB Forum. In addition to these, there are other domain specific requirements, such as Certificate Transparency for web server certificates, Cloud-, IoT and Grid security standards. More regulations are coming.

> *“If you don’t keep yourself updated, your users cannot one day connect to your internal systems.”*

In response to increased threat awareness, audit standards are also rapidly evolving and keeping up, meaning that it is nothing you can implement once and after that can rest. You must keep abreast with new changes in the requirements every year.
Examples where strict guidelines have changed recently, and you need to adapt, are for TLS, code signing and digital signature certificates.

Software changes faster

You may think that you are not affected because you only run an internal PKI in your organization, and that these standards only affect regulated CAs. But that can be a dangerous assumption. Much of the software in the ecosystem, such as web browsers and email clients that your users rely on everyday, also change rapidly in response to new threats and updated requirements. Therefore, you may find that if you don’t keep yourself updated, your users cannot one day connect to your internal systems, or are faced with security warnings, after a simple web browser update.

Be educated and keep security and DevOps together

Keeping up to date is hard for seasoned security experts, so how can the normal enterprise be on top of it? The simplest recommendation is that if you are affected by any of these standards, you should set time aside for a person responsible for compliance, to monitor the landscape and plan changes in good time. Changes are usually announced well in time, before going into effect and with good planning, these changes can be rolled into your normal DevOps routines.

> *“Security today is an integral part of an agile enterprise and security and operations teams must work closely together, align goals and plan activities together.”*

Security today is an integral part of an agile enterprise and security and operations teams must work closely together, align goals and plan activities together.

Upgrade your PKI systems

PrimeKey spend a lot of time implementing new standards and features as they emerge, both in EJBCA for the pure PKI and in SignServer for time stamping and digital signature standards. Our aim is that new versions of our solutions containing the features you need to be compliant, are out there in good time. We love working with you to understand your discussions about new requirements. ☒

Protecting *MEDICAL* BIG DATA

By Daniela Previtali, Wibu-Systems

On 11 September 2016, a gang of three men drove up to a hospital in the quiet seaside town of Sande on Germany's North Sea coast. CCTV recordings show the men walk into the hospital and come out again, unperturbed, with almost a million Euro's worth of medical equipment stashed away in their bags. Brazen as this heist may seem, these days, the real danger to hospitals and medical device makers lies not in material theft, but in the risks to more immaterial goods: confidential patient data, the software operating critical medical equipment, or the intellectual property invested by medical technology specialists. Security-by-design becomes a prerequisite when lives are at stake.

□ As the recent disastrous WannaCry ransomware attack revealed, healthcare providers are a prime target for the new breed of criminals trying to skim off an illicit share of the vast medical technology and health business. With the world's population still growing at an unprecedented rate and aging at the same time, the number of people needing and deserving high-quality medical care is rising everywhere. Deloitte estimates the healthcare market to reach a full $418 billion in global revenue, as more and more emerging economies are upgrading their medical and care systems. At the same time, new technological advances are dramatically changing the nature of healthcare.

Gone are the days of the one-size-fits-all treatment, as the rise of big data paves the way for more personalized and digitalized medicine. The patient is no longer just a number in a hospital file or a faceless individual occupying a bed on a ward. Modern medicine works with detailed patient profiles to deliver customized care and perfectly targeted drugs and medical devices to cater to each patient's specific needs. All of these advances need to be achieved with therapies and devices that are simple to use, by older and infirm patients in the case of self-medication, or by the broader medical workforce beyond skilled specialists.

What medical professionals and the new entrepreneurs and established brands in the medical technology field now need - in order to seize this unique opportunity - is the ability to deliver such individualized therapy in a way that does not compromise the patient's physical safety or sense of trust; that rewards the complete value chain from the inventor to the maker to the distribution channel; and that is affordable and economical for doctors, hospitals, and other medical professionals. Care needs to be deliverable in smaller medical centers around the world and in emerging economies with still-developing social insurance systems, giving every potential patient basic access to the advances of modern medicine. A pricing point for the medical devices that lowers the investment threshold and ensures a reliable income for the efforts of the companies involved, while securing these same devices and the vital data in them, is the challenge of the new millenium.

> *"Fritz Stephan, the highly respected maker of medical respirators, has acknowledged these risks, while also fully embracing the commercial potential of intelligent, connected medical devices."*

Fritz Stephan, the highly respected maker of medical respirators, has acknowledged these risks, while also fully embracing the commercial potential of intelligent, connected medical devices. The company recently unveiled its new EVE (Easy Ventilator Emergency) product line with many groundbreaking features, from the simplicity of its user interfaces to the revolutionary feature upgrading capabilities, all protected with Wibu-System's unbeaten CodeMeter technology. Lightweight, mobile, and designed for use anywhere from the scene of accidents to neonatal wards, the EVE units are easily set up for newborn, child, or adult patients and immediately ready for action. With three models available to cater for emergency response (EVE_{TR}), intensive care (EVE_{IN}), or infants in critical need of post-natal care (EVE_{NEO}), the functionality of the system is software-realized and can easily be upgraded at the point of need.

Under the hood, Fritz Stephan relies on Wibu-Systems' CodeMeter Embedded to protect its intellectual property and provide the licensing capabilities for feature upgrades in the field. The solution is integrated via a special SD card (CmCard/SD) that comes with Infineon's state-of-the-art SLM97 security controller and industry-grade Single Layer Cell (SLC) flash memory, accessed through CodeMeter's API. As the entire EVE product line is certified to global (RTCA DO160F) and Germany's exacting standards for medical devices (DIN EN 794-3 and DIN EN 80601-2), the technology of Wibu-Systems and Infineon integrated in them, by implication, meets the same standards. The CmCards are built directly into the ventilators and thus protected from tampering, short of would-be attackers breaking the cases apart. Together, Wibu-System's CmCards and CodeMeter software and Infineon's SLM97 security controller form a robust gatekeeper and rugged container to store the digital signatures, certificates, and entitlement rights that define the feature set of the respirator.

> *"Fritz Stephan, Infineon, and Wibu-Systems celebrated this successful collaboration when the three partners showed up in force at Germany's premier digital industry summit, the Digital Gipfel."*

Whenever the user needs an extended set of functions – imagine a smaller hospital needing to upgrade its intensive-care EVE$_{IN}$ for use with a premature baby whose life is in danger – there is no need to purchase a second ventilator or even return the EVE$_{IN}$ to Fritz Stephan for a feature boost. The user simply buys a new license from Fritz Stephan online via the company's implementation of Wibu-Systems' CodeMeter License Central. One download and upgrade later, and the EVE$_{IN}$ has the added features of the EVE$_{NEO}$. The solution is a win-win outcome for all parties: Wibu-Systems and Infineon demonstrate the robustness and versatility of their technology, the user saves money by keeping the upfront costs for a limited feature set low, and Fritz Stephan has a reliable new aftersales revenue source without compromising the security of the medical devices or the protection of their intellectual property.

Fritz Stephan, Infineon, and Wibu-Systems celebrated this successful collaboration when the three partners showed up in force at Germany's premier digital industry summit, the Digital Gipfel. Designed to raise awareness around the challenges and promises of the new digital frontier, the Digital Gipfel is promoted by Germany's Federal Ministry for Economic Affairs and Energy and represents the culmination of many initiatives by the leading actors in the field. This year's event gave particular prominence to several facets of cybersecurity – a topic critically important to the three enterprising companies behind the new technology at the heart of the EVE ventilators. With robust security, uncompromising ease of use, and flexible licensing to allow users to mix and match their device's features to their needs, the EVE ventilators realize the best promises of the digital age. Hospitals might still be appealing targets for thieves, and hackers might still be trading in stolen data or trying to blackmail healthcare providers, but their illegal attempts continue to spur the development of new technological countermeasures and innovation of new business models. ☒

WELCOME *the* Silicon Trust *INNOVATION Council*

The Silicon Trust is delighted to introduce its Innovation Council. These distinguished experts will help define the core areas of product innovation and application trends in the Government ID sector for the Silicon Trust.

Professor Keith Mayes B.Sc. Ph.D. CEng FIET A.Inst.ISP

Professor Keith Mayes B.Sc. Ph.D. CEng FIET A.Inst.ISP, is the Director of the Information Security Group (ISG), and the Head of the School of Mathematics and Information Security at Royal Holloway University of London; which has been pioneering information/cyber security research and education since 1990. Keith joined the ISG in 2002, originally as the Founder Director of the ISG Smart Card Centre, following a career in industry working for Pye TVT, Honeywell Aerospace and Defence, Racal Research and Vodafone. Keith is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology, a Founder Associate Member of the Institute of Information Security Professionals, a Member of the Licensing Executives Society and an experienced company director and consultant.

Isabelle Möller

Isabelle Möller is a biometric expert instrumental in the growing network of The Biometrics Institute. She has played a key role in the establishment of independent and impartial international Biometrics Institute in particular through bringing together biometric experts from around the world. Isabelle has also managed many government funded projects successfully including the Biometrics Vulnerability Assessment Project, which was co-funded by the Australian Department of Prime Minister & Cabinet and the Biometrics Institute Privacy Code.

Isabelle holds a Master of Arts in English Literature, Business and the Arts from the Johann-Wolfgang-Goethe University in Frankfurt Main, Germany.

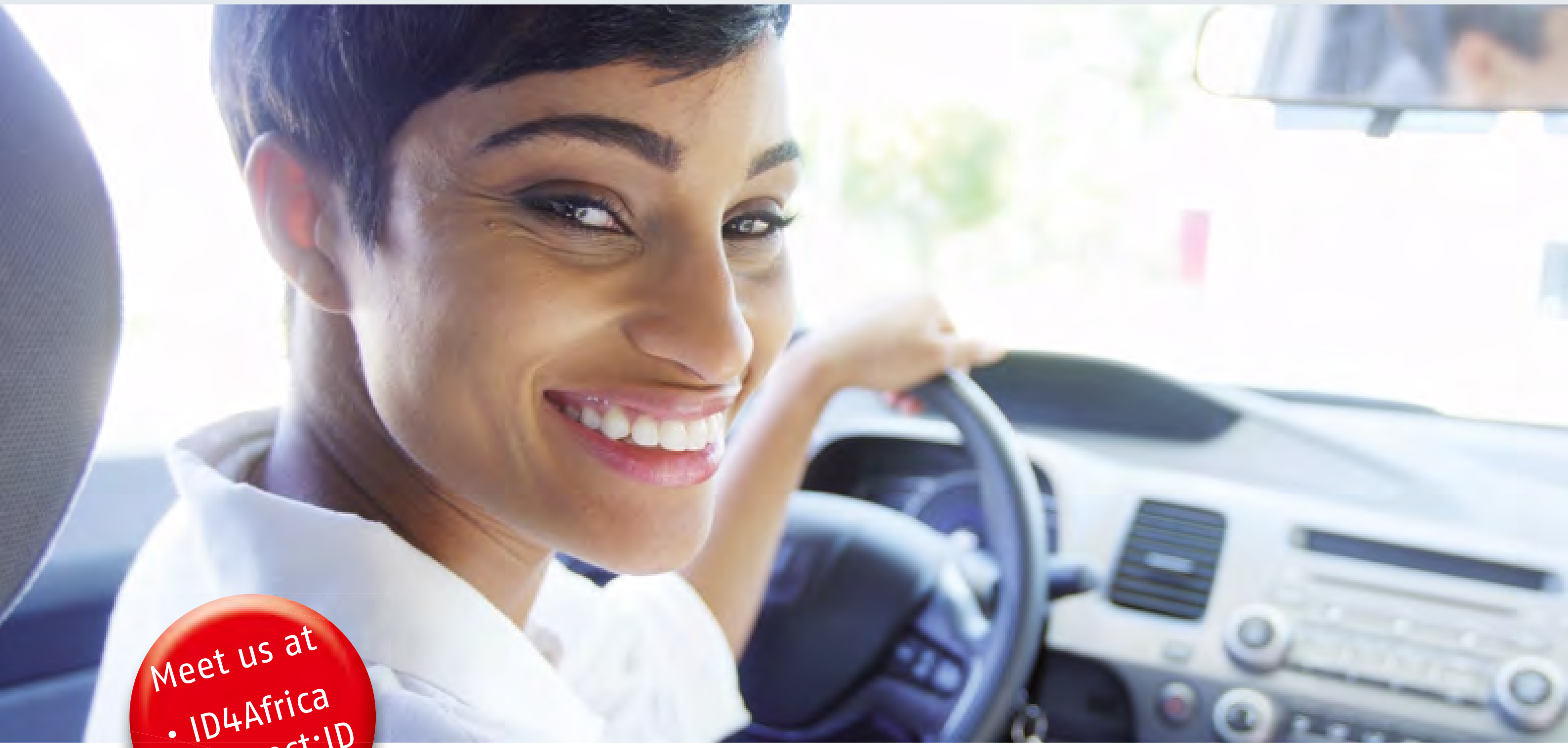
Dr. Joseph Atick

Dr. Joseph Atick is a recognized worldwide expert and advocate on identity matters, having been one of the founders of the identity industry more than 25 years ago, where he had led several companies in the space and developed some of the foundational algorithms underlying secure digital identity today. He retired from the industry in 2010 and founded the Identity Counsel International, to focus on helping nations, especially in developing countries, and international organizations seeking to design and launch responsible digital identity programs to accelerate socio-economic development, improve service delivery and security and enhance privacy and people's rights. He has been a strong advocate of privacy and responsible use of identity technology for social protection. In 1998, he co-founded in Washington the International Biometrics and Identification Association, to provide responsible use guidance to the industry and to policy makers. He is currently the Executive Chairman of ID4Africa, a pan African movement to promote the responsible use of digital identity in Africa.

Dr. Atick earned a Ph.D. in Mathematical Physics from Stanford University.

MASKTECH

We make chips intelligent



Meet us at
• ID4Africa
• Connect:ID
• SDW

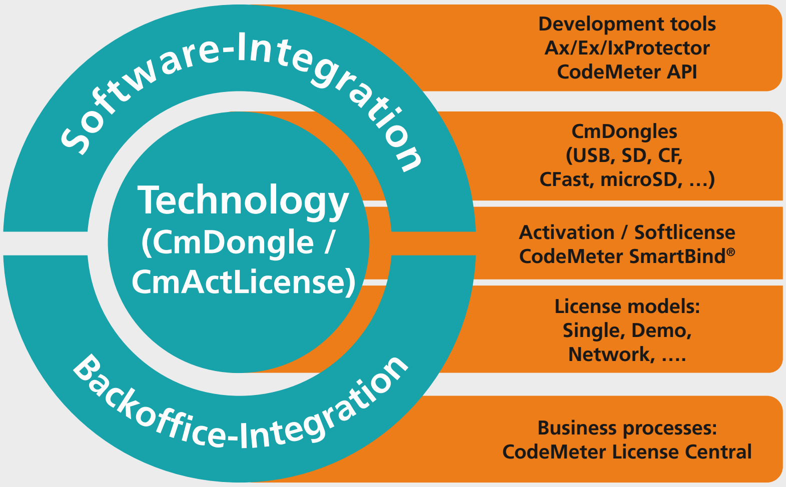
MTCOS® – ID CHIP SOLUTIONS FOR eGOVERNMENT APPLICATIONS

- High Security Operating System (MTCOS®), e.g. ePassports, eIDs, eHealth cards
- Independent worldwide supplier
- More than 65 eID-document references
- Up to EAL5+ Common Criteria certified on a unique variety of chip platforms

SecurITy made in Germany

Common Criteria

MaskTech GmbH • Nordostpark 45 • 90411 Nuernberg • Germany • sales@masktech.de • www.masktech.de • +49(0) 911 95 51 49 0



SILICON TRUST DIRECTORY 2018

THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

The Silicon Trust is a well-established marketing program for smart card solutions with high visibility in the worldwide government and identification (ID) markets. With over 30 companies along the value chain, the Silicon Trust forms a strong community of like-minded companies.

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

- Educating government decision makers about technical possibilities of ID systems and solutions
- Development and implementation of marketing material and educational events
- Bringing together leading players from the public and private sectors with industry and government decision makers
- Identifying the latest ID projects, programs and technical trends

EXECUTIVE COUNCIL

The Executive Council has been the steering committee of the Silicon Trust since 2008. It drives the Silicon Trust by defining the topics and directions of the program's publications, workshops and meetings.

INFINEON TECHNOLOGIES

Infineon Technologies AG is a world leader in semiconductors. Infineon offers products and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2016 fiscal year (ending September 30), the company reported sales of Euro 6,5 billion with about 36,000 employees worldwide. Infineon is the world's leading vendor of secure chip card ICs used for passports, ID cards, payment cards, mobile subscriber authentication (SIM cards), access cards and trusted-computing solutions as well as being a technology driver in the hardware-based security field.
www.infineon.com

ADVISORY BOARD

The Silicon Trust Advisory Board supports the Executive Council in defining the direction of the program in terms of public policy and scientific relevance.

BSI

Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security. It has been established in 1991 as a high level federal public agency within the area of responsibility of the Ministry of the Interior. The BSI's ultimate ambition is the protection of information and communication.
Especially in the area of smart card technology, BSI is responsible for the design and definition of secure solution requirements for governmental identification documents. The German ePassport has been introduced in 2005, the second ePassport generation followed 2007, and starting in 2010 the all-new German eID card has opened a new trustworthy approach to Internet authentication for all German citizens. Security of all these documents is based on BSI specifications, developed in close collaboration with European/international standardization bodies and leading industry partners.
www.bsi.bund.de

FRAUNHOFER AISEC

Fraunhofer AISEC supports firms from all industries and service sectors in securing their systems, infrastructures, products and offerings. The institution develops qualitatively high-value security technologies, which increase the reliability, trustworthiness and tamper-resistance of IT-based systems and products. The approximately 80 members of the Fraunhofer AISEC scientific and technical staff balance economic needs, user-friendliness, and security requirements to develop optimally tailored concepts and solutions.
The security test labs are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyze the security of products and hardware components as well as software products and applications. In our laboratories, functionality, interoperability and compliance are tested to give clients targeted,

effective advice. Strategic partnerships with global corporations as well as with internationally recognized universities guarantee scientific excellence as well as its market-driven implementation.
www.aisec.fraunhofer.de

SILICON TRUST PARTNERS

Partners of the Silicon Trust are a vital element of the program. The partners represent all aspects of the value chain and are international representatives of the ID industry. They all share one common goal – to create awareness, to educate and to promote the need for silicon-based security technologies.

ABNote

ABnote™ is a leading global supplier of secure documents, services and solutions. If you have a credit card or an identity card, or have received a gift or loyalty card, or any other plastic card, chances are that you have used an ABnote product. If you have interacted with a financial institution, or have used your smart phone to make a payment, you have likely taken advantage of an ABnote service.
We are proud of our legacy – over 200 years of manufacturing high quality, tamper-resistant products to governments, financial institutions, retailers and other organizations throughout the world. Today, our products and technology encompass multiple markets, keeping pace with today's rapidly changing requirements for convenient and secure transactions.
www.abnote.com

AdvanIDe

Advanced ID Electronics – is one of the leading silicon distributors, focused on components for RFID transponders, chip cards and RFID readers and terminals. Thanks to its optimized semiconductor supply chain, AdvanIDe can guarantee manufacturers of smart cards, RFID transponders and readers the most efficient access to the latest semiconductors.
www.advanide.com

AGFA

Agfa is commercially active worldwide through wholly owned sales organizations in more than 40 countries. In 2014 the Group achieved a turnover of € 2,6 billion. Agfa develops, produces and sells special films for the card industry. PETix™ is a range of high-performance polyester films, for cards with a lifetime above 10 years and a high chemical, scratch and thermal resistance.
www.agfa.com

ATOS

Atos SE is an international information technology services company with 2014 annual revenue of € 9 billion and 86,000 employees in 66 countries. Serving a global client base, it delivers IT services through Consulting & Systems Integration, Managed Operations, and transactional services through Worldline, the European leader and a global player in the payments services industry. It works with clients across different business sectors: Manufacturing, Retail & Transportation; Public & Health; Financial Services; Telcos, Media & Utilities.
www.atos.net

AUSTRIACARD

Austria Card AG is a holding company of businesses providing end-to-end solutions and products in the field of Digital Security and Information Management. The Group brings together the century-long heritage in printing services and state-of-the-art digital data solutions (Information Management division) with the well-established production and personalization of smart cards and the offer of cutting-edge digital payment solutions (Digital Security division). The combination of well-established industrial roots with an expanding services portfolio that meets the needs of the increasingly digital and mobile economy is at the very core of the Group's confidence in its future.
www.austriacardag.com

BALTECH

BALTECH is specialized in ISO14443/15693/NFC Reader technology. The core competencies are RF-Interface technology and sophisticated high level functionalities supporting the latest card technologies and security mechanisms. All products are 100% developed and manufactured in-house. This is the basis for customization capabilities offered to deliver application tailored, cost optimized products from readers up to terminals with individual functionalities for various applications.
www.baltech.de

CARDPLUS

CardPlus is a consulting firm with a focus on customized, enterprise level, Identity and Security Management Solutions. We offer a full range of Professional services to build, transform, implement and manage our customized enterprise level security and identity solutions. Due to our vast hands-on experience in designing and implementing secure travel and identification systems for governments and large public sector customers, we are uniquely positioned to understand your highly complex security requirements and translate the same into practical, workable solutions.
www.cardplus.de

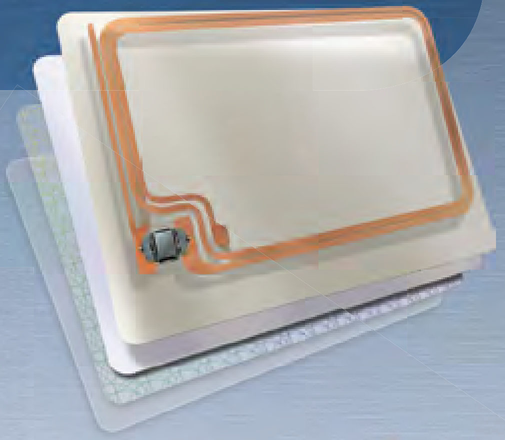
De La Rue is a leading provider of sophisticated products, services and solutions that help keep the world’s nations, economies and populations secure.

At De La Rue, we provide governments and commercial organisations with the products and services that enable countries to trade, companies to sell, economies to grow and people to move securely around an ever-more connected world. With a 200 year heritage, we work to the highest ethical standards and stand firm in the fight against counterfeit and fraud.

DeLaRue

www.delarue.com

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®

Please visit us at: TRUSTECH · Cannes, France | **HSP Europe** · Warsaw, Poland | **INTERGRAF** · Dublin, Ireland | **RFID Journal LIVE!** · Orlando, Florida, USA **more** ▷

www.melzergmbh.com

CHARISMATHICS

charismathics® has been pioneering the global identity management arena since 2005 and is offering security products and services for a variety of industries ranging from corporate to finance, from e-government to health services, from e-education to telecommunications. The company delivers PKI security solutions addressing traditional smart cards, convenient USB keys, handy soft tokens or even cutting edge mobile applications.
www.charismathics.com

COGNITEC

Cognitec develops market-leading face recognition technology and applications for industry customers and government agencies around the world. In various independent evaluation tests, our FaceVACS® software has proven to be the premier technology available on the market. Cognitec's portfolio includes products for facial database search, video screening, and biometric portrait capturing.
www.cognitec-systems.de

CRYPTOVISION

cryptovision is a leading supplier of innovative cryptography & public key infrastructure (PKI) products. The lean and intelligent design of the complete product range makes it possible to integrate the most modern cryptography and PKI application into any IT system. cryptovision PKI products secure the IT infrastructures of diverse sectors, from private enterprise to government agencies. The consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems to the design of complete cross-platform cryptographic architectures.
www.cryptovision.com

DE LA RUE

De La Rue is a leading provider of sophisticated products and services that keep nations, their economies and their populations secure. At the forefront of identity management and security, De La Rue is a trusted partner of governments, central banks and commercial organisations around the globe.

DIGITAL IDENTIFICATION SOLUTIONS

Digital Identification Solutions is a global provider of advanced identification solutions, specialized in secure government and corporate applications for ID cards and ePassports/Visa. By applying innovative technologies, they develop unique, scalable credential solutions, which perfectly meet the ever-changing demands of international customers.
www.digital-identification.com

HBPC

Pénzjegynyomda Zrt. (Hungarian Banknote Printing Shareholding Company) is the exclusive producer of 'Forint' banknotes, and is one of the leading security printers in Hungary, specializing in the production of documents and other products for protection against counterfeiting. Currently, HBPC produces passports, visa, ID documents, driving licenses, securities, duty and post stamps, tax stamps and banderols, paper- and plastic-based cards, with or without chip, and is aiming to provide complex system solutions.
www.penzjegynyomda.hu

HID GLOBAL

HID Global Government ID Solutions is dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide. HID Global Government ID Solutions offers government customers an end-to-end source for their most demanding state and national ID projects. With Genuine HID™, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Government ID Solutions offerings include expert consulting services, data capture, credential management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelaminates, LaserCard® optical security media technology, and FARGO® card printers.
www.hidglobal.com

HJP CONSULTING

HJP Consulting (HJP) with headquarters near Paderborn, Germany, is an internationally operating firm of IT consultants specialized in the planning, procurement and approval of smart card solutions with focus on e-identity and e-health applications. The manufacturer-independent specialists at HJP supervise large-scale projects for introducing e-passports and eID systems at both the technical and strategic level. The firm's consulting services encompass the areas of system architecture, software specification, tenders, quality and security management as well as project management.
www.hjp-consulting.com

THE IDENTIV GROUP

Identiv provides secure identification (Secure ID) solutions that allow people to gain access to the buildings, networks, information, systems and services they need – while ensuring that the physical facilities and digital assets of the organizations they interact with are protect- ed. Based in Orange County, California, it is a technology-driven company with significant experience in diverse markets, and is uniquely equipped to address the needs of customers worldwide in an evolving technological landscape.
www.identive-group.com

MASKTECH

MaskTech is the leading independent provider of high secure system on chip designs, embedded ROM masked products, security middleware, certification and integration services focused on human credential applications. MTCOS – MaskTech Chip Operating System – is a high performance and high security operating system, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.
www.masktech.de

MELZER

With 60 years of experience MELZER has been internationally recognised and established as the leading equipment supplier for the production of the most advanced ID documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customized solutions, the modular machine system and the lean production approach ensure and maintain unsurpassed yield rates, flexibility and profitability. The MELZER product portfolio also includes a broad range of versatile RFID converting equipment.
www.melzergmbh.com

MICROPROSS

Established in 1979, Micropross is the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Micropross has proven expertise in the design of laboratory and manufacturing test tools which are all considered as references in their domains. These tools allow users to fully characterize and test the electrical and protocol performance of products such as smartcards and smartphones in design, conformance, and production. In 2015, National Instruments acquired Micropross in order to accelerate their development and strengthen them as the leader on their market, constituting a major milestone in the life of both companies.
www.micropross.com

MIKRON

MIKRON was founded in 1964. With main activities in semiconductor manufacturing (Power Management Products and RFID) MIKRON is an important player within the financial strong industrial group of JSFC SISTEMA. MIKRON has about 1600 employees and is with a capacity of 50 Mio inlays and labels per month and a chip capacity of about 100 Mio per month the largest RFID manufacturer in Europe. Major activities are within the RFID and Industrial/Consumer market. Joint Venture and cooperation for technology will secure strong standing within the fast growing future market.
www.mikron-semi.com

OPEN LIMIT

OpenLimit SignCubes AG (www.openlimit.com) was founded in 2002 and is a wholly-owned subsidiary of the publicly traded OpenLimit Holding AG. The company is headquartered in Baar, Switzerland and has a subsidiary in Berlin, Germany. The group currently employs more than 60 highly qualified employees.
www.openlimit.com

OVD KINEGRAM

OVD Kinegram protect government documents and banknotes. More than 100 countries have placed their trust in the KINEGRAM® security device to protect their high security documents. OVD Kinegram is a Swiss company and a member of the German Kurz group. The company has accumulated over three decades of experience in the protec- tion against counterfeiting and maintains close contacts with police forces, customs authorities and internationally reputed security specialists. OVD Kinegram offers a full range of services: consulting, design, engineering, in-house production, application machines and support as well as after-sales service.
www.kinegram.com

PAV

PAV Card is a German, family-run business and one of the leading manufacturers for smart cards and RFID solutions. PAV products are used in many applications, ranging from hotel access, airport and stadium technology to the use in retail outlets and smart card applications, such as payment and health insurance. PAV's product range includes special heat resistant and tamper-proof ID cards as well as smart cards using the latest contactless technology for secure access solutions suitable for corporate buildings or sensitive access areas, such as airports.
www. pav.de

PRECISE BIOMETRICS

Precise Biometrics is an innovative company offering technology and expertise for easy, secure, and accurate authentication using smart cards and fingerprint recognition. Founded in 1997, Precise Biometrics today has solutions used by U.S. government agencies, national ID card programs, global enterprises, and other organizations requiring multi-factor strong authentication. Precise Biometrics offers the Tactivo™ solution, a smart card and fingerprint reader for mobile devices.

www.precisebiometrics.com

PRIMEKEY

One of the world's leading companies for PKI solutions, PrimeKey Solutions AB has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

www.primekey.com

PWPW

PWPW is a commercial company, entirely owned by the Polish Treasury, with a long tradition and extensive experience in providing security printing solutions. The company offers modern, secureproducts and solutions as well as highest quality services which ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.

www.pwpw.pl

REINER SCT

REINER SCT Kartengeräte GmbH & Co. KG, based in Furtwangen (Black Forest), Germany, is a leading manufacturer of OTP generators and smartcard readers for eCards, electronic signature and online banking in Germany. REINER SCT also develops products for secure online authentication, time attendance and access control. The technology company employs 45 staff and is part of the global and family-owned REINER group.

www.reiner-sct.com

ROLIC

Rolic Technologies Ltd. is an innovative Swiss high-tech company headquartered in Allschwil (Basel). Rolic modifies surfaces on a nano scale with polarized light to achieve unique optical effects and to manage light. New industry standards were set for LCD TVs, forgery-proof security devices and efficient OLED lighting products. Highly skilled staff in the Swiss headquarter continually develop, refine and extend Rolic's proprietary core technologies. The subsidiary Rolic Technologies B.V. (Eindhoven, Netherlands) engineers industrial solutions for the global customer basis.

www.rolic.com

SMARTRAC N.V.

SMARTRAC is the leading developer, manufacturer, and supplier of RFID and NFC transponders and inlays. The company produces ready-made and customized transponders and inlays used in access control, animal identification, automated fare collection, border control, RFID-based car immobilizers, electronic product identification, industry, libraries and media management, laundry, logistics, mobile & smart media, public transport, retail, and many more. SMARTRAC was founded in 2000, went public in July 2006, and trades as a stock corporation under Dutch law with its registered headquarters in Amsterdam. The company currently employs about 4,000 employees and maintains a global research and development, production, and sales network.

www.smartrac-group.com

TELETRUST

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the quality seal "IT Security made in Germany" and runs the IT expert certification programs "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Engineer for System Security" (T.E.S.S.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

www.teletrust.de

T-SYSTEMS

Drawing on a global infrastructure of data centers and networks, T-Systems operates information and communication technology (ICT) systems for multinational corporations and public sector institutions. T-Systems provides integrated solutions for the networked future of business and society. With offices in over 20 countries and global delivery capability, the Telekom subsidiary provides support to companies in all industries. Some 50,000 employees combine expertise with ICT innovations to add significant value to customers' core business all over the world.

www.t-systems.com

UNITED ACCESS

United Access is focused on secure, high-end smart card and RFID based solutions. We are acting as a security provider with a broad range of standard and integration components. United Access is the support partner for the Infineon smart card operating system SICRYPT. United Access provides secure sub-systems to various markets like public transport, road toll, logical access, logistics, parking systems, brand protection, physical access control and others.

www.unitedaccess.com

WATCHDATA TECHNOLOGIES

Watchdata Technologies is a recognized pioneer in digital authentication and transaction security. Founded in Beijing in 1994, its international headquarters are in Singapore. With 11 regional offices the company serves customers in over 50 countries. Watchdata customers include mobile network operators, financial institutions, transport operators, governments and leading business enterprises. Watchdata solutions provide daily convenience and security to over 1 billion mobile subscribers, 80 million e-banking customers and 50 million commuters.

www.watchdata.com

WCC

Founded in 1996, WCC Smart Search & Match specializes in the development of enterprise level search and match software for identity matching. Its software platform ELISE delivers meaningful identity matches using multiple biometrics and/or biographic data from a wide range of sources at sub second response times. ELISE is highly scalable and extremely robust, and is used by large health insurance companies and government agencies for immigration, border security and customs control. The company is headquartered in the Netherlands and has offices in the USA and the Middle-East.

www.wcc-group.com

WIBU-SYSTEMS

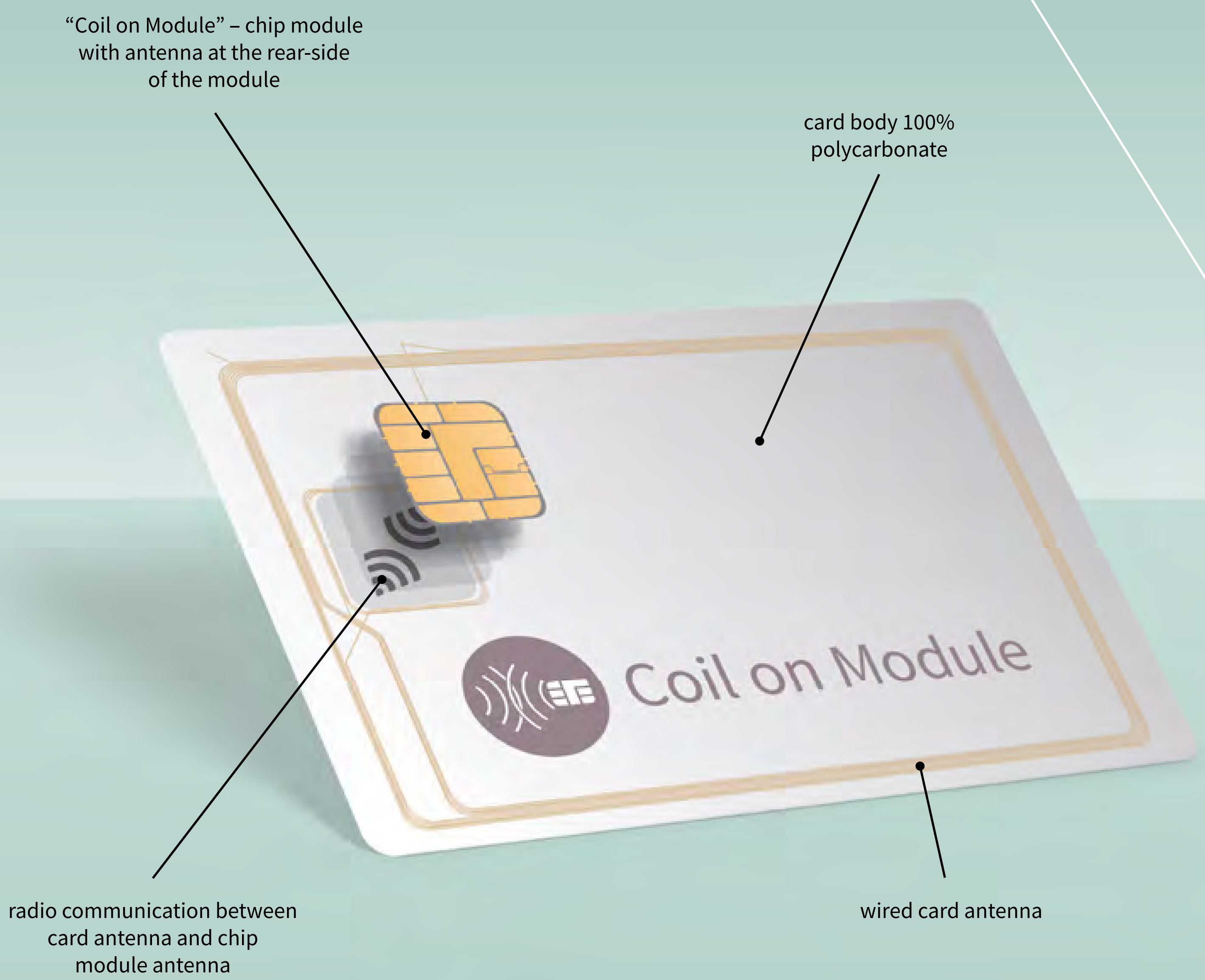
Wibu-Systems AG (WIBU®), a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market. Wibu-Systems' comprehensive and award winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and intelligent device manufacturers who distribute their applications through PC-, embedded-, mobile- and cloud-based models.

www.wibu.com

X INFOTECH

X INFOTECH, a leading systems integrator and a developer of software suite Smarteo, delivers premium solutions for issuing, managing and verification of electronic ID documents and smart cards. The company's turnkey solutions are fully independent and flexible, and in combination with unrivalled team expertise, allow smart card and eID programs to be implemented easily, adapting to any environment by supporting any equipment and chip type. With successfully implemented projects in 45 countries already, X INFOTECH is now a trusted business partner and preferred solutions and services provider for hundreds of customers.

www.x-infotech.com


"Coil on Module" – chip module with antenna at the rear-side of the module
card body 100% polycarbonate
Coil on Module
radio communication between card antenna and chip module antenna
wired card antenna

Go contactless with Coil on Module (CoM)

- CoM is designed to simplify your transition from contact-based to dual-interface card production
- CoM delivers a new level of card body robustness and reliability
- CoM is THE solution for 10 years life time – essential for ID documents

www.infineon.com/CoM

LIFE IS SAFER WITH

1st U2F certified smart card

www.austriacardag.com

AUSTRIACARD