NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2019 | #24

The VAULT

FEATURED ARTICLE

BORDER CONTROL ALONG INTERNATIONAL STANDARDS

Status, Trends and Outlook

ALSO IN THIS ISSUE

Contents

Imprint

THE VAULT
Published bi-annually by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Sächsische Straße 6, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Rainer Bergmann, Daniela Previtali, Detlef Houdeau , Philip Seebauer, Markus Hoffmeister, Klaus Schmeh, Steve Atkins,
PHOTOS: WIBU SYSTEMS, INFINEON TECHNOLOGIES, ISTOCKPHOTO, AUSTRIACARD, MÜHLBAUER ID SERVICES, OVD KINEGRAM, CRYPTOVISION, KROWNE COMMUNICATIONS, MELZER MACHINEBAU, PAV CARD
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE

Three DECADES ahead of the *CURVE*

Wibu-Systems at 30: Solving tomorrow's problems today

In early 1989, the world was a very different place: A continent divided by the Iron Curtain. In one of the very first cybercrime cases to make the headlines, German hackers had sold US military data to the Soviets. But most computer crimes were not feeding global political intrigue; it was all about floppy disks of cracked games sent through the mail.

In Karlsruhe, Germany, two students at the Karlsruhe Institute of Technology (KIT), Oliver Winzenried and Marcellus Buchheit, were already working to solve the problems of a future few people could imagine: Protecting digital assets with cutting-edge cryptographic means. Henceforth, WibuBox, a novel dongle-based DRM solution, was born. Finding answers to global issues long before society had even taken heed of the risks ahead, became one of Wibu-Systems' core characteristics.

The original WibuBox has since evolved into today's avantgarde software, hardware, and cloud-based CodeMeter software monetization technology. Then as now, Wibu-Systems protects the invaluable digital IP that is guiding and aiding more and more of our lives, from desktop applications to smart factories to critical infrastructures.

This year, Wibu-Systems is celebrating 30 years in business with its many channel partners, its loyal customers, and its faithful employees. For three decades, Wibu-Systems has been synonymous with excellence and perfection in protection, licensing, and security technology, making the business of software publishers and intelligent device manufacturers simpler and more profitable, while safeguarding jobs, health, safety, and the environment.

Since its inception, Wibu-Systems has remained true to its principles. An unwavering focus has been rewarded with a position as the unbeaten champion for protection technology, put to the test in many international hacking contests. In parallel, its versatile license and entitlement management platform has continued to advance and provide relevant insights that allow ISVs and IDMs to tailor their offerings to the delight of their customers, while growing their business. There is no better sign of the company's belief in its future and commitment to continued progress in its field, than the new headquarters and the House of IT Security that Wibu-Systems is building in Karlsruhe.

The pioneers of the company's earliest days are still at the helm: For Oliver Winzenried and Marcellus Buchheit, moving into the fourth decade of Wibu-Systems is simply the next milestone in their story: "When we started the company, there was no Internet. We did not know what the future held, but we wanted the world to be secure nonetheless. Now that the Internet of Things is becoming reality, we are continuing on that same mission – brought to life by our great people and enjoyed by our users everywhere."

Silicon Trust caught up with Wibu-Systems' co-founders Oliver Winzenried and Marcellus Buchheit at the company's headquarters in Karlsruhe and asked them to share their thoughts about Wibu-Systems' values, their customers, and what the future holds for the company.

L-R Oliver Winzenried, Founder & CEO Wibu-Systems AG, Germany, Marcellus Buchheit, Founder & CEO Wibu-Systems USA

Let us start with the most basic principle: What does Wibu-Systems stand for?

Oliver Winzenried: We provide protection, licensing, and security. What that means in practice is that our products empower our clients by giving them IP protection, novel licensing concepts that enable new business models, and security mechanisms that create value not just for them, but also for our society as a whole. That's a win-win situation for the makers of software and devices, for their operators, and for the end users. And we do all of this in a way that is fair and delivered in an ethical manner to ensure business success and a better environment for everyone involved.

Marcellus Buchheit: Wibu-Systems sells software licensing products. With effective software licensing, you know that every copy of your software that is in use was sold and bought legitimately – no illegal copies can slip through the net. We use top-notch security technology to protect licenses against hacking by anyone trying to crack our protective measures. And we do this via hardware, software, or the cloud, so that our customers enjoy the highest usability and flexibility. Our goal is that whenever a customer requires licensing – in any location, with any technology, on any platform – we have a solution for them.

What are the Unique Selling Points (USPs) of Wibu-Systems?

MB: Technology has changed over time. In the past, most people had a simple choice of operating systems: usually Windows or DOS. Today, we also have mobile platforms, embedded platforms, and even platforms created as homegrown solutions. Wibu-Systems intends to have a software licensing and protection solution available, no matter which requirements our customers bring to the table. We start with CodeMeter Runtime, which is available out of the box for operating systems such as Windows, Linux, and macOS; we also have very specific adaptations for other runtime platforms or embedded systems like Wind River VxWorks and Linux Embedded. For extreme cases, when customers want to start their own implementations from scratch, we can also provide the source code of our solutions.

The biggest advantage of CodeMeter over a homegrown solution is the sheer flexibility it offers for licensing. Consider licenses for on-demand or leasing products: Options like these are very important for our customers when it comes to marketing and selling their software solutions and products. We provide the same licensing flexibility for embedded systems or on-silicon solutions via CodeMeter License Central. It is all built to integrate seamlessly into our customers' back office systems, so their modules work with their own ERP, CRM, and e-commerce platforms.

> *We are committed to supporting our customers with new technology and will continue to innovate. This means balancing their demands with "blue-sky" work in domains like post-quantum cryptography, the IoT, edge, and embedded computing.*

OW: For me, Wibu-Systems' Unique Selling Point (USP) is our sole commitment to software security, software protection, and software licensing. To that end, we are investing in people, in infrastructure, in the development and innovation of our products, and in our relationships with our customers to build long-term trust and confidence.

This year, Wibu-Systems is celebrating its 30th anniversary. We have provided continuity from the very beginning; products from our company's legacy catalogue are still available (of course, in heavily improved versions). We are also investing in new branch offices abroad: We have wholly-owned subsidiaries in the USA, China, and Japan, as well as sales offices throughout Europe, which enable us to provide expert local consulting service for our customers. With Wibu-Systems being a financially independent and family-owned, mid-sized enterprise, we remain true to our vision. We are not looking for short-term profit, but rather for long-term relationships with our partners and customers.

How would you characterize the customers of Wibu-Systems? Are they specific to any industry? What are they looking for in Wibu-Systems' solutions?

OW: Every one of our customers expects something different from our solutions. What they have in common is that they need their IP protected – this is very important, as more and more functions and features are realized in software, and as the real intellectual property of manufacturers is hidden in the algorithms of the software code they own.

Our customers come from a very broad spectrum of industries. When we started the company in 1989, it was PC software that required protection; today, software is everywhere. Many of our clients are involved in industrial automation (PLCs, engineering tools, sensors, actuators), and there is growing interest from medical device makers as well. Medical technology is getting more and more connected (to a medical network or a hospital network), and more of its features are realized by software. Sophisticated companies like this have very specific requirements for licensing to create new business models. Security is increasingly on their minds: Medical device manufacturers want to protect the integrity of their units and the confidentiality of patient data. There is also the automotive sector, the after-market segment in particular, where we have many customers.

We are working in up-and-coming fields like the Internet of Things (IoT) or Edge Computing, where devices need to be managed through the cloud. That can be accomplished with our CodeMeter technology. And with technologies like artificial intelligence, we have leading manufacturers who need to protect the algorithms for their AI applications, like facial recognition for example.

MB: The great flexibility of our products is reflected in the wide variety of our customers. We're not really industry-specific nor are we specific to a platform; we have customers of all shapes and sizes. Some of them require ten licenses a year, others have millions of licenses a year. We have customers all over the world. We have customers with simple, low cost products; we have others with very expensive, very complex products; and we have customers who need to license a vast range of different features. Some of our customers require different licenses on demand. And then there are customers who are selling their products for embedded solutions, as well as those still for desktops. And they need both types to work with the same license and to be sold over the same in-house system. You cannot expect them to run two different licensing systems in parallel for embedded and desktop products.

Wibu-Systems is a big believer in 'Security Made in Germany' – Why is this so important to you?

OW: 'Made in Germany' is very close to our hearts. We have long-standing cooperation with German organizations like VDMA and bitkom, and we are working in research and development together with Germany's academic world, like the Karlsruhe Institute of Technology (KIT), the Karlsruhe Research Center for Information Technology (FZI), and Fraunhofer Gesellschaft. Internally, our engineering processes are designed carefully to meet the highest quality standards. This is especially important in the security field in which we operate, where small mistakes could be catastrophic and compromise the business of the thousands of active customers that trust our technology.

MB: Products 'Made in Germany' are world renowned for their perfection. That perfection does not just mean the high precision of the technology, but also its usability and the ability to understand the whole concept of the product. When you have a very complex technology like CodeMeter, you have different pieces that need to work together, and it is very important that these pieces are easily replaceable, can run over a long period, and remain backwards compatible. Our customers can feel confident that their products will fulfil their needs far into the future.

What's next in store for Wibu-Systems?

MB: For the past 30 years, Wibu-Systems has always remained dedicated to the needs of our customers. The most defining ideas for the future of our technology come from our close interaction with our customers. At the same time, we always keep an eye on new academic research and new innovations, and we adapt them to our business. In one recent case, our cooperation with the local KIT brought about Blurry Box, a cryptographic method that won the German Security award. It pushed obfuscation techniques beyond their current limits to even stronger, as yet unbeaten protection against reverse engineering.

OW: We are committed to supporting our customers with new technology and will continue to innovate. This means balancing their demands with "blue-sky" work in domains like post-quantum cryptography, the IoT, Edge, and embedded computing.

We are also investing heavily into our global growth. We are starting up new offices in other locations, which will result in a broader geographical footprint over the next five years. We are also investing into our new headquarters here in Karlsruhe – A new building is going up right now, close to our current one. It will host the House of IT Security as well, which we envision to be a hub for innovation in the security area, attracting companies from Germany and abroad. ☒

The CASE for the *eDATAPAGE*

By Philip Seebauer, Infineon Technologies

As globalization becomes more prevalent, so too are the number of passport holders and annual border crossings. Due to their safety-critical character, official identification documents must be developed according to the highest security standards in order to enable a reliable protection against manipulation and fraud. Safety must be guaranteed over an entire lifetime of at least ten years.

☐ With such a scenario, it is increasingly important to improve protection against passport forgery. A developing trend in this field are Polycarbonate datapages with an embedded security controller. The combination of security IC and Polycarbonate datapage has resulted in new possibilities to make passports even more forgery-proof.

The material attributes of Polycarbonate with its multilayer structure, which is indivisibly fused after lamination, enable significantly more security features at multiple levels. The vision panels also offer additional protection.

In comparison to conventional solutions, where the chip is located in the cover, Polycarbonate datapages with embedded security controllers – the so called eDatapages – increase protection significantly.

eDatapage upsides against manipulation

The eDatapage can prevent attempts of fraud. One example of this is Recycling, where several parts of documents are used to create a new one. The implementation of personal data on only one page makes the manipulation of the documents far harder.
Since the security features of the data sheet protect the security controller against manipulation, fraud is nearly impossible. Attempts to destroy the chip itself are easily recognized as mechanical damages, e.g. scratches, will remain on the PC material as evidence of any physical manipulation

In conjunction with the antenna, which is necessary for every electronical passport, eDatapages result in an effective, easy, safe and convenient solution against counterfeiting. The antenna, for example, can be used as a prevention against counterfeiting and manipulation techniques such as ‘Back Side Milling’. With Back Side Milling, the datapage from the back has to be milled and the passport photograph replaced with another one. Special antenna technologies with embossing or a nanogram coat will make it impossible to cover up such manipulations. Furthermore, the antenna can be used as an additional watermark, which, similar to banknotes, only appears when viewed by transmitted light.

A possible downside of the eDatapage

Due to its module design, standard CL packages, which are used for ePassports, require a multiple layer construction of compensation and crack prevention layers. This layer structure impairs the mechanical robustness on one hand, and on the other hand, only relatively thick data pages are possible.

This leads to rigid and inflexible data pages, which do not meet the flexibility and haptics of traditional passports without polycarbonate data pages. Due to the high costs for polycarbonates, a thicker data page is additionally more expensive than conventional solutions.

An Infineon solution for a more flexible and cost-effective eDatapage

Infineon Technologies has developed a special package solution for highly robust, flexible and thinner government ID documents – Coil on Module.

Infineon has developed its Coil on Module system, based on inductive coupling, to reduce the cost of dual interface data page 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 an ePassport with a ten-year lifecycle.

While the standard thickness for an inlay is currently 330µm with inductive coupling technology, Infineon now has a roadmap for contactless inlays to 200µm, giving the end document manufacturer much greater flexibility. This is an attractive argument for passport manufacturers, as they look to reduce the thickness of the eDatapage that carries the chip. Current eDatapages 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.

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 an advanced ruggedness of the eDatapage with enhanced tamper resistance, as well as a more flexible eDatapage. With these functionalities in place, the ten-year lifetime requirement of the ePassport becomes more of a reality.

With module solutions that are 50% thinner than standard packages (S-COMCL1-0-1 only 125µm) and do not require crack prevention, innovative antenna techniques like Coil on Module, and unique optical module authentication solutions (Nanogram) from Infineon Technologies offer the right solutions for the highest rigged security for the entire lifetime of the ePassport. ☒

BORDER *CONTROL* SECURITY along *international* standards: STATUS, *trends* and *OUTLOOK*

By Detlef Houdeau, Infineon Technologies

Back to 1979 the International Civil Aviation Organisation, called ICAO, published the standard on Machine-Readable Passport (MRP). Passport booklets with this function need a Machine Readable Zone (MRZ) based on the typeface Optical Character Recognition (OCR-B). The phase out of all non-MRP was set for CY 2015. By springtime 2006 ICAO has collected the first standard on electronic MRP, also named eMRP. Both "world standards" of travel documents have significant impacts on border control security and processes. This article give an overview on both aspects, the border process and the travel documents round the globe, starting with the application view.

Border control security without any electronic equipment

With the movement of persons into other territories since the late 19th century, passport and visas are used to allow foreigners to enter, remain within, or to leave another territory. The first travel document captured handwritten text, a seal and stamps of government authorities. The border control process along such travel documents was a completely manual workflow. Border police or other public or private authorities inspected the travel documents at the sea, air or land border and verify the face photo in the travel document with the face of the traveler.

Over many years, some of the weak aspects of this manual workflow were published. For example, the travel document is original and valid, but the traveler is not the same as the data in the travel document (it is reported that Malaysia airline flight 370 had two illegal travelers in the aircraft). Border police have overseen some minor differences between photo and the traveler face, where the travel documents showed some manipulation.

The only binding aspect between the travel document and the traveler is the face photo. This means many document frauds are based upon a manipulated face photo. To avoid such fraud, travel documents capture, as well as the face photo, a second hologram image of the photo, typically in smaller size. However, human behavior also plays a role; Border police can store typically up to 10 face photos of “wanted persons” in their mind. Computers can verify the traveler face photo with many thousand photos in central databases in a very short time. Two examples of such databases are Schengen Information Systeme (SIS) in Europe and Visitor and Immigration Status Indication Technology (VISIT) in the US, with hundreds of millions of traveler data sets. To avoid this weaker aspect of border control security, ICAO has collected and published the MRP-standard, as reflected in the next section.

Border control security with electronic document verification

With the roll out of MRPs, border police can use MRZ-inspection systems at the three borderlines - land (green), sea (blue) and air - in a 2-way inspection approach:

1. The inspection system will read and verify the MRZ-line in the holder page with an optical scanner.
2. The MRZ information represents all the data printed in the data page of the booklet. The first symbol of the MRZ-line define the country that issued the travel document. The inspection system uses this information to verify all optical security elements of the data page against a reference data set, stored in the inspection system in a library, which are based on optical security level 1 (visible) and level 2 (visible with simple technology, like UV-lamp).

With this approach, the inspection system can verify existing travel documents from all 189 member-states of ICAO in different document generations. The document library in the inspection terminal requires, from time to time, an update of the data because some states change the optical feature set of travel documents – typically every 10 years or more.

This new technology has increased border control security significantly. However, some fraudulent travel documents look very similar to the original. The verification of the face photo in the travel document with the holder must be done manually by the border police. To avoid such weakness, ICAO has collected the international standard on biometric verification of the traveler against the travel document, as addressed in the next chapter. Today, more than 50% of the ICAO member states use MRZ-Inspection systems and many airlines use swipe readers in keyboards computer for the check-in process. In addition, many banks needs the MRZ inspection system to register a new bank customer with 3rd country nationality.

' This new technology has increased border control security significantly. However, some fraudulent travel documents look very similar to the original.'

Border control security with electronic document and biometric holder verification, offline

With the standard ICAO 9303 part 3 and the related electronic travel documents (eMRP), border police have the possibility to use the 3-way verification approach:

- Verify MRZ and the validity of the travel document
- Verify the face photo in the booklet against the face of the traveler, manually
- Verify the electronic stored face photo against a camera photo of the traveler with a computer
- Verify the face photo on the data page with the electronic stored data, manually

The face photo as an image data set is stored in Data Group 2 (DG2) of the chip. Typically, JPEG or JPEG2000 compressed photos of the faces are stored. This could reduce the data set of 12 kbytes and with this, the reading time of the inspection system. The ICAO standard refers to the quality of the digital photo in ISO/IEC 19794-5.

If the procedure with the verification of the electronic stored photo and the camera photo of the traveler fails, some states have stored two fingerprint images (DG3), a second biometric data set, for a second line verification process. In Europe, this policy is defined with the directive EC/2252/2004 and since 2009, travel documents must be issued in all EU member states with both biometric data sets. In addition, some states in Asia, such as Singapore and Thailand, store two fingerprint data in the eMRP.

The data set in the ICAO-standard for fingerprint biometrics definesthe ISO/IEC 19794-2. On the point of data transmission quality, some government authorities have published their own requirements, like the FBI in the US with EFTS/F and the BSI in Germany with TR 03104. One fingerprint image needs approximately 16kbyte of data.

As well as the face photo image and two fingerprint images, ICAO has also defined an iris image, but this is not in use today along border control systems. The first tender on border control system based on iris have been publish in March 2019, for example, in Colombia. With the increase of passenger numbers(in air-traffic), some countries and the related airport ground handlers have fostered the development of Automatic Border Control (ABC) systems to speed up the security border control process. The next section describes the principle of ABC-systems also called ‘e-gates’.

Automated border control systems (e-gates), offline

After the first wave of eMRP’s roll out in 2006, it took two years for the first installation of e-gates to be implemented at airports, which use the electronic travel documents along with the ICAO standard. Some years earlier, some states spent effort on e-gates based on the Registered Traveler Programs (RTP). Such examples of these gates are CLEAR in the US, ABG in Germany, PEGASE in France, SAPHIRE in The Netherlands and iPass in Japan. Today more than 50 member states of ICAO have e-gates in use, mainly at airports, using the ICAO standard and the related travel documents. More than 90% of such e-gates are using face recognition technology. Between 2014 and 2018 the EU Commission spent some effort on pilot tests of ABC-systems along seaports and land border control systems, with two public funding projects FASTPASS and ABC4EU. Overall, ABC-systems can speed up the secure border process and can deliver the same high quality for the inspection process over many hours and perhaps more importantly, the human factor, as fatigue appearance can be avoided.

Automated border control systems online

The ICAO-standard has specified not only electronic travel documents collected with biometric data, but also many infrastructure aspects and so called ‘background checks’ are described. Some examples of this are;

- PKI/CSCA: member states of ICAO, which issue eMRP, must create an individual document identifier, created in a PKI trust center from a Country Signer Certification Authority (CSCA).
- CSCA-master list: this can be used to verify if travel documents from another country are valid or not.
- PKD: a worldwide central database can be used to identify lost or stolen eMRPs.
- “No-Fly-list”: PNR- and CSCA-data can be used to identify no-fly passengers.
- “Wanted-list”: different databases can be used to find “wanted persons”, for example SIS and API in Europe or VISIT and PNR in the US.

In any case, additional background checks need an online connection to a central database and consume more time at the e-gates than offline systems.

Travel document, trends on optical and electronic security

Back in the summer of 2003, ICAO NTWG started the standardization of electronic MRPs. Some 16 years later, a broad range of ID documents use this standard beside passport booklets (ID-3), such as;

- National ID-card with travel function; ID-1
- Residence Permit with travel function; ID-1
- Seafarer ID-Card with travel function; ID-1
- Frequent traveler card with travel function; ID-1

This section mirrors all relevant ID-documents, new standards, possible synergies and technical trends.

eMRP, 1st Generation
Based on the US Patriot Act from Oct. 2001 and the EU Thessaloniki declaration from Jun. 2003, ICAO NTWG started the work on the standardization of eMRP; on data groups, on access security, on mutual authentication and on biometric data. The world-standard for the 1st generation was publishes springtime 2005 and addresses four biometric data sets, with face (mandatory), fingerprints, iris and handwritten signature, and three security settings, with Passive Authentication (PA), Basic Access Control (BAC) and BAC/AA. AA stands Active Authentication. The deadline for issuing for 26 US Visa Waiver Countries was defined by Oct. 2006. The EU regulation 2242/2005 fixed the deadline for 27 Member States 2 months earlier in August 2006. The worldwide frontrunner was Belgium, with the issuing started by Nov. 2004.

eMRP, 2nd Generation
To reduce document fraud a 2nd generation of eMRPs were created from the Brussels Interoperability Group (BIG) by 2007, which captured an additional key, called EAC-key, to get access to the two-fingerprint data in the chip. The Brussels Interoperability Group (BIG) was an ad-hoc expert group under the article-6-committee of the EU Commission. The deadline roll out of all 27 Member States was set for Jun. 2009. Today, few states outside of Europe use this security architecture in their travel documents.

eMRP, 3rd Generation
To reduce the risk of eavesdropping travel documents, ICAO NTWG created and published an additional standard in 2012. SAC replaced the access security protocol BAC, now named PACE. The deadline for the EU Member States was fixed in Dec. 2014. Today PACE is mainly used in Europe.

eMRP, 4th Generation
During the first wave of issuing passports in 2006, ID-3 Polycarbonate (PC) holder-pages were only used in a few countries, like Finland, Sweden and The Netherlands. Since 2018 more than 55 countries around the globe are now issuing passports with a PC-holder-page. This evolution can be define as 4th generation eMRP to avoid document manipulation and fraud.

Today worldwide, more than 130 states issue eMRPs; the mainstream today is the 1st generation of eMRP. The annual cumulated volume is close to 150 million pieces. ICAO has defined the phase out for non-eMRP by the end of 2022.

LDS2.0, a new standard
With that view in mind, (the ICAO 9303 standard digitally addresses mainly the printed data of the holder-page (or cover-page) and biometric data),in 2014 ICAO NTWG started a new work item on digitalizing the “rest” of the booklet, meaning visas and stamps. As well as the previous Logical Data Structure LDS1.7, a second container is standardized, named LDS2.0. The standard has been published at the end of CY 2018. The integration into Doc 9303 is pending.

National ID-card with travel function
More and more countries put the ICAO-data set, including electronic security, biometric information and contactless interface into National eID-Cards. The first country to do so was Sweden in 2005. One of the largest programs running today is in Turkey with more than 10 million issued documents per year. Last year the EU Commission published a new directive COM(2018)212 on the minimum security of Member states ID-cards and refers to the ICAO-standard. The implementation deadline is defined for May 2021.

Residence Permit Cards with travel function
More than 50 states issue Residence Permit cards in ID-1 format for 3rd country nationals. These documents typically also use the ICAO-standard for data, security and biometrics.

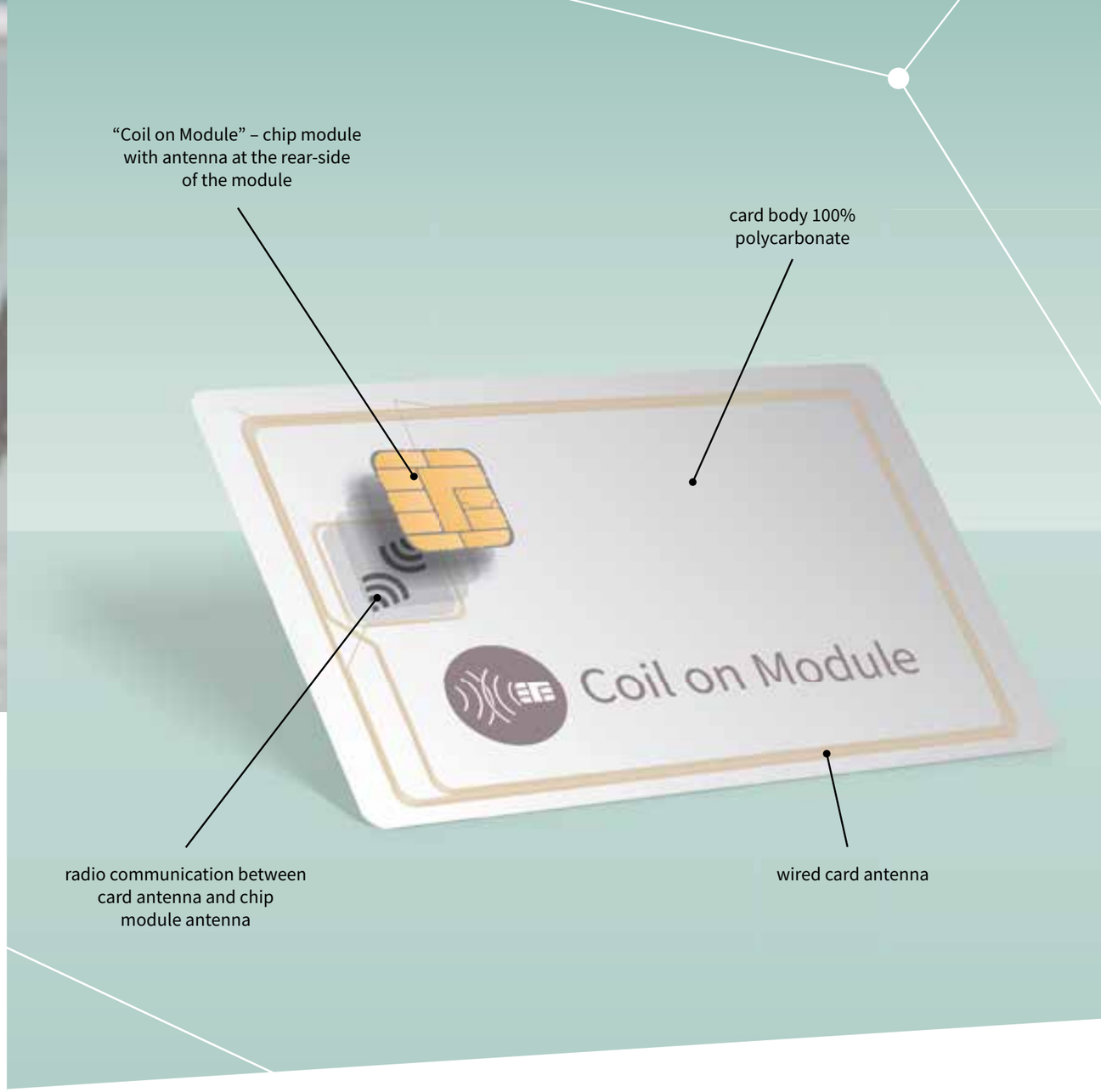
Seafarer Card with travel function
ILO publish in 2012 at a technical recommendation for a secure seafarer card, and refer in this recommendation to the ICAO 9303 standard. One of the frontrunners is Myanmar.
It is expected, that in a few years, the cumulated annually issued quantity of ID-1 documents, which need the ICAO standard, would be higher than the traditional ID-3 booklets.

Frequent traveler card based on the ICAO standard
Back in 2009, China tested, and later implemented, along the border control process to Hong Kong and Macao, a frequent traveler card, as a replacement for a booklet with a short time valid visa. The administration effort for the application can be reduced and the speed at the borderline can be increased significantly. Along both borders approximately 700.000 travelers cross the borderline every 24 hours.

Synergy amongst various ID-documents
Using the ICAO standard in different ID-documents can create some synergies in;

- Document production, such as personalizing
- Infrastructure, such as PKI/Trust Center
- Forensic lab, e.g. for verification of level 3 optical security elements

For the police on the street, a family concept on the optical design between the holder-page in booklets and ID-cards could be helpful.



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

New optical security elements
Similar to banknotes, the transparent window technology has moved to ID-documents, such as ID-3 booklets and ID-1 cards. In addition to banknotes, inside the transparent window an additional individual hologram can be placed. This hologram could be the face image of the document holder.

Another optical security topic would be a color photo in PC-ID1-Cards, which can´t be created using traditional laser engraving equipment.

Some security companies have created samples with 3-D face photo, collected on the PC card or holder-page.
All such research programs address additional optical security, to reduce fraud of official travel documents.

Outlook

The worldwide number of travelers is increasing dramatically, mainly in the area of air-traffic. IATA forecasts that passenger numbers will grow from 4.1 billion in CY 2017 to 7.8 billion in 2036. New standards for travel documents, such as the change from MRP to eMRP, and new technologies, as seen with the change from manual processes to ABC-systems, increases both border security as well as speed for the border process itself. In combination with other smart border processes, such as Electronic System for Traveler Authorization (ESTA) for online registration trust is increased for all stakeholders, such as travelers, transport organizations, border police and government.
If the border process doesn´t need visa and/or entry- or exit-stamps, the ID-card with the ICAO data and functions will take over the role of the travel document. As well as trust this will bring additional convenience to the traveler.
New standards, such as LDS2.0 and passport datasets stored in HW-security in Smart Phones have the potential to create new workflow processes and further increase border security and speed once again. The standard LDS2.0 has already seen over 95% of data collected. So, it is safe to say that the technology change from SIM-card to eSIM will remain a priority for the immediate future. ☒

Abbreviations

AA	Active Authentication
ABC	Automatic Border Control
ABG	Automat. Biometriegestützte Grenzkon.
API	Advanced Passenger Information
BAC	Basic Access Control
BIG	Brussel Interoperability Group
CSCA	Country Signer Certification Authority
DG	Data Group
EAC	Extended Access Control
EFTS/F	Electronic Fingerprint Transport. Spec.
eMRP	electronic MRP
eSIM	embedded SIM
ESTA	Electronic System for Traveler Authorization
EU	European Union
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ISO	International Standardization Organization
JPEG	Joint Photographic Expert Group
LDS	Logical Data Structure
MRP	Machine Readable Passport
MRZ	Machine Readable Zone
NTWG	New Technical Working Group
OCR-B	Optical Character Recognition
PA	Passive Authentication
PACE	Password Authentication Connection Establishment
PC	Polycarbonate
PKD	Public Key Directory
PKI	Public Key Infrastructure
RTP	Registered Traveler Program
SAC	Supplemental Access Control
SIM	Subscriber Identification Module
SIS	Schengen Information System
TR	Technische Richtlinie
US	United States
UV	Ultra-Violet
VISIT	Visitor & Immigration Status Indication Technology

ENROLLMENT, *Personalization* and DELIVERY of National ID Cards for *El Salvador*

Mühlbauer Provides the Citizens of El Salvador with ID Cards

Mühlbauer is operating the National ID project for citizens in the Central American Republic of El Salvador; the Salvadorian government has already extended the 2017 cooperation contract until June 2021.

☐ In 2011, the Government of El Salvador entrusted Mühlbauer with the task to implement and operate the National ID Card project. This project includes the provision of the actual ID card, approval and issuance clients, national databases, biometric systems, data and document management systems, secure communication methods with all national and international sites via MB DEOS, as well as twenty enrollment, personalization and issuance offices endowed with high-tech personalization machines and state-of-the-art software.

The project is based on a Public Private Partnership agreement and is executed as a Built-Operate-Transfer (BOT) project.

Decentralized Issuance of ID Cards

The Salvadorian ID cards are issued decentralized in 24 personalization centers across the country. All of the centers are connected to a central system that enables an automated identification of the citizens' fingerprints (AFIS, capacity of 12 million registries), system and data management (SDM, capacity of 10 million applications), user management and storage. In addition to these 24 service centers, there is also a headquarters, as well as a service and training center for staff. Mühlbauer also enabled 16 El Salvadorian consulates in the USA and Canada, so they can receive applications and issue National ID Cards to El Salvadorian citizens abroad.

In the meantime, the former, obsolete system has been completely replaced by a secure, modern and innovative system that has been designed by Mühlbauer specifically for this project. Within the first 15 months, the Salvadorian government deployed 3 million ID cards with high security features. Up to now, over 6.88 million national identity documents have been issued to the country's citizens.

In June 2017, the contract was renewed for an additional four years, so that Mühlbauer continues to be the strategic partner of the government of El Salvador until June 2021. Within the scope of the contract extension, the second generation of ID cards with enhanced security features is being issued.

Exceeding Expectations

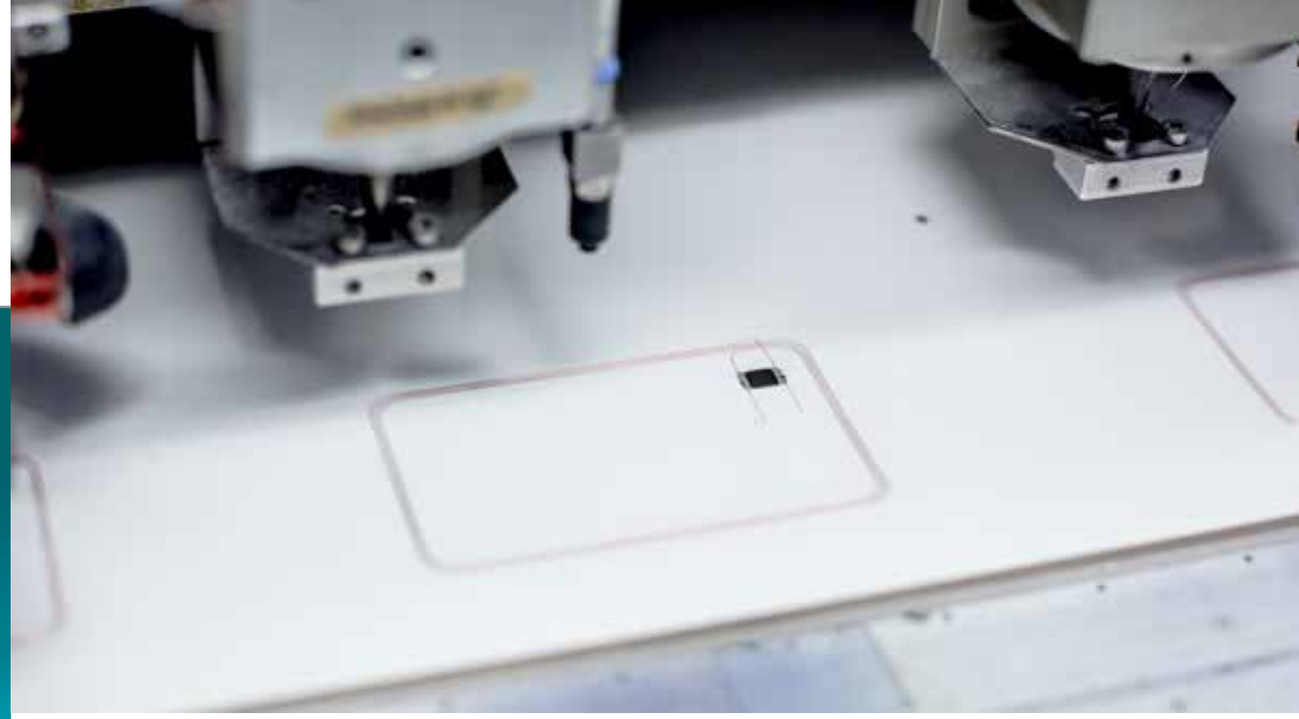
In 2018, the daily production reached a record of 15,949 issued documents. A fact that is particularly remarkable considering the system was initially required for a production of just 3,490 documents per day, exceeding expectations with a five-fold increase in capacity. The speed from data collection to the issuing of ID cards is equally impressive: on average, it only takes 15 to 20 minutes from the citizens' entrance to their exit with a brand new, personalized ID card.

This efficiency is made possible by a well-organized service, as well as by the standardization of the enrollment process, ID card personalization and final delivery to the citizens in all of the passport centers.

Better Employment within El Salvador

Today, Mühlbauer employs over 400 people in El Salvador. Mühlbauer El Salvador, with its qualified staff, is the backbone for all Mühlbauer operations in Central America. Furthermore, the government of El Salvador has also awarded the company for its exemplary work conditions in the Service Centers across the country.

In addition, the Salvadorian Social Services Institute recognizes Mühlbauer as a national example in the implementation of better working conditions for women and Mühlbauer is leading in terms of inclusion and equality of Salvadorian citizens in the workplace.☒



PAV Card

– A FAMILY FIRM supplying *worldwide SOLUTIONS* for Govt. ID, HEALTH and *FINANCE*

As a family business, headquartered in Lütjensee near Hamburg, PAV is one of the leading manufacturers of card and RFID solutions for global players in all industries. Therefore, their products can be found (almost) everywhere. At the hotel, traveling, at the stadium, shopping, in the mailbox, and most likely in your wallet.

The company's products and solutions range from heat-resistant ID cards for the police in Abu Dhabi, contactless employee ID cards for numerous DAX companies and contactless cards for airport access control. PAV also supports many companies in the development and production of initial samples, such as smart cards and rely on proven components from the world's leading semiconductor manufacturers. All cards are produced in their high security area, which meets the highest security requirements.

Government ID and Passports

In addition, PAV supplies a large number of European, African and Asian countries with passport and ID card inlays. Synthetic paper or PC inlays can be processed in any conventional passport. These inlays can be easily integrated in the cover, as well as into the data page. The RFID technology makes it possible to read out the data contactlessly and offers the highest level of security against counterfeiting. The polycarbonate inlays are mainly used for passport data pages or ID cards, whereas the synthetic paper inlays are excellent for e-cover solutions of passports.

Inlay production at PAV has been evaluated by the Federal Office for Information Security (BSI). In 2004, PAV was chosen, because of their highly advanced production technology, to participate in one of the first field tests for e-passports in Europe. Today, the family-owned company supplies numerous states with inlays for e-passports and ID cards.

Health & Donor Services

Around 90 per cent of the population in Germany is insured by the statutory health insurance system. PAV has also been a partner to the German health industry for many decades. Their portfolio ranges from production of the electronic health card (eGK) for health insurance funds, to customised prescription forms for physicians in private practice in Germany.

As a renowned producer of the health insurance card, PAV has also been commissioned by numerous health insurance funds to produce the electronic health card. The card's innovative technology helps to improve communication between physicians, dentists, pharmacies, hospitals and health insurance funds. One of the main features of the electronic health card is a photo of the insured person, which stops card abuse from the outset. PAV obtains the photos beforehand by letter, online upload or MMS. The image management system which was specially developed by PAV, reflects our extensive experience in image processing technology.

PAV also personalises and encodes the cards. The electronic health card stores the insured persons data, such as name, date of birth, gender, address, insurance number, status, etc. The cards are sent to the respective insurant by PAV's lettershop. To ensure that all the cards are reaching the right recipients, in the high-security area each chip is read out and compared with the assigned address before being enveloped.

There is also a growing demand for applications that provide complex solutions and higher levels of security in the German health insurance system. Microprocessor cards with large storage capacities are particularly suitable. One example is the new blood donor card issued by the German Red Cross. The regional ID cards which were previously used have been replaced step by step since 2012, by a smartcard with an integrated RFID chip and a microprocessor.

The blood donor services commissioned PAV to produce the new blood donor cards, which also includes personalising and encoding the cards. In addition to the blood group, only the holder's surname, first name and date of birth are stored on the chip. This modern system now allows blood to be donated anywhere in Germany.

The electronic blood donor cards are also produced in their high-security zone, which meets all the security requirements and the cards are send directly to the holder by PAV's in-house lettershop.

Contactless, RFID and NFC

The growing demand for contactless cards continues as they are deployed for access control, time tracking, as tickets for public transport or as cards for spas and tourist areas. PAV is able to supply customers with RFID cards containing chips from all major semiconductor manufacturer, including the RFID market leader Infineon. Additional security features, such as holograms, can also be integrated in the cards on request.

Microprocessor-embedded cards are now used whenever applications involve a security dimension, for example in closed payment systems. The chip on such cards has its own operating system, ensuring that data can not only be stored, but also processed and encrypted on the card itself. That means that different applications can be configured freely and strictly separately from each other in respect of size, access rights management, security levels and password management.

Customised antenna layouts also enable PAV to change the shape of the card, or to include slotted holes for card clips and all cards are produced in their high-security, ISO 27001-certified area, which meets all data security requirements. PAV also provide two or more chips in one so-called hybrid card. One example of how a hybrid card can be used, is a globally operating company which uses different card types for access control at its various locations. Employees who work at several locations can be given easy access to the respective buildings using just one card, thanks to an appropriate solution designed for this case.

In addition to classical contactless RFID cards, PAV also produces NFC cards (tag type 2+4) which can be read and written into using NFC-capable mobile phones. A customised antenna enables an optical personalisation with hardly any restrictions on the cards. Combined with PAV's ability to equip the cards with additional storage or microcontroller chips, the cards are also suitable for security applications. PAV's NFC cards in credit-card quality have a long service life, in accordance with the ISO standard.☒

Why eID cards and DIGITAL *Signatures NEED* each other

By Markus Hoffmeister & Klaus Schmeh, cryptovision GmbH

Developed in the 1970s, digital signatures are the technology of choice when it comes to protecting eID cards from forgery and manipulation. More generally speaking, digital signatures are an important means for making digital documents – such as contracts, receipts, and orders – reliable, provided that the private key used is stored in a protected environment. An eID card is an ideal solution for this purpose. It is therefore justified to say that digital signatures are an important means to enable electronic identity documents, while electronic identity documents are an important means to enable digital signatures.

> *Almost all major future technologies in the IT sector, including cloud computing, internet of things, and blockchain, will profit from digital signatures or even require them.*
>
> *-Ben Drisch, cryptovision*

☐ Digital signatures: mathematics used in practice

There was a time when a discussion about digital signatures typically started with an explanation that a digital signature is not a scanned manual signature. Meanwhile, at least in the eID business, such a clarification is not necessary anymore. Instead, it is common knowledge that a digital signature is a checksum created with a private key and verified with a public key. The theory behind digital signatures, mainly developed in the 1970s, is an interesting example of how advanced mathematics (in this case: number theory) can be applied in everyday life.

Digital signatures solve one of the major security problems that occurs whenever analogue processes are digitalized. While it is difficult to alter a physical document – such as a money bill or a signed order – without leaving traces, it is ridiculously easy to change or forge a digital document. To prevent this, data can be digitally signed. As a digital signature requires a private key only known to its owner and as each alteration of the signed data changes the signature (i.e., the checksum), fakes and changes are easily detected.

Digital signatures are an important technology enabler for electronic identity documents. Virtually every eID card bears a digital signature that protects its digital content from alterations and prevents forgeries. The ICAO 9303 standard requires a digital signature as a part of the Logical Data Structure (LDS), which contains the personal data stored on an eID document.

However, a digital signature does not protect data from being copied (because it is always possible to copy the signature along with the signed data). In addition to including a digital signature, an electronic identity document therefore should be equipped with physical security features that are hard to counterfeit. Apart from this, such a document needs to contain a tamper-proof chip, the content of which cannot be copied. To unambiguously identify this chip (and the card and its holder), again digital signatures come into play. Using a private signature key stored in the chip, the card holder can identify himself in a secure and easily verifiable way by creating a digital signature.

eID enables digital signatures

Digital signatures are not only a technology enabler for eID cards – it's also the other way around. There are numerous applications of digital signatures that are not eID-related, examples including contract signing, signed receipts, signed bills, and code signing. It is clear that such a usage is only secure and convenient if the user's private key is stored in a protected environment he has easy access to. An electronic identity card is ideal for such a purpose. For this reason, modern multi-purpose eID cards usually provide a digital signature application.

Electronic identity cards with a digital signature application are generally expected to make digital signatures more popular. Ben Drisch, eID consultant at cryptovision, explains: "The more people have an electronic identity document that supports digital signatures, the more attractive this technology will be for both users and service providers." The legal foundation for a widespread digital signature use has long been laid, with countries all over the world having created digital signature acts. As one of the most important legal frameworks of this kind, the European Electronic Signature Regulation (also known as eIDAS) has been put into practice.

While it is easily possible to implement digital signatures in software only, with keys stored on the user's hard drive, eIDAS and most other digital signature acts require that the private key of the user is stored on a smart card or in a similar hardware environment – at least for the more important digital signature applications. As eID cards are ideal for this purpose, digital signature legislation is generally considered an important eID supporter.

Digital signatures and future technologies

In many countries, it is already possible to digitally sign a tax declaration and other e-government documents. Code signing and workflow signing are popular digital signature applications, too. Nevertheless, there is still much room for additional digital signature usage, including electronic banking, e-procurement, and digitally signed contracts.

cryptovision's Ben Drisch expects that additional application fields will develop soon: "Almost all major future technologies in the IT sector, including cloud computing, internet of things, and blockchain, will profit from digital signatures or even require them." Cloud computing, for instance, by definition takes away data from the user's control, which makes alteration easily possible – something that can be prevented with digital signatures. In the internet of things, protecting data and identities with digital signatures plays a crucial role, too.

And then, blockchain is a technology that inherently depends on digital signatures, because all transactions need to be digitally signed. Using an eID card for signing a blockchain transaction is an interesting option that may close the gap between independent payment systems, such as BitCoin, and state-run identity cards. Perhaps, a blockchain-based payment function will one day be a standard application of an eID card. The digital signature functions of electronic identity cards will certainly support this. ☒

Where *INNOVATION* meets RETURN on INVESTMENT for *identity SOLUTION* manufacturing

An interview with Dirk Melzer, Melzer Maschinenbau

Silicon Trust spoke with Dirk Melzer of Melzer Maschinenbau, to find out more about why this “Made in Germany” brand has managed to stay successful in a slow-moving market. We also discussed ensuring return on investment when production equipment makes up such a substantial part of any new system.

☐ Mr. Melzer, your company has been at the forefront of innovation when it comes to specialized machine construction. What are the drivers behind this success?

DM: Well, for more than 60 years now, MELZER has been serving customers all over the world with tailor-made solutions. Our clients appreciate the flexibility, reliability, experience and competence of our team, which in turn ensures that the customer requirements are turned into high quality machines. All of the design, manufacturing and assembly of our machines, parts and components are done in-house to the highest standards. Combined with the company’s flexibility, this enables MELZER to quickly analyse special requirements and turn them into high quality solutions.

Which markets are you targeting with your machines?

DM: Our modular designed machines are being used to manufacture highly precise and very sophisticated multi-layer products for the pharmaceutical, automotive, microelectronic, public transport, printing and many other industries. In terms of products, this includes the production of high-end RFID cards, chip cards, inlays, ID cards, e-passports, e-visa-stickers and RFID labels.

What is MELZER’s mission?

DM: The worldwide success of MELZER is the motivation to continuously improve quality, reliability and cost-effectiveness

of our products, while achieving higher levels of performance. So, really, anticipating the latest developments and doing whatever it takes to serve customers' needs is MELZER's mission

How does MELZER serve the market for secure ID solutions?

DM: We offer flexible production solutions for the next generation of multiple ID and security documents that, according to the ICAO standard, are provided with contactless technologies. Thanks to the modular and compatible design of each machine series, individual solutions can be created out of the existing components. This not only saves development time, but makes each MELZER production line a reliable and future-proof investment. Whether electronic Passports, NID cards, Driving Licenses or visa stickers – all RFID documents have an inlay that can be produced on MELZER M4 machines.
For ePassport holder page production, eNID cards and all other RFID data carriers made of plastic and being in ID-1, ID-2 and ID-3 format, the MELZER card lamination line offers the ideal production environment. Short cycle times are easy on materials and electronics and the highest precision and process stability ensure the absolutely reliable production of high-end RFID products.
For producing ePassport covers and eVisa stickers, MELZER also offers special solutions that can be adjusted to the requirements .

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 more than 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 the 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 to 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. ⊠

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

AUSTRIACARD 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

AVATOR

AVTOR LLC is an integrator of cybersecurity solutions and the leading Ukrainian developer in the field of cryptographic protection of confidential information. The AVTOR's hardware secure tokens and HSMs are based on smartcard technology and own smartcard operating system "UkrCOS" are compliant for operations with qualified digital signatures and classified information.
AVTOR provides services for development and integration of complex cybersecurity systems for automated systems for different purposes and any level of complexity and predominantly deals with: protection of data transfer (IP-traffic); secure electronic document management; developing corporate and public certifying authorities (CA) in public key infrastructure (PKI); integration of complex information security systems; development of special secure communications systems.
http://www.avtor.ua/

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

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.
www.delarue.com

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

MÜHLBAUER ID SERVICES GMBH

Founded in 1981, the Mühlbauer Group has grown to a proven one-stop-shop technology partner for the smart card, ePassport, RFID and solar back-end industry. Further business fields are the areas of micro-chip die sorting, carrier tape equipment, as well as automation, marking and traceability systems. Mühlbauer's Parts&Systems segment produces high precision components.
The Mühlbauer Group is the only one-stop-shop technology partner for the production and personalization of cards, passports and RFID applications worldwide. With around 2,800 employees, technology centers in Germany, Malaysia, China, Slovakia, the U.S. and Serbia, and a global sales and service network, we are the world's market leader in innovative equipment- and software solutions, supporting our customers in project planning, technology transfer and production ramp up.
http://www.muehlbauer.de

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, secure-products 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, 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 computers, PLC, 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

IDENTITY WEEK

GLOBAL • TRUSTED • VISIONARY

SDW2019 | PLANET BIOMETRICS 2019 | DIGITAL:ID 2019

EXPLORING NEXT-GENERATION GOVERNMENT, COMMERCIAL & CITIZEN IDENTITY SOLUTIONS

- Identity Week comprises of three world-class events: Digital:ID, Planet Biometrics and SDW - all focused on the concept of identity.
- At Identity Week 2019 join: **3000+ Event Attendees | 500+ Conference Delegates | 200+ Exhibiting Organizations | 250+ Speakers | 3 Co-located Events | From over 80 countries**

IDENTITY WEEK
3 Days • 3 Exhibitions • 3 Conferences
11-13 June 2019
ExCeL, London, UK

Created by

science media partners

SPARK SOMETHING TERRAPINN

www.terrapinn.com/identityweek