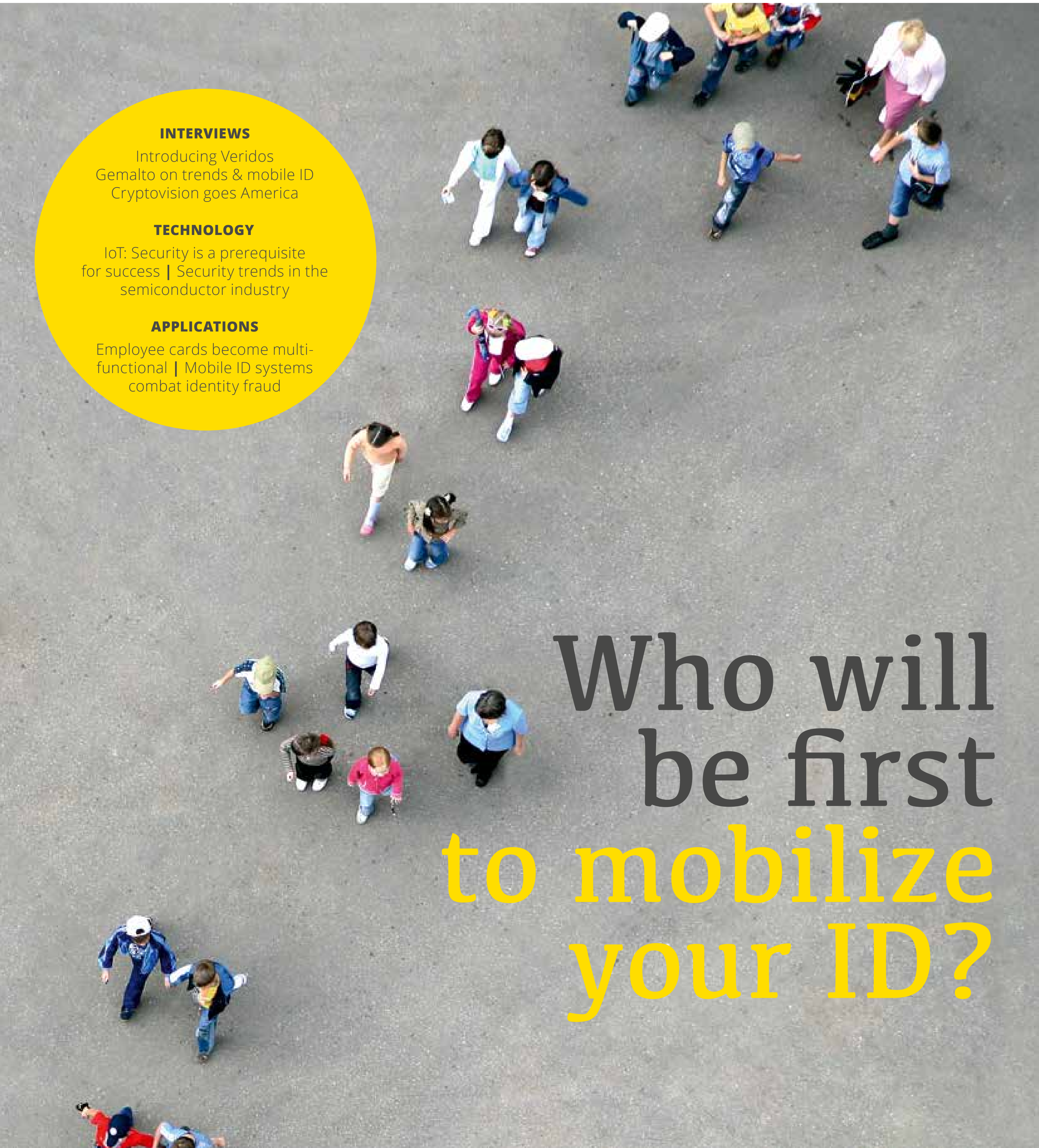
NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

MAY 2015 | #16

# The VAULT



**INTERVIEWS**

Introducing Veridos
Gemalto on trends & mobile ID
Cryptovision goes America

**TECHNOLOGY**

IoT: Security is a prerequisite for success | Security trends in the semiconductor industry

**APPLICATIONS**

Employee cards become multi-functional | Mobile ID systems combat identity fraud

## Who will be first to mobilize your ID?

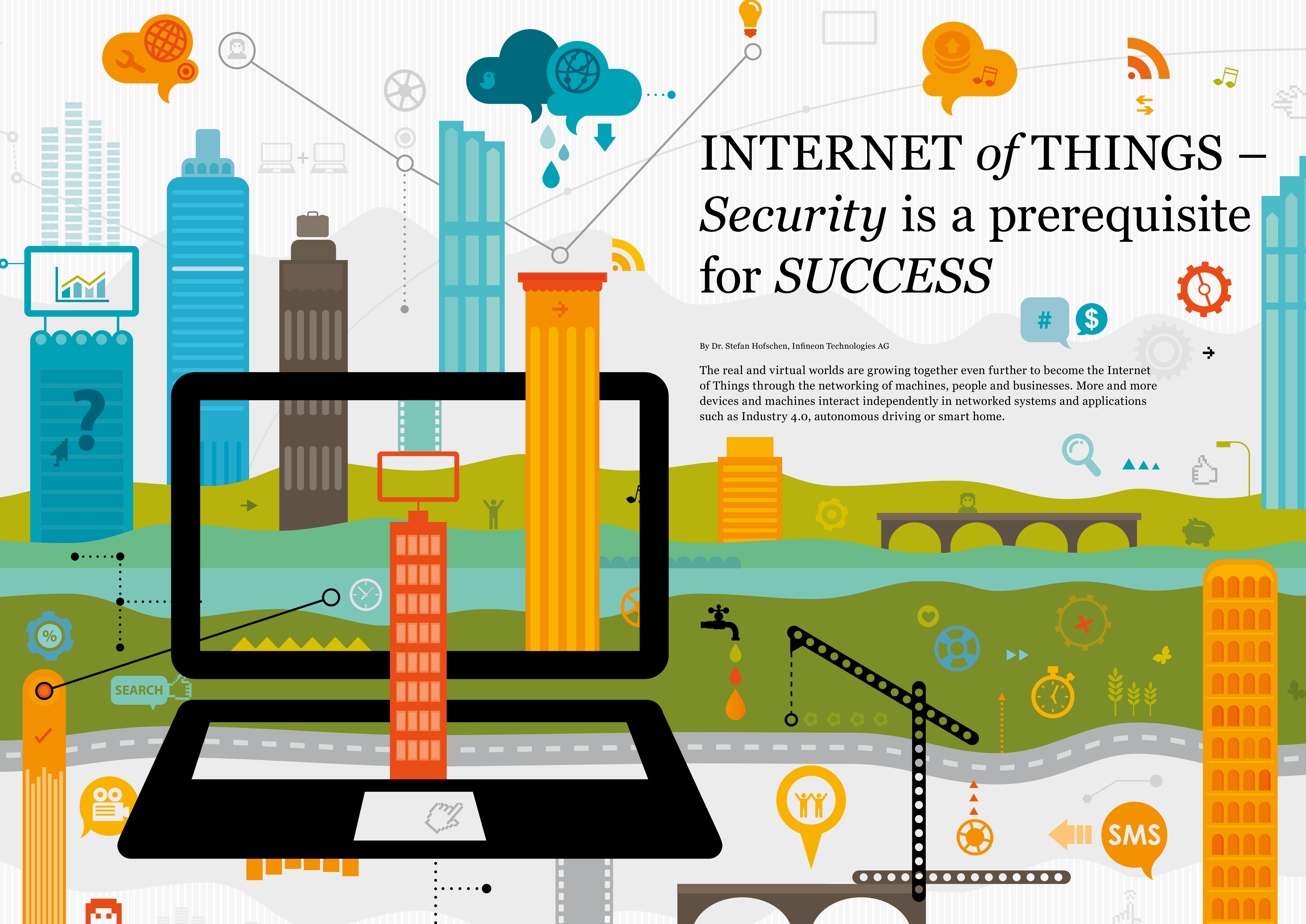
# Contents

## 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: Veronica Atkins
ART DIRECTOR: Katja Gebien

EDITORIAL CONTRIBUTIONS: Dr. Stefan Hofschen, Youzek Kurp, Rob Haslam, Sonja Schöberl, René Schädler, Wolfgang Kunz, Hermann Sterzinger, Dr. Dirk Woywod, Daniela Previtali, Brian Kowal
PHOTOS: Veronica Atkins, Infineon Technologies, Wibu-Systems, istockphoto, Veridos, HID, Gemalto, Bundesdruckerei GmbH
PRINTING: Druckerei Häuser KG, Cologne
EDITION: Spring 2015



# INTERNET *of* THINGS – *Security* is a prerequisite for *SUCCESS*

By Dr. Stefan Hofschen, Infineon Technologies AG

The real and virtual worlds are growing together even further to become the Internet of Things through the networking of machines, people and businesses. More and more devices and machines interact independently in networked systems and applications such as Industry 4.0, autonomous driving or smart home.

□ Especially in the context of Industry 4.0 and the automotive industry, the increasing connectivity provides a great number of opportunities for the economy. Yet, it also presents great challenges for businesses, foremost in questions of data security. How can business secrets and intellectual property be protected on the open Internet? How is data protection and confidentiality ensured? How secure is the communication between the different devices or components? And how can attacks be recognized and potential damage prevented? In short, data security and system integrity are essential for the success of new business models, because they protect the availability and reliability of products and services.

## Security controllers protect networked IoT systems from unauthorized access and manipulation

Industry has come to understand that connected systems cannot be adequately protected with software alone. The combination of software and hardware offers significantly more efficient protection against attacks and manipulation. Depending on the application scenario, there are special security chips that take the required security standard and the application's efficiency optimisation into account.

## Internet of Things in the example of Industry 4.0

The next revolution in industrial production, the so-called smart factory or Industry 4.0, presupposes a secure data exchange. Intelligent machines, storage systems, production facilities and intelligent products are connected globally. This networking increasingly also takes place between supplier and customer, especially for large or mid-sized companies. Figuratively speaking, Industry 4.0 opens the doors to the factories. This openness increases the need to prevent manipulation and sabotage of networked production systems and avert related financial losses. After all, smart factories can only be put into practice and accepted when they can be implemented in a stable and efficient manner, and when the process know-how and intellectual property (IP) is protected reliably.

> *Figuratively speaking, Industry 4.0 opens the doors to the factories. This openness increases the need to prevent manipulation and sabotage of networked production systems and avert related financial losses.*

At the IT Summit 2014 in Hamburg, Infineon, Deutsche Telekom, Fraunhofer SIT, TRUMPF, WIBU-SYSTEMS and Hirschmann (a Belden Company) demonstrated how a "security solution made in Germany" can be implemented in industrial applications. The demonstration shows how seamless communication security works beyond the boundaries of sites or businesses. An employee at the Munich site starts a production order on his tablet PC and transmits it via a secured communication channel to the production site in Hamburg. The order is then automatically executed by a production machine there.

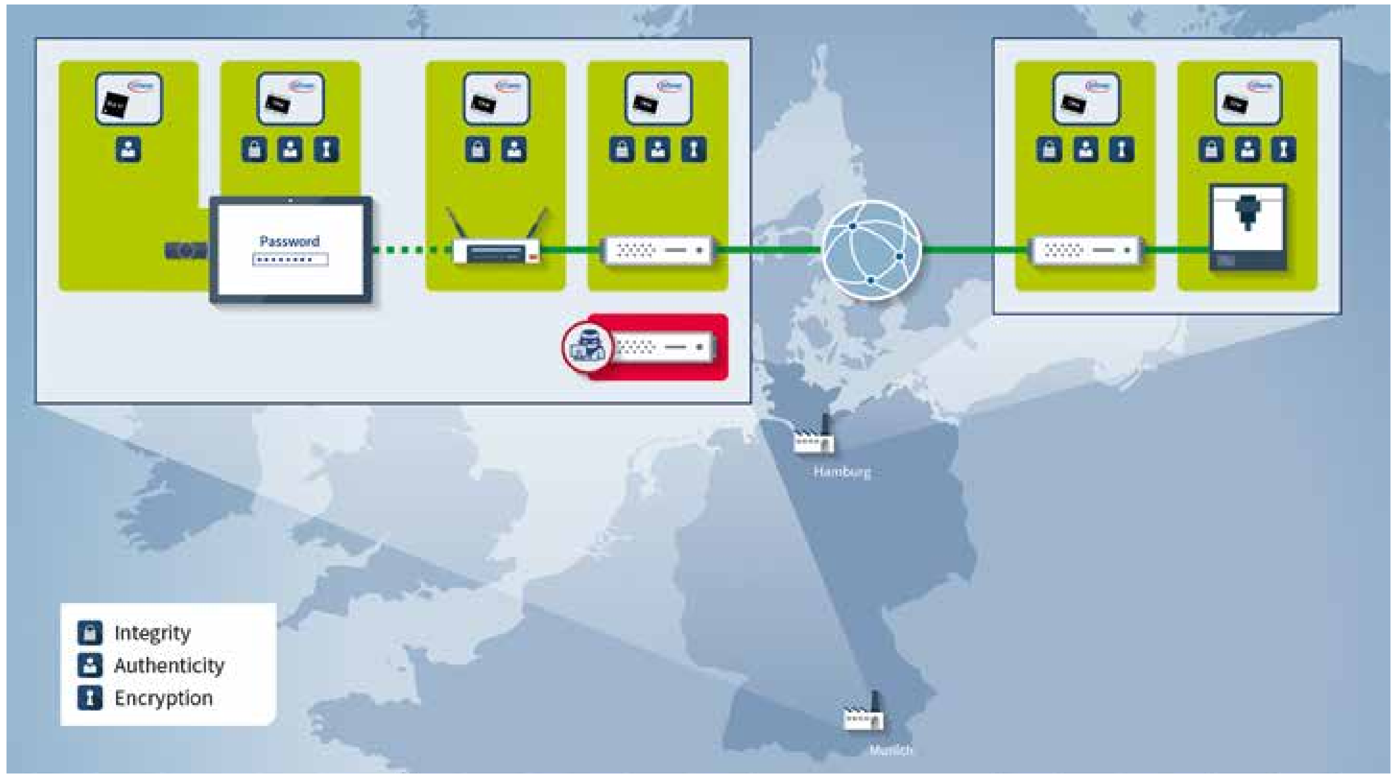


*Figure 1: Seamlessly secured end-to-end communication (diagram of the demonstrator solution presented at the IT Summit 2014)*

To secure the communication from one end of the value chain to the other (Figure 1), security controllers – in this case Trusted Platform Modules (TPMs) – are integrated in all devices of the IT network (tablet PC, wireless access point, router, production machine). They function as data resource, and as encryption and authentication components. They fulfill multiple functions at the same time:

- Similar to electronic identity verification, they securely identify the individual system components. Only authorized persons and devices obtain access to the network.
- At the device level, they are the basis for detecting manipulation or attacks on components or on the device itself. This way, both logical as well as physical attacks can be detected and corresponding pre-defined measures can be initiated.
- As a Secure storage location, they secure secret information that is needed to encrypt a secure communication channel.

The solution fulfills particularly high security requirements because the security controllers are evaluated and certified by the BSI (Federal Agency for Security in Information Technology) as well as according to "Common Criteria", an international standard. The certification meanwhile is not only granted at the product level, but also includes the complete production and supply chain. This affords the greatest possible security to the users and increases flexibility in the users' own production.

A secured complete system was presented as the first prototype at the IT Summit and the solution is to be marketed as soon as possible in 2015. The hardware components already exist today, so that further scalable solutions can be developed for every other application case.

## Trusted Platform Module as security anchor for end-to-end communication

Thus far, communication within company networks is primarily secured by means of pure software solutions. However, these harbor a few drawbacks compared to hardware-based security such as a TPM (Figure 2) and they are inadequately secure over the long term. Software in principle always consists of written code that can usually be read, copied or overwritten relatively easily, which enables attackers to bypass the security functions programmed by it. The TPM in contrast can serve as a security anchor for components and software: keys that are stored in the TPM are protected from leaving the security chip and are used in combination with authorization only.

> *Software in principle always consists of written code that can usually be read, copied or overwritten relatively easily, which enables attackers to bypass the security functions programmed by it.*

*Figure 2: OPTIGA™ TPM (Trusted Platform Module) from Infineon*

At the same time, the TPM that is installed on the motherboard uses international standardized cryptographic algorithms. Integration is provided via standard interfaces like I2C or LPC. The module also permits for example, that keys, data and digital signatures are stored securely, verified and transmitted. The TPM is equipped with a special internal processor for the purpose of the aforementioned authentication and encoding, which enables it to generate keys in a trustworthy environment. At the same time, a specialized crypto processor system allows the quick calculation of RSA cryptography at up to 2048 bits and thus permits the secured execution of complex cryptographic operations. A non-volatile memory with its own encryption preserves important data and keys stay on shut-down.

The integrity of the software structures and the executed programs on the system can be checked in that the boot process of the system is logged and confirmed against stored cryptographic checksums. Any manipulation of the software can thereby be recorded and stopped, by shutting down the affected components or disconnecting them from the network. This way, also the execution of malware like viruses, Trojans and worms can be detected and their spread stopped. Otherwise, this malware can execute unnoticed in the boot process and even spread throughout an enterprise without detection.

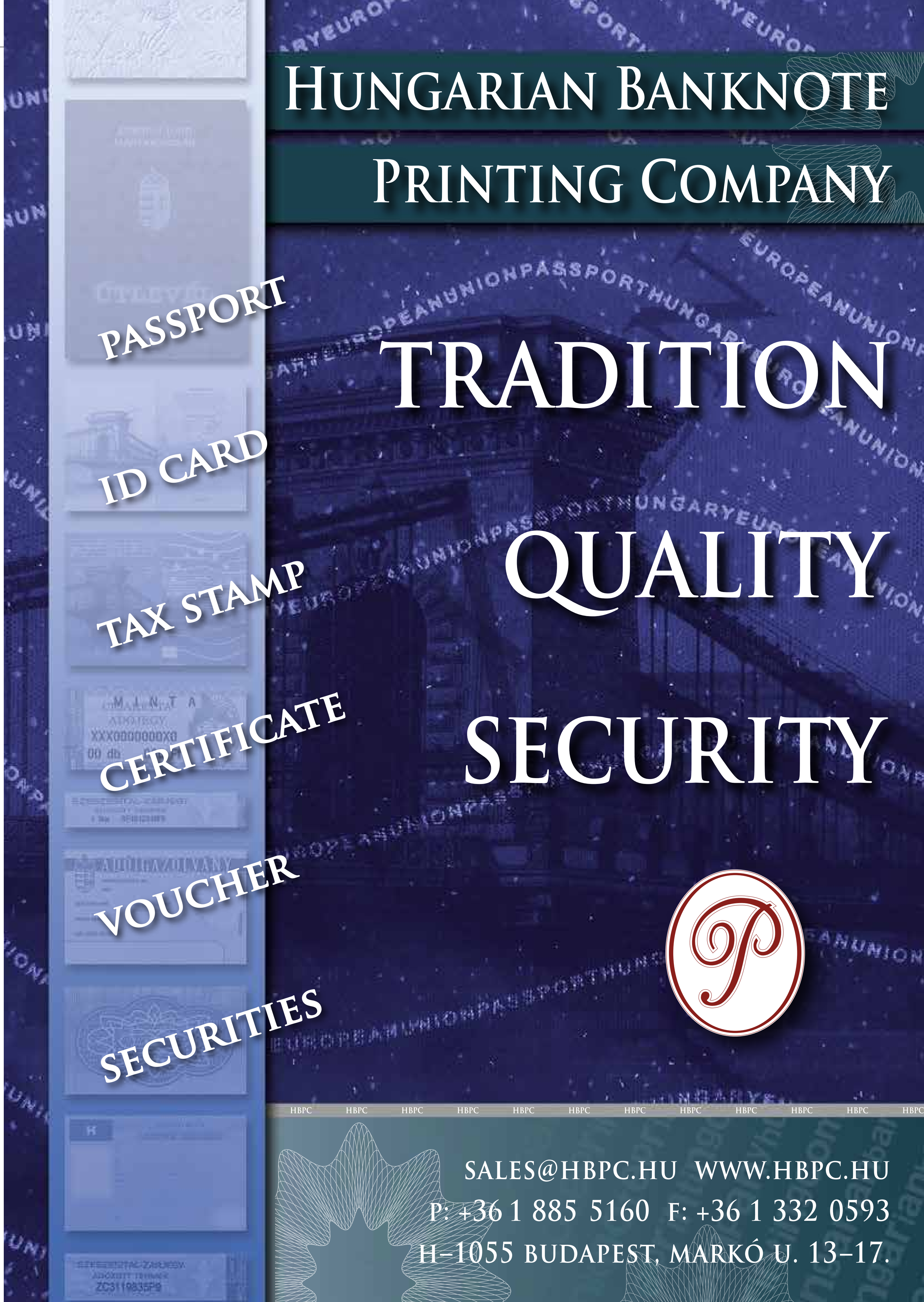
## Long-term planning reliability – the Trusted Computing Group (TCG) sets standards for industry and consumers

TPMs are based on the open standards of the Trusted Computing Group (TCG) and have already been used for many years in PCs and notebooks. New applications benefit from this experience of many years. In its certification program, the TCG documents all those TPM products that officially meet the standard and thereby provides better orientation in the market for all users. The standard furthermore presents additional benefits: the detailed specifications of the TCG improve the compatibility of the multitude of different operating systems and customer applications. Users can combine different solutions at any time in the design of the system architecture and thus they also have long-term planning reliability.

More and more networking, however, also raises the security requirements in other areas. The TCG already reacted early on to this development and designed the new TPM 2.0 Standard in such a way that a multitude of applications can be covered. Special attention has been given to security in embedded systems for everything from routers to automobiles and medical devices.

## Conclusion

In the Internet of Things, individual devices and components must no longer be viewed in isolation. A forged spare part or manipulated firmware updates on a production machine are sufficient to already cause damage to the entire production chain. By means of specific security chips, networked systems can be optimally protected to a vast extent. Meanwhile the fields of application are manifold: be it Industry 4.0, automotive connectivity, building automation, smart home or eHealth applications. Regardless if a clinic doctor is checking her patient's medication or a 3D printer producing a component, data security and system integrity are prerequisites for the success of the Internet of Things and the related products and services. ☒



# “*User* acceptance is the *biggest* CHALLENGE”

An Interview with Youzek Kurp, Gemalto

… at least when it comes to Mobile ID. When we met up with Youzek Kurp of Gemalto to talk about the market in Europe and beyond, the eIDAS framework as well as about the role of governments in the digital future, we found Gemalto well prepared for things to come. And because being one of the biggest players in the field is not enough, there is now even an Alliance with peers and governments to drive the market.

□ *What are your thoughts on the eIDAS regulation and do you think it will make a difference in regional eServices deployment?*

We warmly welcome the approval by the European Parliament of the proposal for regulation on electronic Identification and Trust Services for the EU market. The eIDAS regulation lays down a framework for mutual recognition of electronic identification and authentication and set rules for trust e-services as well as creates a legal framework for electronic signature.We think eIDAS will strengthen the EU single market by boosting trust and convenience in secure and seamless cross-border electronic transactions. This EU initiative is positive news for consumers and citizens as well as businesses and governments.

For consumers and citizens, it sets a legal framework which will allow secure cross-border transactions while ensuring citizen data privacy. For businesses and governments, on the other hand, it sets the foundation required to ensure deployment of e-services in an open and secure environment.

It is also good news for the digital security industry as eIDAS is driving the long awaited interoperability framework required to bridge the physical and digital world in the single EU market. We also expect this initiative will support smartcard and associated solutions market growth in Europe by helping deployment of secure electronic Identity programs as well as by accelerating deployment of e-government services to both citizens and enterprises.

> “ *For consumers and citizens, it sets a legal framework which will allow secure cross-border transactions while ensuring citizen data privacy.*

Through constant commitment towards interoperability and open standards, Gemalto is actively engaged in supporting and technically contributing to the eIDAS regulation implementation. For instance, Gemalto is active for quite a while now at working within Industry Associations (ACSIEL in France or EUROSMART in EU) as well as international standardization committee level to define a public eIDAS compliant secure & privacy enabled token specification.

*Do you see any threats to a positive market development in Europe?*

Indeed, Europe has become a mature market for eID and ePassports but still, there are a number of EU and neighboring countries that are planning the migration or the upgrade of their electronic Identity documents.

We see the eIDAS regulation, as well as the development of Mobile ID, as strong market enablers for public and private sector eServices deployment.

In terms of the ePassport, EU member states are currently engaged in the SAC migration which is contributing to the market growth and we expect that, once released, the ICAO LDS-2 standard will strongly stimulate market development and raise new opportunities both for secure documents upgrade and also for associated solutions such as Border Control.

As such, we think the fundamentals are there to ensure a sustainable market growth in the coming years, not only for secure identity documents deployment, but also for associated solutions and in particular in the field of document usage and verification infrastructure.

*Looking beyond Europe and towards emerging and developing countries, the speed of large-scale eID implementations is picking up speed. Do you see a future for multi-application schemes?*

Definitely! Emerging and developing countries are showing very strong potential for growth of digital identity. Many countries in Africa, Latin America or Asia are engaged in setting up or modernizing their identity management infrastructure and planning large scale electronic ID deployment. “Financial inclusion” is a way for governments to secure financial transactions with citizens, specifically targeting the unbanked population. We see it as “Financial and Social inclusion” which incorporates a variety of potential applications such as fuel or food subsidies distribution, pension or social grants payment or access to healthcare services. Governments are constantly working on reducing fraud and operational cost and there is indeed an obvious bridge to be made between the citizen identity and these new use cases. As such, multi-application but also multi-issuer schemes where eID could support additional government applications is becoming a market standard in most emerging and developing countries.

*On a more abstract level, what do see as the future role of the visible sovereign document? Isn’t it an outdated approach to securing data in a digital society?*

Not at all. I would even consider that the digitalization of society reinforces the need to secure citizen identity in the connected world. National citizen registries and sovereign documents are and will remain the foundation of a citizen’s identity.

The digital world is showing a strong need for this identity to be as secure as it is in the physical world. As such, we think sovereign documents will stay the 'breeder document' for required derived identities in the digital arena. In my opinion, there is no reason to oppose identity in the physical (secure document) and digital identity, which actually complement each other in different environments. The current challenge is more about making sure we provide the required technology to secure the digital identity relying on a sovereign document.

*How does Gemalto define Mobile ID and how does it fit into the Government sector strategy?*

One of the biggest challenges in the market is user acceptance. If the solution is too complex, the citizens may shy away from it. Using a mobile as a signing and authentication device is natural for almost all users and we can also see it as the most democratic method of all – available to anyone who has a mobile phone.

The emergence of Mobile ID is a good illustration of this MUST for governments to provide means to enhance security provision and to catch the opportunity to accelerate eServices adoption.

For governments, we offer solutions to bridge the physical and the mobile digital world relying on what we call Derived Identity.

Here the overall principle we believe in is to ensure strong citizen enrollment relying on its sovereign document to derive a mobile digital identity, which can be stored on either the SIM card or the Secure Element of the mobile device. NFC interface generalization is a good way to ease implementation of such schemes where the mobile user can utilize his sovereign document to derive a temporary mobile digital ID.

> “ *The Alliance plays a key role in sharing best practices and uncovering the new generation of eIdentity and eDocuments*

*The private sector – mobile network operators, handset manufacturers, corporations like Google and Facebook, all want to play in the same park when it comes to secure credentials. Do you see a threat to the role of the government as the primary protector of its citizens' identites?*

Indeed with the variety of needs and use cases arising, the secure credentials market is currently very stimulated with many different initiatives, both from the private and the public sector. Our view is that there will be multiple identity providers depending on targeted applications and eco-systems.

This will, for sure, reinforce the role and responsibility of governments to provide the required means for the digital business to grow, to offer new services to their citizens but also to ensure they protect their citizens' personal data and privacy.

Government will have a key role in deploying the required infrastructure and delivering the secure 'breeder document' for the citizens' online identity and this will bring with it new opportunities for the industry.

*Gemalto initiated the Secure Identity Alliance two years ago. What was the motivation behind the initial scope of the Secure Identity Alliance?*

The Secure Identity Alliance was indeed initiated in 2013 by Gemalto with Morpho and Oberthur Technologies. Other private actors such as 3M and and Trüb quickly joined the initiative with also Public Entities such as the Emirates Identity Authority and the BMI, Ministry of Interior of Germany.

The Alliance plays a key role in sharing best practices and uncovering the new generation of eIdentity and eDocument technologies crucial to building the trusted framework on which to drive the adoption of eGovernment initiatives. The Secure Identity Alliance is dedicated to supporting sustainable worldwide economic growth and prosperity through the development of trusted digital identities and the widespread adoption of secure eServices. It is unique in the sense that it brings together the global expertise of the public, private and non-government organizations to foster international collaboration on Digital ID challenges.

*What has the SIA achieved to date and what are the next milestones?*

Most of the Secure Identity Alliance output is publicly available through its web site www.secureidentityalliance.org. Among main SIA achievements, I would mention:

- The eServices Provision Tracker (eSPT), referencing online the key eID projects existing around the world and giving details on their substance, with for instance, detailed description of large scale and successful Government eService programs such as in Estonia or UAE.
- The eSecurity awareness mode (eSAM), online self assessment model for governments to evaluate in an anonymous manner their level of Security and Convenience on key processes such as: IT and Facility Security, Document design, Personalization and Issuance Solution, Application, …
- A survey published with the Boston Consulting Group on the key benefits that online services could bring to governments and their citizens in terms of convenience and savings (up to 50 billion Euros globally in 2020), with guidelines to implement successfully the eGovernment programs.
- A joint position paper, with the GSMA, on mobile identity and how to unlock the potential of the digital economy.

It is also worth mentioning a series of workshops on the eIDAS implementation best practices. These initiatives will of course be continued and enhanced while we will also be working at strengthening our partnership with the World Bank on the "ID4D", Identification for Development program which vision is "Making Everyone Count by Providing an Identity and Delivering Digital ID enabled Services to All". ☒

# ROLIC TECHNOLOGIES ESTABLISHES A JOINT VENTURE *in China*

□ Just a few weeks after the Free Trade Agreement between Switzerland and China was signed at the start of July 2014, the Swiss high-tech company Rolic Technologies from Allschwil launched Rolic Technologies (Shanghai) as a joint venture with the Chinese company CINIC Chemicals Shanghai. Based on Rolic's innovative technology, the company will produce customized formulations to be used in the manufacture of high-quality LCD displays. Eventually, the company will also manufacture other Rolic products. With this forward integration, Rolic has opened a new chapter in its young history. Its goal is to roll out Rolic technology even more quickly and meet customer needs more effectively. As the majority shareholder in the new company, Rolic has now taken the final step towards becoming a manufacturer of ready-to-use formulations for the global high-tech industry. The products manufactured by the new joint venture company Rolic Technologies (Shanghai) are developed at the headquarters in Switzerland. Also the key materials are produced in Switzerland, before being combined with local components in China to create the final products. "From both an economic and an environmental standpoint, this approach will bring significant advantages," says Norbert Münzel, CEO of Rolic Technologies Ltd. "In addition, thanks to our joint venture in China we will be able to provide local customers in the rapidly expanding display industry with a faster, more direct service on site." Münzel believes that the new Free Trade Agreement is very important for a company like Rolic, not least because the international copyright laws are clearly stated and recognized by both sides. "This serves as a binding obligation and strengthens mutual trust. If there is any infringement of these regulations, it is possible to introduce effective measures and sanctions," explains Münzel. For its joint venture with Rolic, CINIC is providing the infrastructure as well as resources and manufacturing experience. Kevin Wang, President of CINIC's Board of Directors, says, "I expect the joint venture to open up interesting new opportunities in the rapidly growing Chinese market, in particular a chance to expand business operations to the display industry and other high-tech applications." For Münzel, another key advantage for the Swiss partners is that CINIC has a management team that already has working experience in an international environment. "On the one hand, the staff are familiar with our standards and way of working. On the other, as a result of their backgrounds and language, they have very direct contact with local suppliers and customers on the ground," says Münzel. Rolic Technologies Ltd. has a 70-per-cent share in the new joint venture, Rolic Technologies (Shanghai). The local partner CINIC, which employs 500 staff, owns the other 30 per cent. ☒

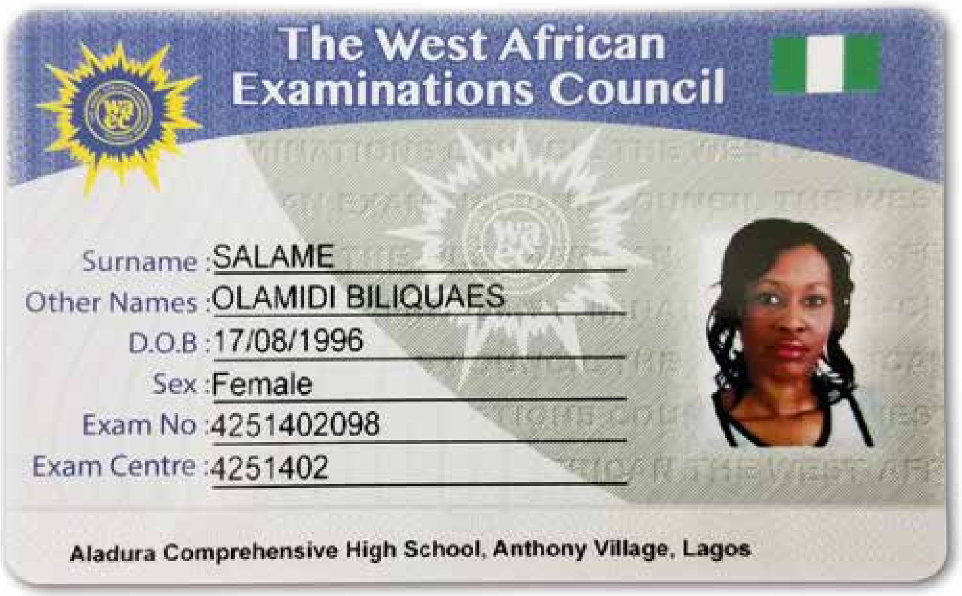
By Silicon Trust

Cultural identity is shared by all.
Our secure identities can be shared by no one.
nal Identity Card
GANIS
ADEM
10.04.1979
UTO
UTOPIA
18.06.2020
HID Global provides governments worldwide with highly secure, counterfeit-resistant ID solutions.
HID®

# Mobile ID *COMBATS Identity* Fraud

The vision of developing secure mobile ID applications has become reality, as demonstrated by emerging government, financial, education and civil secure ID programs. We are seeing a wide range of mobile solutions enter the market to fit the unique needs, budgets, and geographic requirements of ID programs worldwide.

By Rob Haslam, HID Global and Babatope M. Agbeyo, Botosoft



The West African Examinations Council

Surname : SALAME
Other Names : OLAMIDI BILIQUAES
D.O.B : 17/08/1996
Sex : Female
Exam No : 4251402098
Exam Centre : 4251402

Aladura Comprehensive High School, Anthony Village, Lagos

□ One such example is found in Nigeria where the West African Examinations Council has adopted a mobile ID system to combat the high instance of identity fraud and to improve the overall student validation process at the time of the exam. Now more than 2.2 million students register online and receive machine-readable HID Global smart cards every year.

## The West African Examinations Council

The West African Examinations Council (WAEC) is West Africa's foremost examining body. It was established in 1952 and today is comprised of five member countries – Nigeria, Gambia, Sierra Leone, Ghana, and Liberia. Services provided by the WAEC include:

- Conducting public examinations for primary and junior/senior secondary school levels
- Conducting aptitude tests for institutions and corporate bodies
- Issuing results and certificates of completion/passing on the examinations administered

Every year, WAEC registers more than 2.2 million students for annual exams conducted in more than 13,000 participating exam centers across Nigeria. With an admirable mission and high standards, WAEC soon realized that maintaining the integrity of the organization was going to require more than the basic security procedures to identify, authenticate and monitor students during the examinations process while at the same time providing a professional and comfortable testing environment.

## Cards + mobile devices = greater security and fraud protection

Increasingly, smart ID cards and mobile devices are working together seamlessly within a centralized identity management system. For WAEC this has resulted in greater security and protection against fraud.

Students now register online. The information is used to personalize and issue a machine-readable smart card to each student. This same information is stored in a central biometric database that can be accessed in real-time by the new mobile readers at the time of the exam. Today, more than 15,000 mobile readers have been distributed to over 3,500 exam centers throughout Nigeria allowing supervisors to identify and authenticate students at the time of the exam by accessing student information from the HID smart card and validating it against the central database in real-time.

Similarly, information about the testing process including, date, time and the name of the testing center is added to the student's online records. WAEC's vision to be a world-class examinations body and gain international recognition now inspires and challenges more than 2.2 million African students every year. To facilitate improvements in the annual examinations, WAEC teamed with BotoSoft and HID Global to develop an electronic Student ID card program that would address high volume issuance requirements and the need to improve the efficiency and accuracy of the annual exams.

## A historical perspective

Historically, WAEC's method for exam registration and authorizing has been manual, time consuming, and susceptible to fraud. Students registered online and were provided a paper receipt that was later manually validated at the time of testing without a secure process to confirm the student is who he or she says. For this reason tracking and recording cases of identity fraud has been difficult and suspect. While WAEC knew it needed to do something to remedy the situation, with so many exam centers spread throughout the country, building a more secure infrastructure from the ground up was not economically feasible.

To this end, WAEC turned to Botosoft, based in Lagos, Nigeria who commissioned HID Global to assist with the development and deployment of a secure card issuance and mobile ID system, which allowed WAEC to meet and exceed its security needs within budget.

## The solution: A mobile ID system

Online registration for an identity card, read using a mobile device at each examination site, was decided to be the most practical solution. These cards would be valid only for the examinations being held in a particular semester and expire immediately on completion of the final paper. Without a valid card, students would not be allowed to take their exams. With security, flexibility and quality at the forefront, WAEC required a secure issuance system that could print upwards of 1.8 million cards in the spring term and another 400,000 cards in the autumn term. Furthermore, the cards needed to be checked and authenticated at the examinations sites by local officials.

HID Global leveraged its Government ID expertise and offerings to deliver a customized solution to accept the raw data from WAEC's online enrollment process; validate the information and prepare it for use in personalizing the cards in the Botosoft facility. Once issued, Botosoft's Candidates Identity Verification, Attendance, Malpractice and Post-Examinations Management System (CIVAMPEMS) ensures effective administration of the "Exam Day" process.

## Innovative card and personalization technologies

The WAEC student ID card incorporates multiple technologies to facilitate the greatest security and protection against ID fraud possible. Beyond visual identification – the candidate whose name and photograph appear on the card must take the card to the appropriate exam center and present it to the Examinations Official upon request – multiple embedded technologies not visible to the naked eye have been incorporated. Specific features unique to the WAEC student ID card include an integrated contactless chip, a UV blue WAEC logo, guilloche graphics, micro-text, warped patterns with faded edges, Text relief and faded photo box edges overlapping with personalized photos

> *The WAEC student ID card incorporates multiple technologies to facilitate the greatest security and protection against ID fraud possible.*

To facilitate the rapid personalization and issuance of secure identification cards, HID Global provided a turnkey software and hardware solution including FARGO® DTC4500 and 4500 ID card printers / encoders deployed in under four months with a capacity of more than sixty five thousand cards per day. HID Global provided hands-on training and support to the Botosoft production team.

## Summary

Innovations in mobile ID technologies are beginning to emerge, allowing secure identification and authentication as well as instant access to critical information. Students are now issued a secure biometric RFID credential that is registered in a central WAEC biometric database. Supervisors at the examinations sites can authenticate students in real-time via a handheld reader that can access the central database. The results are reduced exam fraud, less paperwork and an increased value of the diploma. In addition, with the advancements made by HID Global, the next generation mobile reader could be a smart phone. Using smart phones as readers are expected to significantly reduce infrastructure costs. ☒

# “Veridos POOLS much *sought-after* *EXPERTISE*”

Interview with Hans Wolfgang Kunz and
Hermann Sterzinger, Veridos GmbH

Giesecke & Devrient and Bundesdruckerei, the two distinguished German specialists in secure government solutions, have come together to bundle their international ID business and launched the Veridos joint venture at the beginning of the year. In this interview, Hans Wolfgang Kunz and Hermann Sterzinger tell us what makes this company so unique.

□ *Veridos opened for business at the beginning of the year. How did this joint venture come about?*

[Hans Wolfgang Kunz] Veridos pools much sought-after expertise in high-security technologies for governments and state printing companies in a single company. This expertise is delivered by two globally recognized partners: Giesecke & Devrient and Bundesdruckerei. The joint venture will allow us to rapidly and substantially increase the parent companies’ share in international ID business. Veridos provides us with the critical mass needed to find the best possible position in global competition. It also allows us to boost our footprint. Together, we can leverage our international customer relationships, with each partner contributing its own experience and extensive technological know-how. This joint effort ultimately means that we are much more cost-efficient and this will benefit our customers too.

[Hermann Sterzinger] We also shouldn’t forget one very important aspect in the ID business niche: The former staff of G&D and Bundesdruckerei, who now work for Veridos, enjoy international respect and recognition for their particular skills. Our employees are highly motivated, they speak up to six languages, and are perfectly positioned to understand the specific needs of our customers. Our staff is a perfect blend of employees with extensive experience in the market and new employees.

> “ *Our staff is a perfect blend of employees with extensive experience in the market and new employees.*

*What does Veridos have to offer that the parent companies alone would not be able to offer?*

[Hans Wolfgang Kunz] The portfolio is much more extensive for customers, covering the entire value chain of secure identification. Another advantage is that we can offer bespoke solutions for the international market from a single source.

From our production sites, we can supply reliable, high-security products and, in urgent cases, we can offer our excellent Business Continuity solutions. Our customers benefit from combined technological expertise, fast distribution channels and a broader portfolio.

*Is Veridos the first step towards a general merger of both parent companies?*

[Hermann Sterzinger] Co-operation is restricted entirely to international business with ID solutions for governments. This does not include any of the other segments, i.e. business in Germany, banknote printing, as well as private sector business, which both companies will continue to run independently.

> *“I find it very exciting that although we may be independent we can in fact still shape our path together while relying on our common strengths.*

> *“Veridos customers benefit from combined technological expertise, fast distribution channels and a broad portfolio.*

*Dr. Hermann Sterzinger (COO)*

Dr. Sterzinger (born 1968) studied Mechanical Engineering in Munich. He also went on to obtain a degree in Economics and Labour. In 1997, he completed his doctoral thesis at the Department for Private and Patent Law at TUM in co-operation with Max Planck Institute. Dr. Sterzinger has been COO at Veridos since its start in 2015.
Prior to that, he had served as head of the Government Solutions Division at G&D since 2011.

*Hans Wolfgang Kunz (CEO)*

Mr. Kunz (born 1954) studied Economics in Munich. He has been CEO of Veridos since the start of the company in 2015. At the same time, Mr. Kunz has been a member of the management board of Giesecke & Devrient (since 1996).
At G&D, he has been in charge of the Government Solutions business unit since 2006.

VERIDOS
Identity Solutions
by Giesecke & Devrient
and Bundesdruckerei

**About Veridos GmbH**

- Veridos was established at the beginning of 2015 as a joint venture between Giesecke & Devrient GmbH and Bundesdruckerei GmbH and is headquartered in Berlin, Germany.
- Giesecke & Devrient holds 60 percent of the shares in the company and Bundesdruckerei 40 percent.
- The company offers identification and identity solutions.
- Veridos bundles the expertise of the two parent companies for international business, offering the entire value chain of secure identification.

For more information, go to: www.veridos.com.

*That’s a good point: How can the companies work together as partners and still compete with each other?*

[Hermann Sterzinger] This is not an unusual situation, e.g. in large corporations or in companies with several divisions. The partners complement each other rather than providing complete solutions as isolated partners. As differentiators, both parent companies think and act alike and are equally committed to quality and service. I find it very exciting that although we may be independent we can in fact still shape our path together while relying on our common strengths.

[Hans Wolfgang Kunz] Exactly. Take, for instance, the delivery of the Latvian driver’s license where we worked together or when we jointly won the tender for the electronic ID card in Kosovo.

*What exactly does Veridos offer?*

[Hermann Sterzinger] We offer both individual components and products for identification systems as well as one-stop solutions. The Veridos portfolio includes passports, ID cards, healthcare cards and driver’s licenses. We also produce systems for document issuance, personalization and documentation in addition to solutions for border control, voter registration and personal identification. In the case of passports, for instance, we cover the entire value chain, from paper right through to eGates.

[Hans Wolfgang Kunz] This means that whenever citizens disclose their identity, either in analog or digital format, they can trust in solutions from Veridos. It goes without saying that Veridos also benefits from the experience of its parent companies, for instance, the introduction of the German ID card which is considered to be the most secure solution on the market. We can hence offer our customers a unique product portfolio from a single source.

*Which regions will Veridos focus on?*

[Hans Wolfgang Kunz] Veridos supplies solutions for governments all over the world. Demand for secure and reliable solutions for the sovereign market has been steadily growing for some time now. The number of air passengers, for instance, increases by around five percent each year. Veridos supplies security solutions to meet these requirements, for example, electronic border control systems that make crossing borders faster and smoother for passengers.

*The future is digital and mobile. Is there any room left for paper documents?*

[Hermann Sterzinger] It’s true, digitization is set to spread further and will become even more important for our business. Mobile verification, for instance, is already proof of this. Take, for example, online authentication and authentication in the cloud where secure ID solutions will also be needed. That being said, we are convinced that sovereign documents will continue to exist in the future and will be simply supplemented by digital applications, e.g. by mobile devices, clouds and smart IDs.

*Now let’s look to the future: What changes do you see ahead for ID business?*

[Hans Wolfgang Kunz] We expect to see a lot of movement in the years to come. “Payment-on-eID” could be one example. Smart services could also gain a foothold. We believe that this will also include all types of eGovernment applications. In the ID sector, business models will shift more towards Build Operate Transfer (BOT) business and increasingly also towards Public Private Partnerships (PPP). Industrialized countries will see more qualitative growth, for instance, with new security features and product enhancements. Emerging economies, of course, are initially focused on the basic introduction of state-of-the-art documents like the electronic passport. In these regions, I am thinking of the numerous countries in central Africa, new technologies are also paving the way for new functionalities, such as the previously mentioned “Payment-on-eID” function.

*Finally, to something completely different: What does Veridos mean?*

[Hermann Sterzinger] Veridos stands for our company’s core business: The first three letters “VER” refer to verification. The next two letters “ID” stand for identity or identification and the final two letters “OS” mean overall services. ☒

*Veridos will be exhibiting at SDW in London, one of the most important events for solutions for secure identification. The company will be present on 10 and 11 June at booth J13. To find out more about the conference, go to: www.sdw2015.com.*

# *30 YEARS* KINEGRAM®: Bringing a *brilliant idea* to life

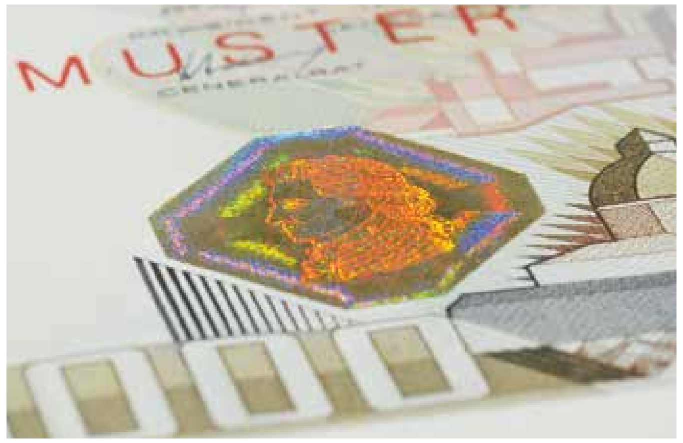
By Sonja Schöberl and René Schädler,
OVD Kinegram

There are many brilliant ideas that light up one particular sector of our lives, reach maturity quickly and then either become stagnant or are superseded by the next brilliant idea. For one idea and the physical representation it created, to remain fresh and relevant for thirty years and to have the potential of being continually further developed and refined for years to come, is something quite rare and remarkable. One of these rare ideas is the KINEGRAM, which changed the look of our banknotes and security documents from being rather dull pieces of paper or plastic to technological marvels, with moving colour changes, realistic rendering and fine details. The KINEGRAM is today one of the most prominent security features both in the banknote and the security document world – and one of the most hated features for any aspiring counterfeiter.

□The crucial word here is 'moving'. The distinguishing characteristic of the KINEGRAM is movement – kinein in Greek means to move – movement of light, colour or shine (reflectiveness) across a given design. The effect is the application of optical science, married to advanced foil technology. It was the work of the development teams at the Swiss company Landis & Gyr in Zug that turned the scientific discovery into a security feature that is "easy to communicate, easy to verify but difficult to copy or imitate".

## Colour copiers as existential threat

The first great awakening of the banknote and security document industries came when in the early eighties the first colour copiers appeared. Suddenly anyone could copy a banknote without any effort. Central banks were alarmed. Landis & Gyr reacted to their concerns by developing an optical feature in the form of a silvery patch that could be hot-stamped onto the paper substrate. The patch carried a design that showed movement when tilted. As the technology was totally new, Landis & Gyr had to develop not only the product itself, but the equipment to produce the first master and also that to manufacture the feature on an industrial scale. An optical feature of that kind also demands a physical support, a problem that was solved together with the German foil technology company Kurz. Although banknotes were the initiator of this development, it was a passport where the first KINEGRAM – as it became known in 1985 – was applied. In that year, Saudi Arabia was the first country that guaranteed the authenticity of its passport with a KINEGRAM PATCH and thus made history in the security document world.



*First KINEGRAM® application on a banknote: Austria 5000 Schilling*

*Continuous innovation for 20 years: KINEGRAM® PATCH on the EU Visa Sticker*

The first application of the feature on a banknote came a few years later, when Austria's national bank, the Oesterreichische Nationalbank (OeNB), decided to add a note of 5000 Schilling to its line-up of denominations. This new, high value note needed the best protection available and the OeNB suggested using the new optical feature from Landis & Gyr, a company OeNB had already used for banknote testing equipment. As the design of the 5000 Schilling banknote prominently featured a portrait of Wolfgang Amadeus Mozart, it was only logical to have Mozart's head on the octagonal, fully metallised patch.

In 1999, OVD Kinegram AG was acquired by the German foil technology company, Kurz Group in Fürth. This proved to be a very good fit, as OVD Kinegram and Kurz had cooperated for years in the development of carrier foils for the optical elements. Now the development of the optical features is done in Zug, as is the production of KINEGRAM features for security documents such as passports, ID cards and driving licenses, while the production of KINEGRAM security features for banknotes is carried out in Fürth.

## A new focus: ID and travel documents

Thirty years ago, most people who needed a visa to travel to another country received a rubber stamp in their passport. However, some countries wanted greater security. The nine member countries of the new Schengen group started to discuss the design of a common Schengen area visa sticker. As the purpose of the Schengen Agreement and later the Schengen Convention was to enable travel without border controls in the Schengen area, the necessary high degree of security was provided by the KINEGRAM PATCH, the Schengen countries agreed on.

The first version was a fully metallised silvery patch showing colour movement in the solid area and in the stars. The next version introduced a totally new idea: selective de-metallisation. Instead of being a solid area of aluminium deposit, which creates the silvery shine, the metal deposit had been removed in certain areas, leaving a pattern of fine metal lines.

## Creating an early masterwork

In 1997, the Deutsche Bundesbank, Germany's central bank, had a serious problem with counterfeit banknotes of the higher denominations. The bank approached Landis & Gyr for a strong, easily recognizable security feature that was exceedingly difficult to replicate. The banknote designer and the Kinegram development team came up with a solution for the 100 Deutsche Mark note that even today is considered one of the masterworks of the genre. It showed the outline form of a lyre – a historic Greek musical instrument – containing a complex number 100 and smaller line drawings of the lyre. Superimposed is half of a larger line drawing of the same lyre, with fine de-metallised lines, which link-up in perfect register with the continuing printed lines of the other half of the instrument. The solid shape is surrounded by de-metallised micro printing, repeating the value of the note. The feature was so successful that the DM 50 and DM 200 notes were upgraded with KINEGRAM elements as well.

*The masterpiece: Germany's 100 Deutsche Mark*

## Protecting identity

Protecting an ID document, such as a passport, presents different challenges to protecting a banknote. A KINEGRAM PATCH signifies that the document is genuine, but the personal information and the photograph still remain vulnerable. To protect the whole area of a data page or an ID card, OVD Kinegram created a number of solutions with transparent KINEGRAM elements. The KINEGRAM TKO – Transparent Kinegram Overlay – was first used for ID documents in Bulgaria and it is now one of the most widely used technologies to protect ID documents. TKO is an ultrathin film containing optically variable elements which can be laminated onto cards or passport data pages or sewn-in during passport production, making it suitable for centralized or decentralized issuance. The optically variable elements are fully transparent and can be lines or images, rainbow coloured or matt, changing to and from a variety of colours, or be seemingly three-dimensional and can even be transparent replicas of the main portrait photograph. The possibilities for designers are virtually endless.

*First KINEGRAM® TKO protecting the passport datapage: Bulgaria passport*

*KINEGRAM® PCI, the leading embedded security device: US Passport Card*

Embedding KINEGRAM elements into the card-body of polycarbonate cards or data pages presented another challenge. Such cards are made up from various layers and the thin foil of the KINEGRAM PCI – Plastic Card Inlay – is one of them. The card layers are fused together with the application of pressure and heat and subsequently the cards are personalized by a laser. OVD Kinegram had to develop the technology of making the inlay survive both heat and pressure and enable laser personalization, all of which presented formidable challenges for OVD Kinegram's engineers.

Today it is impossible to imagine the document market without polycarbonate substrates. The material has enormous potential and thanks to innovative ideas, it enables ever-higher security standards. The KINEGRAM technology was already married to polycarbonate in the 90s and today, as a polycarbonate pioneer, OVD Kingram is leading the integration of security elements in plastic materials.

*KINEGRAM ZERO.ZERO®, today's best-in-class partial metallization solution: Serbia car registration card*

*First KINEGRAM ZERO.ZERO® application on banknotes: Turkey Lira*

## The metal-on-demand solution KINEGRAM ZERO.ZERO®

In the new millennium, the demand for improved integration of the security foil into the document or banknote design led to probably the most significant innovation in the industry to date. KINEGRAM ZERO.ZERO gives the designer complete freedom in placing the metallised areas of a KINEGRAM security feature. Ultra thin metallised lines or lines brilliantly glowing and solid areas in any shape can be designed without limits and thus offer optimal integration into the document as a whole. The fact that brilliantly coloured lines can be created in absolute register – with zero tolerance – with the metal is an insurmountable hurdle for counterfeiters.

The honour of being the pioneering, first application of KINEGRAM ZERO.ZERO belongs to the 2009 series of the Turkish Lira. However, the Canadian banknote series of 2012 is probably the showpiece of what the technology is capable of. KINEGRAM ZERO.ZERO's triumph came with a new banknote using an unconventional substrate, polymer, but the feature is seen just as often on passports, ID cards or drivers' licenses all over the world. And it is not only a technological 'tour de force' but, with a good design, an aesthetic pleasure to look at as well.

## Continuing innovation to secure the future

Thanks to the integration of OVD Kinegram AG into the KURZ Group, the KINEGRAM was able to benefit from continual developments in foil technology, leading to new, innovative security features and intelligent material combinations. Thus, in 2014, the close cooperation between the two companies enabled the Israeli 50 Sheqel note, as the first banknote worldwide, to be secured with the new KINEGRAM VOLUME technology. KINEGRAM VOLUME is a registered, transparent stripe with unique, mono-coloured, diffractive images. Several important banknote projects using the same technology will shortly be introduced.

In the ID document field, one of the latest additions to OVD Kinegram's arsenal of security solutions for ID applications is KINEGRAM RFID. This is an antenna technology that uses the "metal-on-demand" process to deposit a copper track on both sides of a foil substrate to optimize the antenna inductance, capacitance and electrical resistance. The product offering includes complete passport covers containing the KINEGRAM RFID inlay as well as a hot-stamped customized foil design on the cover surface. Other products include thin polycarbonate inlays for passport data-pages and ID cards.

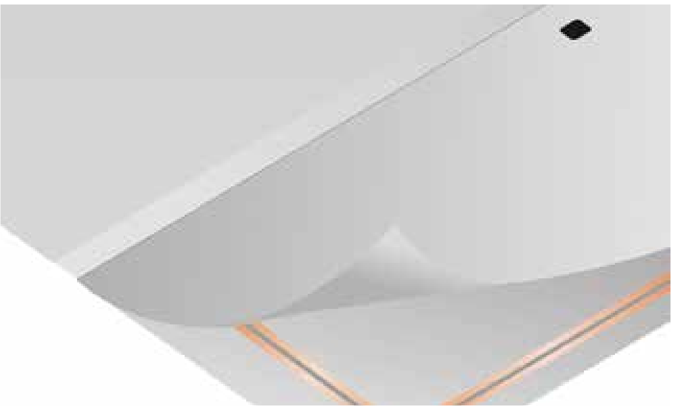
*First KINEGRAM® VOLUME application on banknotes: Israel 50 Sheqel*

## KINEGRAM® MOVE, the latest product innovation for Motor Vehicle inspection

With traffic growing at a tremendous pace worldwide, governments not only have to maintain and build new roads and highways, but control traffic flows, regulate parking, and ensure roadworthiness of vehicles. Industry provides many appropriate tools for this, but many solutions consist of or include documents, which can become targets of counterfeiters. At the request of its government customers, KINEGRAM developed a dedicated motor vehicle solution, KINEGRAM MOVE, which provides optimal security. The first country to use the new security solution for showing the roadworthiness of vehicles is Serbia. The KINEGRAM MOVE windshield label is a finished document which the vehicle inspection authorities personalize and affix behind the windshield, showing evidence to the police that the vehicle is in a fit state.

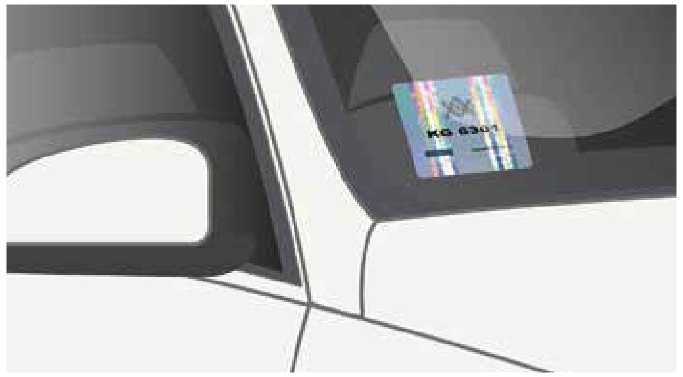
The journey of the KINEGRAM and of the company that created it, from the first silvery patch on a Saudi Arabian passport to today's technological pinnacle on the new Israeli Sheqel, has been remarkable. But the journey is far from over. The KINEGRAM technology and the development team behind the technology are ready to bring many further surprises, for the benefit of the security and the looks of banknote and ID and travel documents. ☒

*KINEGRAM® RFID passport inlay: the antenna technology made by the "metal-on-demand" process*

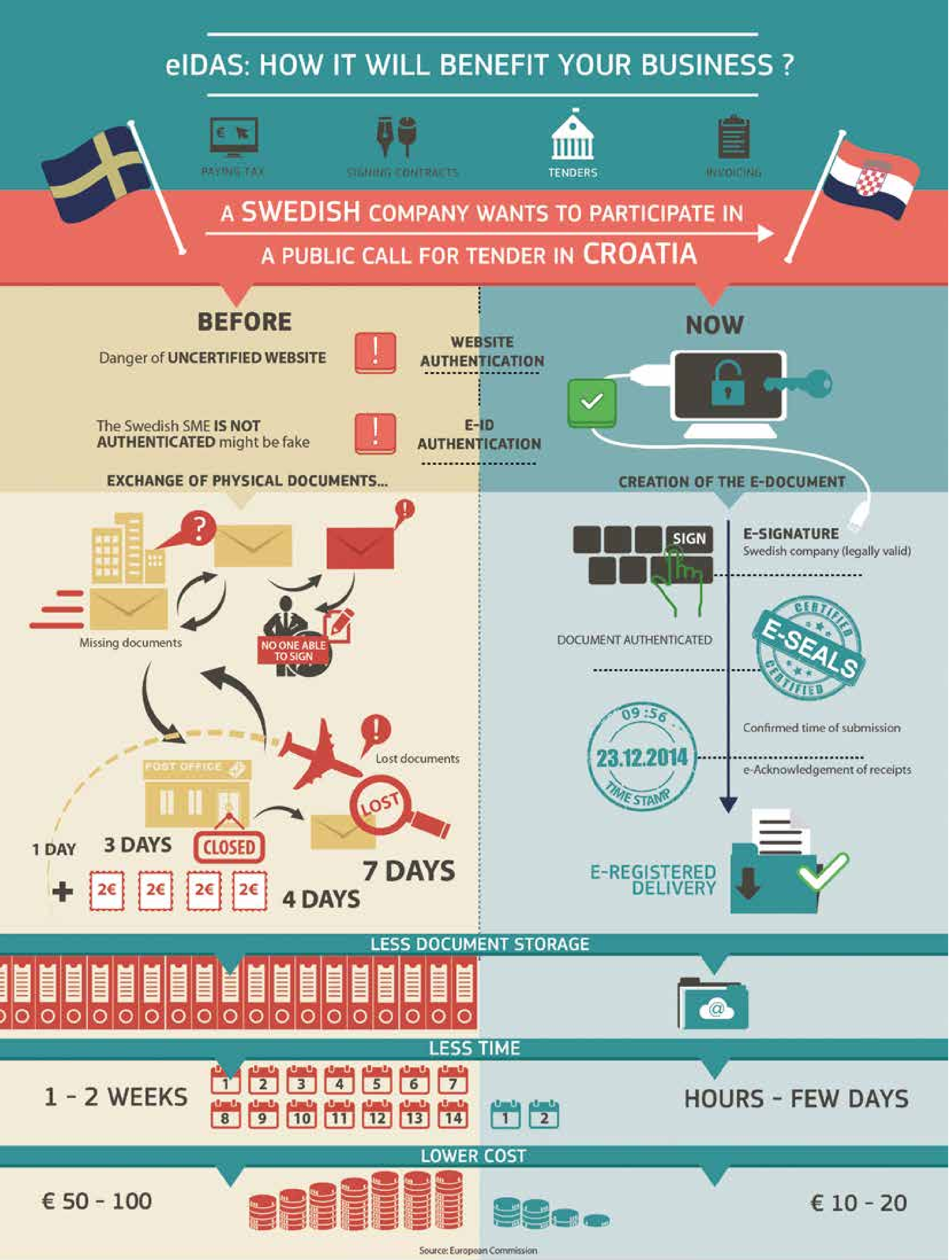


*KINEGRAM® RFID eCover*

*KINEGRAM® RFID eCover: Argentina Passport*



*The latest product innovation: KINEGRAM® MOVE, the motor vehicle certificate*



## eIDAS: HOW IT WILL BENEFIT YOUR BUSINESS ?

PAYING TAX · SIGNING CONTRACTS · TENDERS · INVOICING

A SWEDISH COMPANY WANTS TO PARTICIPATE IN A PUBLIC CALL FOR TENDER IN CROATIA

### BEFORE

Danger of UNCERTIFIED WEBSITE

The Swedish SME IS NOT AUTHENTICATED might be fake

EXCHANGE OF PHYSICAL DOCUMENTS...

Missing documents

NO ONE ABLE TO SIGN

Lost documents

LOST

POST OFFICE

CLOSED

1 DAY

3 DAYS

4 DAYS

7 DAYS

+ 2€ 2€ 2€ 2€

WEBSITE AUTHENTICATION

E-ID AUTHENTICATION

### NOW

CREATION OF THE E-DOCUMENT

SIGN

E-SIGNATURE
Swedish company (legally valid)

DOCUMENT AUTHENTICATED

CERTIFIED E-SEALS CERTIFIED

Confirmed time of submission

09:56 23.12.2014 TIME STAMP

e-Acknowledgement of receipts

E-REGISTERED DELIVERY

### LESS DOCUMENT STORAGE

### LESS TIME

1 - 2 WEEKS

1 2 3 4 5 6 7 8 9 10 11 12 13 14

1 2

HOURS - FEW DAYS

### LOWER COST

€ 50 - 100

€ 10 - 20

Source: European Commission

ec.europa.eu/digital-agenda/en/trust-services-and-eid

European Commission

# *The future* for employee ID CARDS looks *multi-functional*

By Dr. Dirk Woywod, Bundesdruckerei GmbH

High degree of data protection and informational self-determination for users: For centuries, people have wanted to know who exactly they are dealing with. Thanks to today's smart cards, this question can now be answered without a trace of doubt. At times of increasing industrial espionage, companies are well-advised to provide their staff with employee ID cards which, in tandem with suitable background systems, can guarantee that only authorised people enter the company and operate machines. Secure digital identities are the foundation for such solutions by Bundesdruckerei.

*Future employee ID cards could also feature a display and fingerprint sensor, as well as a camera and an input field.*

FULL ID | GOVERNANCE
MATCH OK
Intelligentes Workflow-Management
Sicheres Berechtigungs-management
Effizientes Compliance-Management
www.bundesdruckerei.de

*Go ID! – a smart, battery-free ID document with a fingerprint sensor and display. Sensitive biometric data is only captured there and is safely stored and verified on a chip.*

□ For centuries, people have wanted to know who they are dealing with. In the Middle Ages, paper documents usually served as a means of identification, for instance, a baptism or citizen's certificate, which were accredited by a church seal and signatures. But these documents were frequently forged. This paved the way for the development of ever-more secure identity documents, such as the ID card, which have become more complex, and in recent years, increasingly digitised. This development ultimately culminated in the use of smart cards as we know them today.

## What are secure identities?

We can use smart cards to identify or confirm the authenticity of an individual or an item. Identity describes the totality of all of the specific features that distinguish a person or object or makes them unique and unmistakeable. Identity is hence the foundation for individuality, uniqueness and trust.

Secure identity means that this identity cannot be manipulated, forged or fraudulently used. Secure identities are also a precondition for an individual's security. Strong, secure identities ensure the required trust and the protection needed in open, networked environments. After all, identity is the basis for the assumption of rights and the fulfilment of obligations in private, professional and public life. At the same time, secure identity also means that the principle of minimising data disclosure is observed: For each application, only those features that are needed at that point in time are read out and made available; for instance, when buying cigarettes, only the customer's age rather than their name or place of birth, is disclosed.

For decades now, smart cards have been making everyday business processes simpler, more reliable and more secure. In response to the demands that are being placed on these cards, they have now become all-rounders with a "mind" of their own. This is an important step, not just in order to guarantee security for identities and business processes, but also to increase application areas and boost user friendliness. That's why we are currently seeing a trend where smart cards are being developed to become smart devices.

## State-of-the-art smart cards as a system-on-document

"Go ID!" is the most advanced smart-card based employee ID card. Bundesdruckerei presented this new security concept at this year's CeBIT in March in Hanover. Go ID! is a smart ID document that comes in credit-card format and is based on the so-called system-on-document approach: The document is equipped with its own IT system, comprising various elements, such as a security chip and memory, an antenna for high-frequency power supply and for exchanging information, a fingerprint sensor and a display.

> *The document is equipped with its own IT system, comprising various elements, such as a security chip and memory, an antenna for high-frequency power supply and for exchanging information, a fingerprint sensor and a display.*

Template-on-document technology has been around and in use for some time now. One example of this concept is the electronic passport that allows reference data to be stored and issued on the document. Match-on-document was the next step here; in this case, reference data was compared directly on the document with the identity information captured at that point in time, for instance, the fingerprint data. The "downside" with these two technologies is that they always need an external sensor to capture biometric features, such as the fingerprint, facial image or voice. The challenge now is to integrate biometric sensors, a comparison algorithm, reference data storage and a display on a smart card and, ideally, not to need any separate power supply.

## New level of security and user-friendliness

In addition to be being very user-friendly, the new system-on-document approach has one major advantage: It offers an unprecedented level of security because all of the components are integrated into the smart card and the data is processed entirely on the secure card, i.e. from the capture of biometric data to storage on a chip, image processing, feature extraction and the comparison with the reference value, right down to doubt-free verification and display of the results.

> *This technology, which combines possession of the ID card and additional biometric detection of the fingerprint, offers outstanding security and also boosts user-friendliness.*

The fingerprint sensor integrated into the smart card solves the current password dilemma and secure two-factor authentication is guaranteed. All the ID card holder has to do is place his or her finger on the sensor. The fingerprint is checked in the document itself. This so-called verification-on-card concept offers a high degree of data protection and ensures the user's informational self-determination at all times. All that is then sent, for instance, to an external application such as a smart card reader, is the authentication result. This is sent in encrypted communication as "ok/not ok" information. No personal biometric data is sent to a background system. This technology, which combines possession of the ID card and additional biometric detection of the fingerprint, offers outstanding security and also boosts user-friendliness.

The integrated display, which provides status messages and information, also makes it easy to use the card. This ensures that the holder always knows which step is currently running and what he or she has to do next. Summing up, it can be said that Go ID! is very easy to use, it is fast and offers a high degree of security.

## Very complex technology

In addition to security, technical complexity is also increasing. The biometric sensor supplies fingerprint data; the integrated high-performance processor must store the information securely, process the images and extract and compare the data of the so-called minutiae of the fingerprint. That being said, the document also has to be robust enough for daily use.

That's why system-on-document technology poses huge challenges for its developers, for instance, when it comes to power consumption and processing performance. Battery power is not suitable for smart cards because batteries have a limited life, are difficult to integrate and must be repeatedly recharged. In order to warrant long life and comfort, the system-on-document should not need batteries and should work as a contactless smart card. The power needed is drawn from the electromagnetic field of the card reader and the card antenna.

The biggest challenge during the several years of development was how to integrate this complex technology into such a tiny space. In order to accommodate the different components, Go ID! is 2.5mm thick and only slightly thicker than a conventional credit card. It complies with the new ISO/IEC 18328 ICC-Managed Devices standard for a card type with a comprehensive

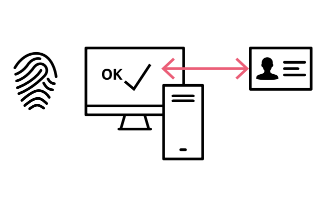
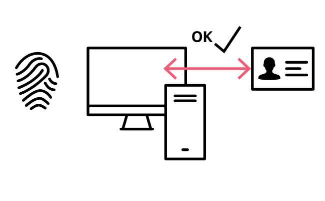
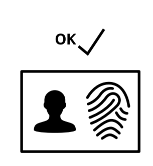
**FULL ID | GOVERNANCE PORTFOLIO FOR THE PRIVATE SECTOR**

– Go ID! can enhance legacy security systems. It is easy to integrate and the contactless readers already installed can continue to be used.

– The level of security can be adapted quickly and as needed by using ID documents with or without biometric components. While it may be sufficient, for instance, for an employee to simply hold the ID card before a reader in order to enter the employees' car park, an employee wishing to enter the server room can be required to additionally authenticate his or her identity with a fingerprint.

Go ID! comes with other electronic functions, such as:
- Secure login processes
- Data or e-mail encryption
- Electronic signature
- Release and payment processes

Go ID! is part of Bundesdruckerei's new Full ID | Governance portfolio that is specifically geared to medium-sized companies and organisations.

| BIOMETRICS | TEMPLATE ON DOCUMENT | | MATCH ON DOCUMENT | | SYSTEM ON DOCUMENT | |
|---|---|---|---|---|---|---|
| | External | In the document | External | In the document | External | In the document |
| Sensor and data capture | ✓ | | ✓ | | | ✓ |
| Comparison (matching algorithm) | ✓ | | | ✓ | | ✓ |
| Reference data storage | | ✓ | | ✓ | | ✓ |
| | – High interoperability demands<br>– e.g. passport | | – Reference data does not leave the document<br>– Greater privacy protection | | – Data captured and reference data do not leave the document<br>– Outstanding privacy protection | |
| |  | |  | |  | |

DOCUMENT COMPLEXITY AND SECURITY

*Comparison of the different technology systems*

chipset. This standard has been developed and will be issued soon. Bundesdruckerei was involved in the specification of the standard.

In recent decades, smart cards paved the way for standardising the shape of ID documents by combining credit-card format and photo ID along with electronic functionality. Smart cards in typical ID-1 credit card format continue to be handy and user-friendly. A few more millimetres in thickness will not change this. They also offer other advantages: Smart cards can be used as conventional photo ID while the card body, for instance, can be used by the issuing company as space for information and advertising. Even when it comes to more critical applications that require high-security authentication, an express declaration of intention or special data protection, smart cards are the means of choice for proving and confirming identity.

If we look further into the future, tomorrow's multi-functional documents will need new concepts for their shape, material and for producing the card body. In the years to come, the global mega trend towards individualisation is certain to be picked up in the field of identity. Smart cards, for instance, could be individualised not just with classical biographic and biometric data, but also with a portrait of the holder as a colour 3D relief. This too can further improve protection against manipulation and forgery.

It is also conceivable to include other components in the card body. Using an integrated camera, the facial image could be compared, while an integrated microphone would enable voice verification. A keypad field could also make it easier for the user to interact with the document. In other words, the cards of tomorrow will be even more multi-functional and user-friendly. ☒

**GO ID! INCLUDES:**

– a robust card body in a handy format
– a certified high-security chip
– manipulation-proof colour personalisation technology
– a display
– a fingerprint sensor
– several security certificates for encryption and signing

» The biometric data never leaves the document nor is it stored on the background system.

# SECURITY TRENDS in the Semiconductor *INDUSTRY*

By Daniela Previtali, Wibu-Systems

There are many aspects to security in automated manufacturing processes and even more so in today's connected factory environment. It is no longer simply a matter of securing the perimeter with access control systems and defining and provisioning rights for different network users' groups. As systems become interconnected, security involves new factors that include the protection of code integrity from tampering, the protection of software from piracy and reverse engineering, and the protection of product and customers' data from depredation.

> *“A multi-chip device is only as good as its weakest link, so it is crucial to track each chip placement to avoid placing expensive chips alongside failed chips. Without a high-quality, fully automated process, end product wastage and risk can be incalculable.*

□ No industry sector is immune to the inception of Industry 4.0: life science, automotive, automation, and even the utilities are about to experience the opportunities and challenges of remotely operated, controlled and maintained technology. As the future unfolds, many companies are optimizing their processes, and strengthening their positioning in the market through the vigilant protection of their intellectual property and the diversification of their business models.

KINESYS Software is a good example of how manufacturing performance should grow hand in hand with the implementation of security measures in order to ensure long-term business stability and profitability. Founded in 1992 in the Netherlands, KINESYS is a global leader focused on the automation of semiconductor manufacturing “back-end” processes. Their flagship Assembly Line Production Supervisor (ALPS) has grown to be the market leading solution for enterprise-wide substrate mapping and device tracking during semiconductor manufacturing. ALPS features mapping for all types of substrates (wafers, strips, trays, etc.), as well as tracking of devices through the multiple processes used in semiconductor assembly and encapsulation. Both Integrated Device Manufacturers (IDM) and Original Equipment Manufacturers (OEM) in more than 1,400 installations around the world use KINESYS' software for advanced wafer and device traceability and process management.

As semiconductor manufacturing rapidly evolved in Silicon Valley in the early 1990's, KINESYS Founder and CEO, Dave Huntley, focused his efforts on back-end processing and testing of individual chips on the wafer. In the past, this was performed unit-by-unit, applying ink on wafers to optically detect defective copies. However, optical recognition was slow and costly, and with the ever-increasing density of the circuits, ink pollution became unacceptable. His solution was to use a BIN code for each element on a wafer and store wafer map files on a hard disk. Thus, he could capture information about the product and the production process and store it in a database.

Another challenge he faced was that testing and assembly could take place in separate factory locations around the world with various types of machines using proprietary data formats. He addressed this issue by adapting the software to a common format to send messages between test and assembly and then to production machines. This readable data process is much faster than optical recognition and is environmentally friendly. The semiconductor industry organization SEMI helped by creating industry standards, allowing Huntley to build on his pioneering work to standardize for all types of substrates (wafers, strips and trays).

Over the years, KINESYS continued to adapt its software and licensing models to the ever-evolving semiconductor manufacturing industry as companies introduced new automation processes and techniques to improve quality and throughput while reducing waste. Multiple chips were often packaged into a variety of devices used increasingly in markets sectors where a chip defect could cost lives, such as medical, aerospace, and automotive systems. Devices became lighter, smaller, and thinner, making semiconductor assembly in large volumes a highly sophisticated industry. Today, the testing and tracing of individual chips is a critical process.

“A multi-chip device is only as good as its weakest link, so it is crucial to track each chip placement to avoid placing expensive chips alongside failed chips. Without a high-quality, fully automated process, end product wastage and risk can be incalculable,” Huntley said.

As the industry became more sophisticated, so did KINESYS' mapping and database technology. Huntley knew that he needed a mechanism to secure the invaluable manufacturing data he was capturing and storing, and protect it against tampering or cyberattacks. At the same time, he also needed a new level of licensing flexibility to adapt to the rapidly changing industry needs.

KINESYS partnered with security technology leader Wibu-Systems and qualified its CodeMeter® platform as the best of breed for data protection, licensing, and security against piracy, reverse engineering, tampering, and cyberattacks. With CodeMeter, KINESYS is able to protect its revenue stream while leaving the door open to more sophisticated licensing models, in line with the constant evolution of chip designs and manufacturing techniques.

A CodeMeter USB Stick (CmStick) is delivered with each installation. The CmStick has an embedded smart card chip where the KINESYS software encryption key and license information is securely stored. The dongle form factor (USB Stick) offers the strongest security against any hacking attempt, and is non-invasive, as it just needs to be present for the system to run without additional intervention from the user.

In addition to providing a foolproof integrated licensing solution, CodeMeter blocks unauthorized use of KINESYS software. Software security is a requisite, but it should not be an inconvenience in everyday use in a manufacturing production control environment. The balance between functionality and quality is always a delicate one.

Moreover, thanks to the collaboration with Wibu-Systems, KINESYS has the opportunity to future-proof their product in line with more flexible licensing models linked to SEMI standards and manufacturers evolving production needs.

> *Software security is a requisite, but it should not be an inconvenience in everyday use in a manufacturing production control environment. The balance between functionality and quality is always a delicate one.*

CodeMeter also provides KINESYS with an accurate accounting of the use of its software, thus helping them to fully monetize their product. In their current license model, customers pay a license fee for each individual piece of production equipment to which the software connects. However, they fully expect other licensing schemes to come into play, such as licensing based on data volume or for subscription license models, as customer's progress to a higher level of product cost accountability.

It is now common for the cost of the software and the equipment to be attributable to the total capital expenditures of a microchip factory. The equipment-connect license fits well with this cost accounting model but KINESYS expects the flexibility to deploy other license models will allow them to evolve in line with the customer's appreciation of more cost-accountable manufacturing techniques. ☒

# Cryptovision *goes* AMERICA

An Interview with Brian Kowal, cryptovision US

The VAULT met up with cryptovision's man in the US, Mr. Brian A. Kowal. Brian himself is no stranger to the Silicon Trust. He has a longstanding career in the high tech industry. Before joining German PKI and smart card specialist cryptovision, Brian was responsible for global Java Card licensing at SUN Microsystems/Oracle – consisting of over 50 licensees distributing over 2 billion Java Card units/year. Last year, he joined German security vendor cryptovision. He is based in California.

□ *Mr. Kowal, what is your vision for cryptovision in the US?*

Well, we differentiate between Latin America and the US. Many of the countries in Latin America are moving to smart cards for national IDs, secure travel documents, ePassports, drivers licenses, voters cards and entitlement cards for women and children. Some of the countries have poor past experiences and lost millions of dollars acquiring proprietary and/or "turn-key" solutions; only to learn that these products resulted in high long-term hidden costs and poor ongoing support. The outcome of this is that these countries are now replacing their proprietary systems with smaller best-of-breed component companies. Key benefit of this new strategy is that companies such as cryptovision offer localized training and consequently empower the local government and enable long-term sustainability.

In the US we are targeting different markets, such as EMV and government ID. EMV is hot right now with the associated credit card companies' mandates to migrate to EMV by 2015/2016. The government ID programs, which are focused on government employee IDs as opposed to citizen IDs, are close to 100% deployment, and thus there is a perceived slow down in this market.

With respect to EMV, there is an interesting ripple throughout other industry verticals that associate the EMV mandate as a smart card mandate for their particular industry. For example, many folks that recently attended the HIMSS 2015 health conference (the largest Health IT show in the world), had the misperception that there was a 2015 mandate for health care ID smart cards in the US, too. This is not the case, but the byproduct is that recognition of smart cards is growing.

My vision of cryptovision in the US is to bring what cryptovision has learned, related to secure e-Documents in 22+ country national ID projects and to apply it to Government employee ID cards as well as to verticals such as education and health care. Government and enterprise smart cards in the US have mostly been focused on authentication and PKI. Outside of the US, national IDs have added standardized secure e-Document functionality to these cards. Cryptovision's applet suite and associated PC and mobile software is a natural bridge integrating both authentication and trusted secure ID e-documents to a single platform.

*What can CV bring to the US market?*

There are numerous solutions that cryptovision can bring to the US market. We have a PKI server solution that can easily be integrated as an appliance, or a "white-lable" plug-in into Enterprise IDM systems or other workflow cloud services. The PKI market still has much life and continues to grow as certificates are evolving for use within network devices, servers and cloud services.

With respect to smart cards, cryptovision will bring new functionality to the US market over the traditional PKI and authentication historic products. The addition of standardized secure e-Document applications, together with PC and mobile apps to access this content, delivers an ID card solution that goes beyond just authentication. ID fraud is a multi-billion dollar problem in the US in various markets. Cryptovision, together with market vertical partners will address ID fraud, leveraging these secure e-document cards.

*Which applications will you be targeting in the next 24 months?*

Cryptovision has some solid PKI server customers in the US that we will be focused on extending their functionality, as well as ensuring that the customers have been delivered solutions that delivers on the sold promises. These lighthouse accounts are foundational and will open doors for driving more PKI deployments. We are also looking to extend our relationships with US-based smart card VAR partners with respect to the cryptovision applet suite and PC/mobile client middleware. These VARs have traditionally been involved in PKI/Authentication enterprise solutions. Cryptovision sees strong potential in addressing ID fraud and has targeted some solution partners that exhibit strong potential. As this evolves, more information will become public.

*Mr. Kowal, you have previously worked for large corporations – what does it feel like to be in a position to build a market presence for a European player?*

All large companies are structured differently, but I will share my experiences having worked for NASA, SUN Microsystems and Oracle. In all of these large organizations, my local team was always fairly small. At the largest, the Java Business Team consisted of about 40 people. This was broken down further as I led the Java Card team, which in total including engineers, sales, product, R&D was never much larger than 20 people. Thus, on a daily basis, the teams were small, focused yet often resource constrained. For larger decisions or requests for budget items, it was necessary to build a justification, which would be delivered to one's immediate manager. This justification would then "disappear" as it traversed up the chain of command, and in Oracle's case usually land at Larry Ellison's or Safra Catz's desk. The end result was that only small progress was achieved regardless of the local team. If the Java Card team, as a standalone entity, could have been spun-out from this bureaucracy, the skill and talent of the team was immense and could have taken the product much further. Working for these large players did have one positive side effect: The name of these organizations immediately opened doors and everyone was always trying to find a way to work with you.

Working for a small European company and establishing its presence has been more exciting than working for the larger corporations. There are some conditions to this statement though, in that the parent European company needs to allow some latitude and flexibility for their US-based staff to run business as a US entity. So it requires compromise. On the plus side, one nice by-product of cryptovision's German-foundation, is that the reputation of German engineering and "by-the-book" rule following extends nicely. Though cryptovision is not yet a recognized name in the US, the company's German roots give it a foundation of respectability that is nice to build off of. As a security company, this also plays well in light of the Snowden NSA exposure where US-based companies have a shadow following them of potential NSA back doors being engineered into their product.

*Thank you very much for your time.* ☒

# WHO will be *first to* MOBILIZE your ID?

Summary of the Silicon Trust Mobile ID Forum, London, April 2015.

By Veronica Atkins, Silicon Trust

□ In April 2015, the Silicon Trust Program organized an expert forum on the topic of Mobile ID and related services. The year 2015 marks the 15th anniversary of the Silicon Trust Program which started the millennium by educating the technology industry and governments throughout the world on the use of silicon-based security and biometrics. Fifteen years on and the world has changed remarkably. Secure Identification in the digital and hyper-connected world – and the technologies associated with ID security – is no longer just the domain of the public sector. Mobile handset manufacturers (OEMs), for example, invested in biometric technology to secure mobile access. The payment sector has made a massive progress and success of using contactless technologies in many parts of the world, with a reader infrastructure that is now ready to take on mobile usage. So where does that leave governments? What role does the private and the public sector play when it comes to ID and the security and commercialization of personal attributes and/or credentials? At the 2015 Mobile ID Forum, the Silicon Trust invited international stakeholders across the value chain to present their visions, solutions and technologies.

## Views from the top: European Commission, Visa, GSMA and FIDO

The Forum kicked off with a keynote from Andrea Servida, Head of the eIDAS Task Force at the European Commission. The presentation on the EU policy on electronic identification and trust services stressed the relevance of the eIDAS Regulation to strengthen the EU Single Market and the Digital Agenda of the EC by boosting trust and convenience in secure and seamless cross-border electronic transactions.

Representing the payment industry, Visa Europe's Can Bayindir stressed in his presentation that consumers will ultimately drive adoption and that success will be built on existing infrastructures. This, as pointed out by the session's expert moderator Marc Sel, PwC Brussels, puts Visa in a good position to tackle the topic of how to ID and enroll existing customers on new channels and how to use their digital ID across multiple channels.

The GSMA joined the Silicon Trust Forum with an introduction to the MNO's answer to the topic of Mobile ID: Mobile Connect. In her presentation, Claire Maslen identified online privacy and security as the biggest threat to sustainable digital growth. The reliance on username and password, she told the audience, leads to abandoned log-ins and shopping carts, online fraud and, as a consequence, high data costs. The solution, called Mobile Connect, is a two-factor authentication approach, using the inherent security of the mobile device thanks to secure embedded hardware and a PIN.

But payment providers and MNOs are not the only ones that have a plan when it comes to the authentication of users in a secure manner. The FIDO Alliance has rapidly expanded since it was formed in the summer of 2012 as an industry program, with PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon, and Agnitio as the founding companies. Dr. Kim Nguyen, Managing Director of the German trust center D-Trust, spoke at the Mobile ID Forum about adding identification to authentication and the usage of certificates on a FIDO token. He stressed that typically, there is no interaction between the world of authentication and identification. Authentication systems are typically proprietary, relying on usernames/passwords, AppleID or tokens whereas governmental eID identification solutions are set up on the basis of a officially verified ID. With the FIDO standard, these two worlds can be bridged, bringing advantages for users and relying parties.

## Mobile ID – all you need is an app?

Next up were two examples of national business cases – based on very different technologies. Anne Marie Pellerin presented the rather successful US Mobile Passport solution by Airside Mobile. Ms. Pellerin, a security expert with past employers such as the Department of Homeland Security and the U.S. Transportation Security

Administration, generated a lot of interest with her use case of using the mobile through an app as a digital credential for a border control process in the US. The app is a pointer system to a central database and the traveler can be identified without a passport.

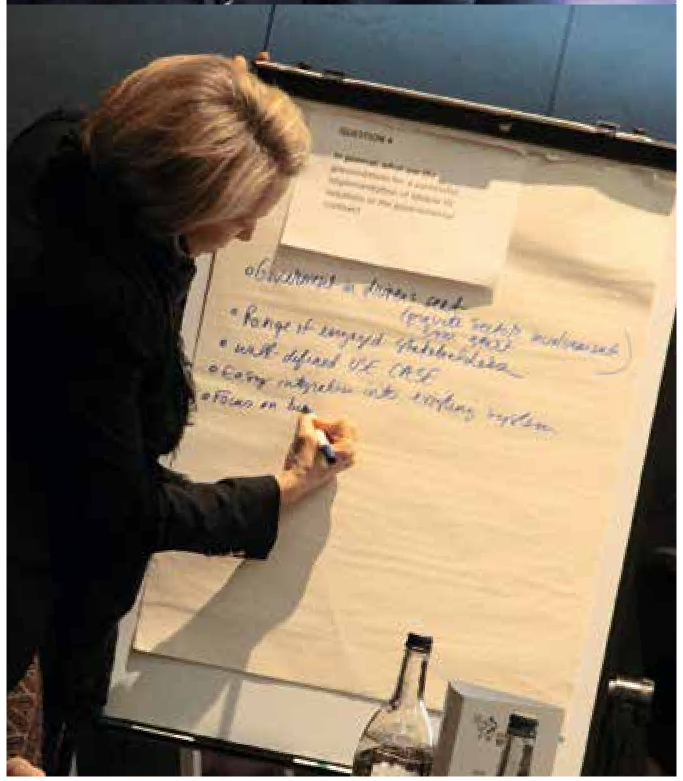
As a nice transition to country presentations in the second session, Dr. Detlef Hühnlein, Head of the German publicly funded SkIDentity project, pointed out that most European countries have some form of national ID, yet only two Member States make use of the existing infrastructure to implement a Mobile ID solution. Hühnlein put forward the idea of a generic eID Mobilizer and introduced to the delegates the concept of the award-winning SkIDentity concept, which enables eID and Strong Authentication in the (trusted) cloud and proposes a Mobile eID as a Service approach.

## Germany, Austria and Estonia exchange ideas on Mobile ID

The International Mobile ID implementation session, moderated by Gemalto's Eric Billiardt, focused on three countries: Germany, Austria and Estonia. Germany, represented by the Ministry of the Interior's Achim Hildebrandt, was quite frank – and humorous – about the convenient amnesia of the private sector on the debate about developing useful applications for the German National ID card. Back in the early 2000s, he told the audience, the big roundtable, made up of industry representatives across the board, was full of promises of the wonderful use cases for a secure eID token, such as a contactless ID card. Now that the card is rolled out to over 40 Mio citizens, with an optional eID functionality, all paid for by the state, nobody remembers that enthusiasm, stated Hildebrandt in his presentation.

Neighboring country Austria sent Herbert Leitold of the A-SIT Secure Information Technology Center, to take the delegates through the Austrian system, which has successfully rolled-out eID cards (named eCard) as well as Mobile eID with the Secure Element "in the Cloud". Interestingly, according to Leitold, Austrian citizens clearly prefer the mobile option with activation being 15 times higher than, for example, activation of the health smart card. For Austria, the next steps forward are how to make best use of the new smartphone generations in terms of device binding and support. Estonia, of course, is the poster boy for innovative eID usage in Europe. Of 1.3 Mio Estonians, there are more than 550000 active ID-card users and more than 48000 mobile-ID users.

The Estonian mobile ID solution, Tarvi Martens of the SK Trust Centre explained, needs no special software combined with a special SIM-Card and works on any handset. The fact that more than 300 services use the Mobile-ID offer explains the high usage. So, is there still room for innovation? Yes, according to Martens, the next step for Estonia is to introduce a Digi-ID with NFC. The Digi-ID card would work as an ID-card but also with an NFC-enabled phone and would also be available to e-Residency holders.



The 2015 Mobile ID Forum concluded with informal "unconference" sessions, where delegates grouped together to work on specific questions around the topic of Mobile ID. In the breaks and during the Networking Lunch, all speakers and attendants engaged in lively discussions. No doubt, the market will move fast in the next 12 months when, once again, the Silicon Trust will invite its network to meet and discuss. ☒

# SILICON TRUST DIRECTORY 2015

## 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 BOARD

The Executive Board has been the steering committee of the Silicon Trust since 2008. Jointly, the three companies drive 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 2014 fiscal year (ending September 30), the company reported sales of Euro 4.3 billion with about 29,800 employees worldwide. In January 2015, Infineon acquired US-based International Rectifier Corporation, a leading provider of power management technology, with revenues of USD 1.1 billion (fiscal year 2014 ending June 29) and approximately 4,200 employees. 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**

### VERIDOS

VERIDOS
Identity Solutions
by Giesecke & Devrient and Bundesdruckerei

Veridos GmbH creates secure and pioneering identification and identity solutions. Founded in January 2015, the joint venture between Giesecke & Devrient GmbH, Munich, and Bundesdruckerei GmbH, Berlin, pools the specialist expertise, the many years of experience, and the innovative power of the two largest German providers for high-security technologies to serve the international market.

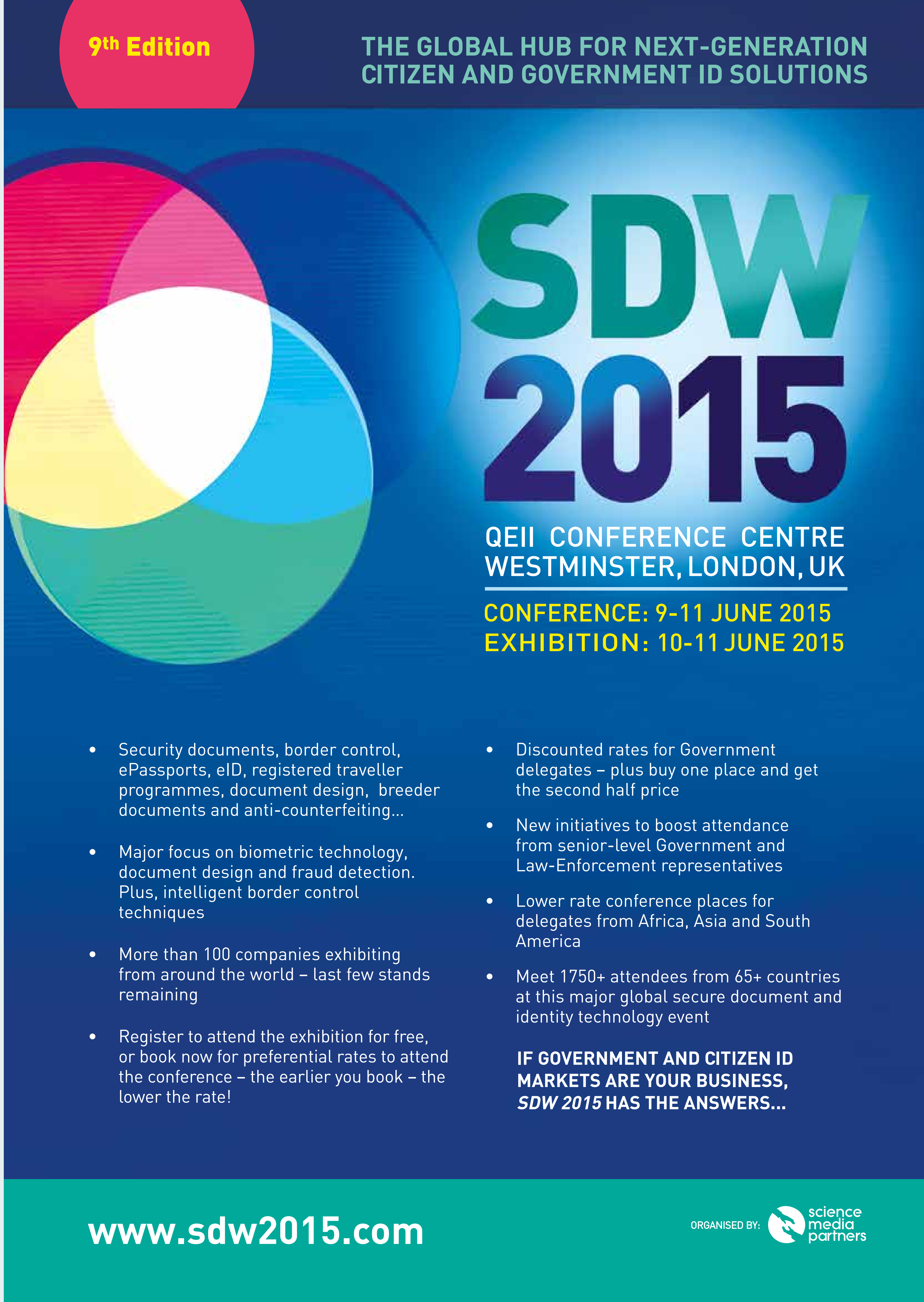
Veridos offers its customers a unique product portfolio from a single source. For instance, it covers the entire value chain for passports, from paper right through to eGates. The German company is a reliable partner valued by governments and public authorities throughout the world. In addition to its headquarters in Berlin and the operating facility in Munich, Veridos is represented around the world including in Brazil, Canada, Mexico, Singapore, the USA, and the United Arab Emirates.

**www.veridos.com.**

### GEMALTO

Gemalto is the world leader in digital security, with 2014 annual revenues of €2.5 billion and blue-chip customers in over 180 countries. 14,000 employees operate out of 99 offices, 34 personalization and data centers, and 24 research and software development centers located in 46 countries. The company helps governments, national printers and integrators design and roll-out secure documents and robust digital identity solutions. Beyond the traditional enrollment, personalization and issuance services, its eGovernment infrastructure and innovative applications will help win citizen's acceptance and boost usage. Gemalto is active in over 80 government programs worldwide.

**www.gemalto.com**



## ADVISORY BOARD

**The Silicon Trust Advisory Board supports the Executive Board 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.**

### 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**

### 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**

### 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**

### 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 HIDTM, 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 protected. 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**

MICROPROSS

Micropross is a leading company in the supply of test and personalization tools for the smartcard industry. Micropross technology covers the whole spectrum of the smartcard industry: they supply protocol analyzers, terminal simulators, smartcard simulators, for both contact and contactless technologies. Depending on the customer requirements, the company supplies turnkey solutions, including hardware and automated test cases (for both analog and digital test plans).
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

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 multi-applications OS, used in more than 40 eID projects worldwide.
www.masktech.de

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 protection 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

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

SID-CONSULT

SID-Consult GmbH works as an independent security consultancy. Dipl.-Ing. Heinz B. Artmann has more than twenty years experience in security printing and smart card technologies and more than forty years experience in the graphic arts industry. The top business domains of SID-Consult are MRTDs i.e. passport and ePassports, Visa and eVisa, national ID and eID, residence permit, driver license, voting cards etc. The areas of their expertise are prepress, printing, finishing, personalization, implementation, inspection, stress tests and border control.
www.sid-consult.de

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**

## TRÜB AG

Trüb, a Gemalto company, is a national and international leader in the production and personalization of secure and high quality identity solutions. Founded in 1859, the company is one of the premier supplier of national identity documents such as identity cards, passports and driving licenses, as well as EMV compliant bank cards, customer loyalty cards and solutions for logical and physical access. Among the governmental clientele of Trüb are Switzerland, Azerbaijan, the Czech Republic, Estonia, Hong Kong and Malaysia. In the financial sector, its clients in Switzerland include UBS, Raiffeisen, Cornèr Bank, PostFinance and many others, as well as more than 40 banks in around 20 countries worldwide. Trüb is part of the Gemalto group, the world leader in digital security with 2014 revenues of €2.5 billion and 14,000 employees worldwide.

**www.trueb.ch**

## 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**

## 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 is a leading system integrator and MultiPerso software developer, delivering security solutions to businesses across a wide range of industry sectors, such as financial, government, healthcare, retail, and public. The company's portfolio supports all activities required for eID and payment card issuance, passport production and management, cryptographic infrastructure development, authentication solution integration, and other activities related to payment security and smart card technologies.

**www.x-infotech.com**

ROLIC technologies

# NEW SECURITY HORIZONS

## BANKNOTE AND IDENTITY SECURITY SOLUTIONS

**Rolic Technologies Ltd.**
Gewerbestrasse 18
CH-4123 Allschwil
Switzerland

P +41 61 487 22 66
F +41 61 487 22 99
sales-security@rolic.ch
www.rolic.com/security

Innovation for Success