NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2015 | #17

The VAULT

Identity management *goes global*

APPLICATIONS

Modern Border Management challenges | LDS2 – Key to mobile travel documents?

INTERNATIONAL

People, Birth and Legal Identity
The Angola National ID program

TECHNOLOGY

The 4 prime elements of an eID project | Industry 4.0: Wibu-Systems and Infineon get serious

Contents

Imprint

THE VAULT
Published bi-annually by Krowne Communications GmbH, Berlin.

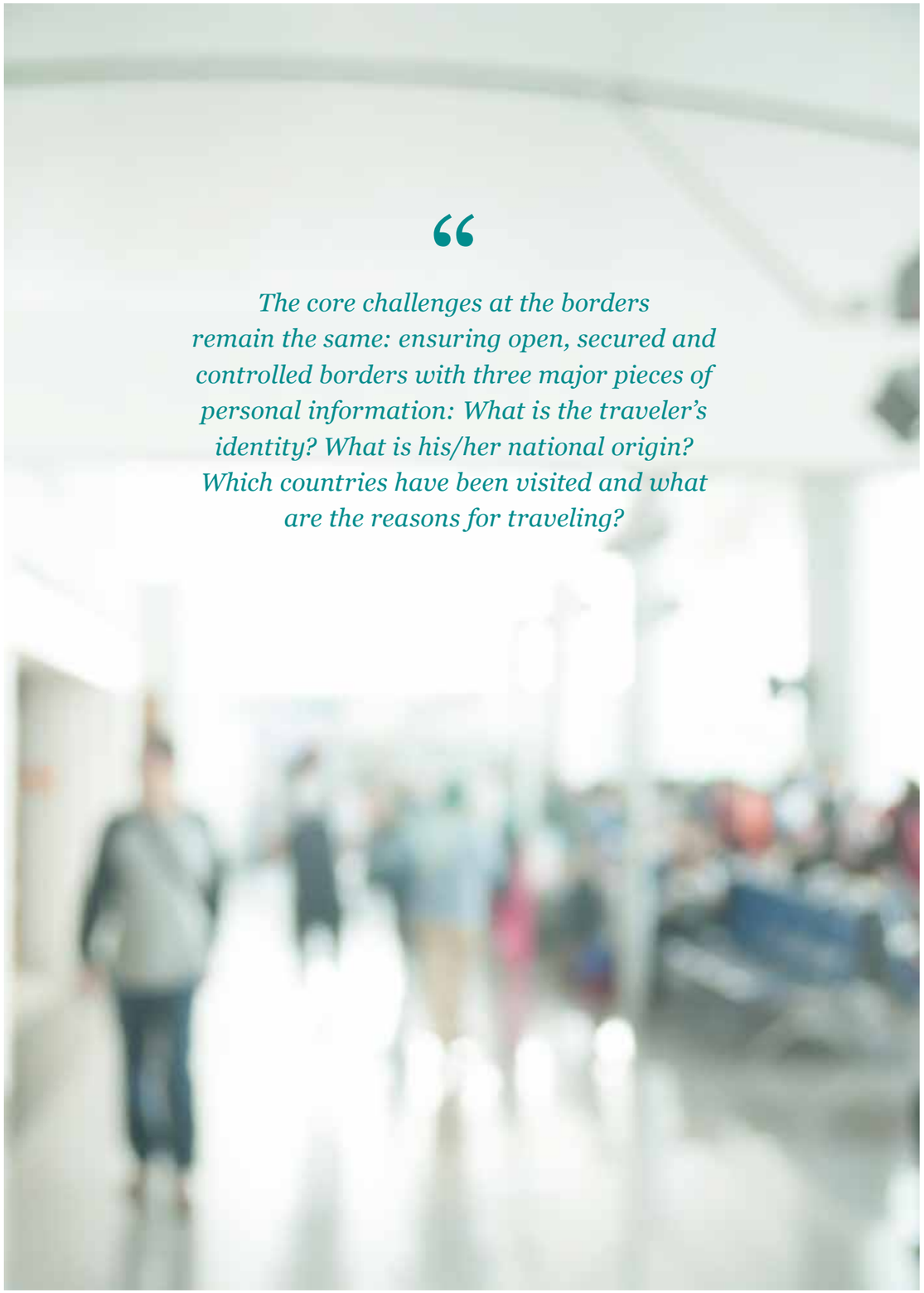
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Sächsische Straße 6, 10707 Berlin
EDITOR-IN-CHIEF: Veronica Atkins
ART DIRECTOR: Katja Gebien

EDITORIAL CONTRIBUTIONS: Gérard Martinez, Frank Schmalz, Sanjay Dharwadker, Rob Haslam, Laszló Balikó, Andrey Golushko, Oliver Winzenried, Lutz Feldhege, Andrea Servida
PHOTOS: Infineon Technologies, Wibu-Systems, istockphoto, WCC, HID, Gemalto, APSCA
PRINTING: Druckerei Häuser KG, Cologne
EDITION: Autumn 2015

The CHALLENGES of *MODERN border* MANAGEMENT

An interview with Gérard Martinez, Gemalto

Silicon Trust met up with Gemalto's Gérard Martinez, Gemalto's Head of Border and Visa Management Solutions, to talk about some of the latest trends in border and visa management and the impact upon people migration and visa control.



The core challenges at the borders remain the same: ensuring open, secured and controlled borders with three major pieces of personal information: What is the traveler's identity? What is his/her national origin? Which countries have been visited and what are the reasons for traveling?

With the recent refugee-based news in mind, are you seeing changes in governments' priorities in Border Management?

The surge of desperate refugees from the Middle East and Africa has indeed put unprecedented pressure on EU countries, especially Italy, Greece and Hungary. The first priority is to provide humanitarian assistance to these refugees. This means food, first aid and shelter but also coordination and reporting.

But I would say that surprisingly there are no changes in the core priorities of governments overall. On the contrary, the main challenges at the borders remain the same: ensuring open, secured and controlled borders with three major pieces of personal information: What is the traveler's identity? What is his/her national origin? Which countries have been visited and what are the reasons for traveling?

Border management is under the spotlight today but it has always been linked to human development, human rights, human mobility and security. That's why it can be such an emotional issue.

Is this making the fight against terrorism and human trafficking a lower priority?

Certainly not! The very process of facilitating travel, economic exchanges and migration can indeed be exploited for human trafficking and terrorism. That's why many authorities around the world have designated the fight against terrorism and trafficking as priority crime areas. They have committed significant resources to protect their citizens from all types of terrorism and to identify and dismantle the criminal networks making millions through people smuggling.

Authorities are fully aware of the need to turn to technology in order to help shape their response to the challenges of processing – in a humane and orderly way – ever growing numbers of genuine travelers into and out of their territory.

Police forces don't have unlimited resources, how can this point be addressed?

That's where IT systems, the redesigning of processes, the implementation of new Border and Visa systems and of course the related training are key.

Authorities are fully aware of the need to turn to technology in order to help shape their response to the challenges of processing – in a humane and orderly way – ever growing numbers of genuine travelers into and out of their territory. I started my career in system integration. Last April marked my second anniversary as head of the Border and Visa Management business unit. Over these past two years, I have traveled around the world, discovering how our authorities are adapting to these challenges. What I also see today is that police forces are relying more on external resources. In fact, when I look at the recent changes, I see two major trends:

More and more players are now engaged in identity checks. For example, airline companies – even the low cost ones – are required by law in some countries to check identity documents. They typically have to compare the passenger, and in particular their entire face, with their identification and to compare the name on the passenger's boarding pass with said identification. In addition, air carriers have the responsibility to decide what to do when the passenger presents a piece of photo identification that does not resemble the photograph or when the passenger does not appear to be the age indicated by the date of birth on the identification presented or perhaps when the passenger does not seem to be of the gender indicated on the identification presented.

This "liability shift", with a growing number of players in the security chain, demands coordinated processes, integrated information on technology systems, knowledge transfer and joint responsibilities with the various stakeholders.

The second trend, which is probably more visible, is self-service technology such as ABC (Automatic Border Control) gates or APC (Automated Passport Control) kiosks. They are designed to speed up processing at the immigration primary line and thus alleviate capacity issues. As a manufacture of ABC and APCs at Gemalto, we've received an exceptional response from travelers, the airports, and the authorities involved in the process. The new technology has been quickly adopted by travelers and has also been positively impacting the officers who can now focus on exceptions.

In short, could you please introduce the specific position of Gemalto in the Border and Visa market?

We've worked to develop a state-of-the-art software platform for border and visa management. Gemalto's expertise is to provide, for each and every traveler, full reconciliation of data for entries, exists and visa authorization.

Coesys Border & Visa Management provides a secure and efficient way to manage the flow of travelers across a nation's borders

by applying a systematic, consistent and reliable control. With this integrated software and services solution, governments can implement their immigration policies and meet the combined challenges of securing borders and simplifying travel procedures.

Information security is built-in at all levels of our border management system. A solution designed to ensure the protection and privacy of all sensitive information during data acquisition, data handling, data communication, data storage and deletion.

Gemalto's Coesys Border & Visa offers a unique integrated border management tool for government initiatives. Combined with Gemalto's professional services, the solution easily integrates with legacy systems while providing a hardware-agnostic approach for data security & privacy protection.

What are your customers achieving with you then?

Gemalto's role is to assist authorities in meeting their operational challenges of border and visa management and with Coesys Border & Visa Management, our customers have been able to build a unified and secure border management system public services and administrations can count on at all times. We can help lay the foundation for an integrated system to merge and streamline layers of disparate processes into a whole cohesive and secure system. This, in turn, is the basis to implement a future-proof, mission critical system, flexible and scalable enough to keep up with the demands of changing immigration policy and technological standards. One really important aspect is that Gemalto provides an uninterrupted operation, with online and offline capabilities. Also, last but not least, it saves costs by automating & optimizing processes, while leveraging technologies for added security and better passenger facilitation.

What are your customers appreciating most?

Well, we made sure that the Coesys Border & Visa Management offer puts the CIO or National Immigration Project Manager in control of a secure and adaptable Integrated Border Management System.

What they appreciate the most is that they are implementing a solution that has already been tested and deployed at international level by other dedicated government security experts.

In these environments, Gemalto is the perfect match as prime contract. We deliver a unique combination of local resources through local partners and international expertise with our own Border & Visa competency center.

The feedback we got also is that our customers like solutions that are built to be hardware-agnostic, ensuring independence from past or future suppliers. Gemalto's solution protects our customers from vendorlock in the fields of biometrics and travel document scanners.

They also value our expertise. Unlike a generalist system integrator, Coesys Border Management provides a full range of applications to implement best-practice immigration processes and state-of-the-art technologies at border management headquarters (HQ) and border control points (BCPs).

In addition, our background is not from networking equipment in airport or working for airlines – but true experience in project management, side-by-side with government authorities and an unparalleled knowledge of secure documents and related processes (enrolment, control/verification).

Would you have a recent example to illustrate this?

> *"Gabon authorities' main objectives are to introduce ICT tools to transform and simplify administrative procedures, for both the visa applicant and the issuing authority.*

As of July 2015, travelers to the Central African nation of Gabon can now apply for visas online. This latest innovation named "e-Visa" forms part of the country's e-government projects, which are aimed at making public services more accessible.

The e-Visa project enables visitors to use the Internet to apply for a visa to enter Gabon. Regular travelers to Gabon have welcomed the government's decision to allow foreigners to apply for visas online, moving away from visa procedures sometimes viewed as complicated.

Once the request for an e-Visa is done on the web, it is processed by la Direction Générale de la Documentation et de l'Immigration (DGDI). The visa is issued at Libreville International Airport.

Visa management is now an essential component of a modern, integrated border management system. It is key to enhancing both security and convenience. Gabon authorities' main objectives are to introduce ICT tools to transform and simplify administrative procedures, for both the visa applicant and the issuing authority. The goal is also to enhance border security through the establishment of a trusted identity — based on document verification, and crosschecks of national and international control lists — during the visa application process. The new system will also facilitate arrival processes, minimize airport congestion and curb visa overstays. In the long term, Gabon seeks to boost tourism and business, and this investment in the right technology will help make this happen. ☒

Visa stamps and stickers could be a thing of the past with latest chip technology

LDS2 – The KEY to *mobile* travel *DOCUMENTS*?

By Frank Schmalz, Veridos GmbH

Preparing for the next business trips I am shuffling through the pages of my German "Reisepass" to see if there is still enough room for stamps and visa stickers. It's still a physical booklet. I do not buy physical books any more. Too much weight and volume for light travel. I am using ebooks. The filofax has been assimilated by the smartphone years ago. It seems like almost everything on paper is moving into the phone; however the passport has been very resistant to that trend. Resistance is futile. At least it has been in the past concerning digitization of processes and paper.

What would be necessary to virtualize the passport booklet and pack it into the smartphone? First, we need an internationally agreed standard to define the data format and interface between the smartphone and inspection system.

Secondly, electronic verification needs an electronic verification device. For the booklet to become really obsolete, this device would have to be available in every inspection situation, in every country, at every border.

During the last 35 years, the International Civil Aviation Organization (ICAO) has done a tremendous job in providing specifications for travel documents; guaranteeing interoperability and acceptance between nations. They also did the same with the chip-in-passport that has been introduced some years ago.

Within an electronic passport, the chip contains the biographic and biometric data of the holder and enables automated border control through the use of electronic gates (eGates). In this scenario, the physical security features of the document have already nearly become obsolete – replaced by cryptographic security. So, the data could come from any device, even a smartphone. But something is still missing…

Currently, eGates to the Schengen border can only be used by EU residents. Third Country Nationals that require a Schengen Visa cannot use the gates, as the current specifications for passport chips do not support all processes at borders. Electronic replacements for entry/exit stamps and visa stickers are still missing.

The ICAO New Technology Working Group (NTWG) is working to change that. A new specification called Logical Data Structure 2 (LDS2) is in the making.

eGates to the Schengen border can only be used by EU residents. Third Country Nationals that require a Schengen Visa cannot use the gates, as the current specifications for passport chips do not support all processes at borders. Electronic replacements for entry/exit stamps and visa stickers are still missing.

This new specification will include electronic replacements for entry/exit stamps and visa stickers. While the NTWG is currently mostly concerned with increasing the security of entry/exit stamps and visa stickers, this step will also enable some new use cases. Travelers with Visa requirements or with limited duration of stay permission, could use eGates. In our time of increased travel frequency, epidemics can spread fast and travelers might not even be aware that they are affected. LDS2 can help to identify if a traveler has been exposed to an infection risk – due to a stay in a country with an infection outbreak, for instance – and enables a fast reaction. Last but not least, it is the last step in making the complete digitization of passports possible.

The ICAO NTWG is following a straightforward approach, by creating a digital representation of the entry/exit stamps and visa stickers in the travel documents chip. There have been cases in the past where this approach has been less efficient than rethinking the whole process and coming up with a different solution more suitable to the digital world.

Entry/exit stamps and visas could also be moved away from the document into large databases of the country being visited. With the increase in electronic travel authorization programs, there is a trend in this direction for low risk travelers from visa waiver countries. However, the database solution also has drawbacks. This database has to be accessible 24/7 at every inspection system that needs to check visas or entry/exit stamps. While this is possible in fixed border crossings by database replication, it becomes more difficult with mobile inspection systems. A database solution basically increases the border requirements from electronic inspection to 'always online'. At green border crossing points in remote areas of the world this could become a challenge.

In contrast, LDS2 works completely offline. The recent hack of the 'Office of Personnel Management' (OPM) in the U.S. shows how difficult it is to secure large databases containing personal data. The security experts have done their utmost to ensure the security of the system, but it is, of course, a moving target: The profit that can be achieved from such a hack justifies extreme investment, thereby creating an unbalanced situation. LDS2 is an example of decentralized data management, which through its architecture destroys every criminal business case, as successfully hacking a passport would reveal only data from one person.

These two aspects of a database approach – high fraud attraction and 24/7 availability – create a difficult scenario. The necessity for constant accessibility makes duplication of the database necessary, which in turn increases the number of valuable attack targets to protect. Finally, new benefits like health risk detection from travel history analysis would require the worldwide exchange of these databases, revealing the personal data of travelers to countries they are not travelling to. LDS2 data, on the other hand, is only accessible to a country the traveler actually wishes to enter.

The constant increase in travelers will boost electronic and automated border control systems, making LDS2 attractive. But electronic visa and entry/exit stamps require nations to allow other nations to access their passport chip and write information into it.

The constant increase in travelers will boost electronic and automated border control systems, making LDS2 attractive. But electronic visa and entry/exit stamps require nations to allow other nations to access their passport chip and write information into it. A special public key infrastructure (PKI) will be needed to secure this access. Many nations will be reluctant to give this access and carry out the necessary investment. But there are always innovative countries that see the additional benefits and act as first movers. Others will follow. Increased efficiency and convenience will pave the way, just as it has been with electronic passports. With electronic inspection systems at every border of a country, the mobile passport can become a reality; as a complementary service to the passport booklets, which will probably stay until the last border in the world has become electronic. ☒

Without identity documents, children risk missing out on essentials like immunization.

People, Birth and LEGAL IDENTITY

By Sanjay Dharwadker, WCC Smart Search & Match

How nations record individuals is subject to constant evolution. In recent decades we saw the rise of biometrics, but the next wave looks to take a more holistic approach comprising foundational identity, civil registration and vital statistics closely coupled to functional systems riding on the latest technologies. How should identity systems cope with this phenomenal evolution? And which issues must be addressed on the road to sustainable, safe and smart identification?

☐ History of identity registration

The history of civil registration goes back to ancient Egypt, Rome, India and China. The first modern national identity systems emerged in the 19th century. The vital events typically recorded are live birth, death, fetal death, marriage, divorce, separation and annulment of marriage, adoption, legitimization and recognition. Legal documents derived from these events include birth certificates, death certificates and marriage certificates.

Standards for identification

Unfortunately, there is little international standardization of identity systems and civil registration, and of laws governing citizenship. For civil registration, there is the UN's Principles and recommendations for a civil registration and vital statistics system. For legal identity, the 2014 "Seoul Declaration" of the Global ID Management Conference recommended the formulation of such principles. For preventing statelessness, the recently developed UNHCR guidelines are an excellent reference. The electronic passport is a good current example of an international identity document, being accepted in 191 countries for border crossing.

Complex foundations

Several complex issues are rooted in the foundations of identity. For one, legal identity does not have a concrete uniform definition in international law. Its scope is often unclear in contexts such as social development and national security. Birth registration is universally understood and defined, but usually addresses two different functions: statistical (baseline data for government planning), and legal (foundation document for establishing identity).

Countries create and maintain legal identity and birth registration records through varying infrastructures and organizational arrangements: under one or several departments and on federal, regional, provincial and local levels. Besides aligning with national legal frameworks, governments also need to recognize international conventions, for example child rights and statelessness.

> *Unfortunately, there is little international standardization of identity systems and civil registration, and of laws governing citizenship.*

The coverage of civil registration varies; many countries use reliable and complete systems, but others still need further strengthening. While the world average coverage of birth registration has improved from 58% in 2000 to 72% in 2015, there is still a long way to go.

Grim consequences

Failure to address these issues will rapidly erode the credibility of legal identity and civil registration systems. At the same time, such systems must operate within both the requisite legal framework and universally acceptable principles of privacy.

People without identity documents are often deprived of education, work, ownership and entrepreneurship. Their children risk inheriting this lack of status. Especially in developing countries whose legal frameworks and identity records are still in their infancy, the inability to establish an identity can have grim consequences, such as:

- Governmental challenges in extending welfare benefits
- Inefficiency and corruption
- Failure to protect vulnerable population sections
- General economic decline
- Wrongful disenfranchisement

In short, guaranteed identification with enforcement of proper checks is an urgent socio-economic necessity.

Pakistani women hold up their national ID cards, ready to vote.

The importance of breeder documents

The UN seeks to fast-track national identity programs per its Post-2015 Sustainable Development Agenda: “by 2030, provide legal identity to all including birth registration”. Framing the objective in this way puts an even sharper focus on linking people to their legal identity through key breeder documents like the birth certificate.

An estimated one billion individuals around the world lack even basic identity documentation. It is this yawning gap that the UN urges nations to close in the next 15 years. In birth registration alone, at least 37 million children are not registered per year. This leaves them at risk of missing out on essentials like immunization and basic education.

Comprehensive civil registration also includes inter alia, registration of marriage, divorce, adoption and death, as these affect the civil status, rights and duties of a person. While birth registration is crucial for establishing legal identity, other breeder documents are often equally important in many contexts.

Legal and administrative aspects of identity

Effective identity registration must meet requirements in five key areas.

Certification: Certificates – undisputable legal proof of identity or civil status – function as breeder documents to obtain other identity documents (e.g. passports, driver’s licenses).

Permanence: Records must be transferred from old to new systems without fail to protect their legal value.

Continuity: The system must render a reliable and up-to-date civil status of each person and of the population at large.

Consistency: Data quality must be consistent across multiple identity systems for the same population.

Privacy: Stringent data security is crucial to safeguard the human right to privacy.

WCC – Adding Value

WCC offers remarkable software and industry expertise to address a wide spectrum of identification issues for governments. These include biographics, multi-biometrics, integrating with multiple data sources and systems, linkage to statistical dashboards, and context-specific identity data. WCC’s software platform ELISE deploys powerful tools such as ELISE Insight and Explorer, and proprietary features such as fuzzy search, multi-cultural name-matching and matching on a mix of different modalities.

The UN seeks to fast-track national identity programs per its Post-2015 Sustainable Development Agenda: “by 2030, provide legal identity to all including birth registration”. Framing the objective in this way puts an even sharper focus on linking people to their legal identity through key breeder documents like the birth certificate.

Easy to integrate, ELISE works equally well in foundational identity, birth registration, and functional systems such as voting and payments. To optimize results, WCC also provides consultancy expertise for managing the complexities of identity programs. WCC understands identification issues and instills best practices for policy-makers, administrators and operational managers.

The evolution of identity and birth registration systems demands far-reaching and long-term solutions. These must be simple and sustainable to address individuals, and yet robust enough when aggregated – often into hundreds of millions of entities. Several national governments are already thinking in this coherent manner. For the industry it means working closer together than ever before. WCC provides the ingredients and impulse for identity programs that meet everyone’s needs and ambitions. ☒

The ANGOLA National ID *program* – A *building* block of DEMOCRACY

By Rob Haslam, HID Global Government ID Solutions

While government agencies have not traditionally been viewed as industry innovators, the tide is changing. Government organizations at all levels are increasingly partnering with leaders in the private sector to make infrastructure investments that will take them well into the future.

Perhaps, the most obvious reason for this trend is that the government workforce of the future will be populated with digitally literate employees, lending itself to a more organizationally open government. We are seeing this model manifest in particular in developing countries where IT infrastructures are being built from the ground up. Governments, such as Angola, which is featured in this article, are building more social, mobile, accessible and information-driven environments to facilitate secure ID applications beyond basic citizen ID.

The Angola National ID Program: A historical perspective

As part of rebuilding its infrastructure following a long period of civil war, the Angolan government decided to replace its outdated national identity documents in the mid 2000's with an ID card system that was not only counterfeit-resistant and durable, but would also provide proof of identity to its entire population of 24.3 million citizens – a daunting task given that 62% of the population lives in widely dispersed urban areas and 38% live in hard to access rural areas.

While an enormous undertaking, the ability to understand the landscape of its citizenry could propel this nation forward and truly change lives. In response, DGM Sistemas of Luanda (DGM) and HID Global partnered to deliver a world-class, custom National ID Card Program to the government of Angola. The program has expanded its overall enrollment, issuance and delivery infrastructure over the past seven years, reaching more than 6.5 million citizens and bringing with it the enhanced ability to securely travel, gain employment and open bank accounts.

The program rollout has been hugely successful. This said, it is the unexpected benefits of the new program that demonstrate the true possibilities for government-to-citizen IDs beyond traditional applications.

A world-class solution

The Angola National ID Card Program incorporates the latest innovations in secure issuance, card technology and citizen-centric services – services that take into account people's needs and expectation for convenience, flexibility and affordability when participating in government programs.

The card

The new National ID system had to meet multiple security criteria, including:

- Matching individuals to their biometrics
- Safeguarding personal data
- Storing substantial amounts of information directly on the card (fingerprint biometrics, images, birth certificates, demographic data)

Angola's dispersed geography required the ability to instantly read the card's data in areas where there was no access to the communications network, as well as modular and mobile data collection and card personalization systems. Delivering on these goals required the deployment of the most counterfeit-resistant document possible, with secure portable data storage, and strong visual security attributes. HID Global's LaserCard® optical security media technology was chosen for its proven security and visual authentication features. Further, LaserCard® optical security media's long-life span and ability to scale with the needs of the nation enables the addition of functions or applications like providing proof of – identity and access to multiple government services.

Angolan cardholders now carry IDs as advanced as those found anywhere else in the world. LaserCard® optical security media allows the cards to not only store personal and biometric identification, but prevents counterfeiting and obstructs tampering, while facilitating quick and accurate authentication of the card. The digital security of optical media-based credentials has never been compromised.

Angola's dispersed geography required the ability to instantly read the card's data in areas where there was no access to the communications network, as well as modular and mobile data collection and card personalization systems.

LaserCard® optical security media encoders allow individuals to have all ten fingerprints encoded, along with photos and personal information, for confident authentication in the field. HID Global supplies both the cards and hundreds of secure ID card printer/encoder systems.

Distributed issuance

The majority of Angolans live in remote, rural locations. In the first phase of the program, the new secure issuance infrastructure deployed to serve these populations included 27 centralized "fixed" centers (9 at Luanda, 2 at Benguela, and one for every other Province) for National ID Card enrollment, personalization and issuance as well as a creative cadre of mobile units (22 trucks) to enroll and issue ID cards to citizens in remote parts of the country. Today there are more than 243 fixed and mobile of issuance centers. DGM, in partnership with HID Global and the Angolan Government's Ministry of Justice, has successfully implemented "Over the Counter" issuance processes in which citizens are securely issued their IDs in less than an hour.

Today the communications infrastructure is able issue new ID cards in an hour – from biometric data collection to issuance to the citizen.

Originally launched without a network communications infrastructure in place, the program has been deployed in stages – evolving along the way. DGM had to construct a country-wide information technology and network communications infrastructure at the same time that initial "fixed" centers and mobile units began to be implemented. Today the communications infrastructure is able issue new ID cards in an hour – from biometric data collection to issuance to the citizen.

Building block of democracy

Beyond the most evident improvements in national security, the Angolan National ID system is contributing to building the fabric of the nation's economy, the legal cornerstones of identity and providing citizens with improvements to their daily lives. As the de facto identification standard for opening a bank account, employment authorization and other daily services the national ID card is not only growing in use, but is now a requirement for all Angolan citizens. The country's focus is therefore on scaling its personalization and printing capabilities, along with greater service and support, especially in remote areas, to build up the nation's central database and reach approximately 24M citizens. The Government is also adopting innovations to enhance the card technology, issuance processes and overall security and efficiency of the program. The LaserCard® optical security media technology originally selected for the card allows this expansion while preserving the security and integrity of the ID system. As the user base grows, LaserCard® optical security media will also allow more sophisticated 1:1 authentication to enhance the security and eliminate all possibilities for fraud or counterfeiting.

What's next?

According to Gartner Group successful citizen eID programs require a trusted relationship between government and commercial vendors and/or partners, with a focus on business value, interoperability and user experience. We actually believe these relationships need to go one step further with entities working together to meet very specific user requirements driven by the unique demographics, geographies and democratic needs of a nation. The nation of Angola provides proof of concept for this approach. ☒

The HUNGARIAN 10 000 Ft *note has* received a *DESERVED* UPDATE

By László Balikó, HPBC

In late 2014 a new banknote appeared in circulation in Hungary; the new 10 000 Ft note. Although looks can be deceptive at first glance with the same size, same substrate and same portrait, an infrequent user might not tell it apart from its predecessor. But this is only true if the older one is not present for direct comparison.

What is obvious at first glance are the vibrant colors, the wider diffractive security foil and the more frequent and emphasized appearance of denomination numeric figures. These are the results of a basic design concept specified by the Central Bank of Hungary well before the banknote's public issuance. The design uses the same thematic as the "old one"; the frontside portrait (1st King – St. Stephen, founder of the Hungarian State) and backside landscape have been kept, complemented by several design elements characteristic of the state foundation era.

The paper contains a watermark with a halftone portrait and built-in Multitype letters, a new embedded security thread with denomination specific magnetic code and cleartext, fluorescent fibers and Shiny Dots. A new, wider holographic foil with large demetallized letters and perfect register fluorescence appears on the frontside.

Keeping basic design and tradition on the one hand and incorporating state-of-the-art security features on the other, was a rather challenging concept. However, it was made a reality by scanning the original hand engravings with an ultra high resolution 3D scanner from Jura Ltd. and completed with the latest intaglio security features provided by Corvina Engraver security design software from the same company (such as increased tactility of intaglio elements, multi-tone effect elements, new intaglio OVI rosette etc.). Increased tactility and livelier background colors help the public – even the visually impaired – to differentiate between denominations. New types of machine readable security features help all of the modern, sophisticated equipment in the whole automatized cash cycle.

Redesigning a banknote was just one part of the project. Modernizing the full banknote printing line was essential to enable the new concept to become a reality. On the prepress side, the DLE (Direct Laser Engraving) device was essential, as many of the new intaglio features are unimaginable using traditional plate originating techniques. The press line of Hungarian Banknote Printing Co. from the mid 80's, was either obsolete or low-performing or both. We have partnered with KBA NotaSys for a thorough on-site refurbishment for much of the equipment and factory overhauling for the rest. Not only did we want to create a new banknote and print it in due quantities, but also cope with the ever increasing quality and traceability demands from the Central Bank of Hungary – driven by the more and more automated cash cycle of the Hungarian Forint. As a response to the above, we have overhauled our BPS 2000/OBIS banknote sorting device, installing the latest development by Giesecke & Devrient: the NotaScan UV, INK and MAG sensor set for the respective security features and with the latest issue of the OBIS3 image comparison system. To respond to traceability and in-process quality inspection issues we have installed the Abaco ICS track and trace system for the whole printing line and Proxima "O" and "I" off-line quality inspection equipment; all from Parvis. The result is a modern banknote line, serviceable for decades, where apart from the devices required for completely new tasks (such as the DLE and Parvis equipment), no new factory installation was needed; and yet it fulfills the Hungarian currency demand. With the creation of this new denomination and putting all of the infrastructure in place to make it work, Hungarian cash cycle and banknote manufacturing can now truly compete on the world stage. ☒

From RUSSIA *with SECURITY*

By Andrey Golushko, Mikron

With the advent of the digital communications era, theft or misuse of personal data stored in electronic documents, transport or even banking cards has become a tragic reality. It brings with it the ongoing challenge to the wide range of enterprises working in the area of data protection and ID security. That's why the manufacturers of secure microcontrollers appear as the real superheroes, ready to defend and establish a sense of order and stability.

☐ First eSignature SIM and strong partnerships

In 2006, Mikron, together with the technology group Giesecke & Devrient GmbH (market leader in payment, secure communication and identity management products and solutions), successfully launched a SIM card production line. Forthcoming collaborations in SIM card manufacturing with Gemalto (world leader in protecting, verifying and managing digital identities and interactions), strengthened Mikron's positions in the Russian and CIS market: all the national communication services providers became the company's key accounts.

The newly developed SIM card microcontroller MIK32C384 was specifically designed with a strong emphasis on code density for secure smart card applications. It was built on a proprietary RISC processor core with hardware program memory protection and user data protection against unauthorized access. It provides fast eSignature generation at very low power consumption, showing power efficiency and competitiveness with best-in-class products. It has already been tested by MTS – Russia's leading communications service provider.

National eID projects

In the hazardous world of digital finances, microcontroller-based smart cards are winning the global fight for secure payments, by handling more and more transactions instead of low security magnetic stripe-based cards. To face the challenges of this fast-emerging technology, Mikron collaborated with Infineon – the European leader in chip cards and security applications. On the basis of this partnership, Mikron was soon able to open its own microcontroller development and production facility.

The dedicated microcontroller MIK51SC72D is a dual interface, one-chip microcontroller, supporting cryptographic algorithms and electronic digital signature. It was designed specifically to respond to the rising demands of contactless, multi-application solutions as well as new government challenges of identifying citizens reliably and securely through the use of multi-purpose electronic ID-documents. Moreover, it has successfully passed EMVCo certification and can be used in certified banking applications. It is currently in use within Russian Universal Electronic Cards (national eID cards). Furthermore, microcontroller MIK51AB72D (from the same product family) acquired cryptography support based on international standards (DES, 3DES, AES, RSA, EC-DSA), a contactless interface (ISO 14443B) and stores significant personal information within the currently issued Russian international biometric ePassport.

Mikron's core competence in the field of contactless communication and secured microcontroller design and manufacturing, allows the company to offer a wide range of products for chip-based security applications: smart cards, transport and other RFID-cards, SIM-cards, e-passports, banking cards with a chip, social security cards and other identification documents. A complete industrial chain from chip design to final product allows us to provide an all-in-one proposition with a full set of IP cores (including crypto hardware), as well as turnkey design services for a very price competitive solution. Mikron also offers development of the chip operating system according to specific customer requirements, embedding a Mikron-developed or any other OS at any production stage, as well as packaging services.

Services and customized solutions

Along with the development and manufacturing of microcontroller and ICs for RFID applications, Mikron offers a complete service including inlays/labels, chip modules, dual interface smart cards (contact and contactless) for system houses using dies from well known suppliers like Infineon, NXP, Impinj, Alien and many others. Providing optimized quality by using predominately state of the art manufacturing equipment from German suppliers, stringent reliability and the highest product quality are guaranteed. Mikron develops antennas itself, mainly taking advantage of aluminum technology in order to achieve the best reading results. A special service by Mikron is the delivery of prototypes for custom solutions in 4-6 weeks.

Mikron offers the entire production cycle from chip design to wafer production to inlays/labels, modules, smart cards and banking cards. By disposing of a complete production cycle, Mikron Group provides partners with benefits, such as making adjustments to meet the client's requirements, prompt response to changes in the client's or market requirements, cooperation starting at any stage in the production cycle, quality control at each stage of production, the highest security rate and optimized logistics. ☒

Founded in 1964, as the "Research Institute for Molecular Electronics" and manufacturing facility "Mikron", the company laid a foundation for the microelectronics industry in Russia. Constantly improving its technological and production facilities, designing new semiconductor products and developing its product portfolio, Mikron Group remains the largest manufacturer and exporter of microelectronics in Russia and CIS – owned by financial industrial group SISTEMA JSFC. Mikron has 3 fabs (3µm; 0,25µm; 180-65nm) and several sales offices in Europe (Munich), USA (Denver) and Asia (Hong Kong, Taiwan), as well as assembly houses in Russia (Zelenograd) and China (Shenzhen).

NEWP@SS

By Silicon Trust

Contactless, multifunctional, fast and secure features are important requirements for the new generation of travel documents. The main challenge lies in the combination of security and convenience: travelers should be able to pass through border checkpoints even more quickly and yet securely and citizens would like to access online services offered by public authorities with their smartphones.

In the past three years, issues concerning the security of electronic identity documents have been addressed by the "NewP@ss" research project. The research conducted by security chip providers Infineon Technologies and NXP, as well as Giesecke & Devrient, was funded by the German Federal Ministry of Education and Research (BMBF) with about 4 million Euro. The companies were part of a consortium of 15 European enterprises and research institutions within the EUREKA program CATRENE.

This project contributes to the Grand Challenge "Consumer and Citizens' security" of the AENEAS/CATRENE VMS. The applications targeted by the Newp@ss project have a large economical, societal and technical impact and are supposed to represent a large part of the complete e-Passport market by 2015-2020. They share in common some stringent needs in terms of security and interoperability at European and international levels.

On eTravel, the European ePassport scheme is viewed as a reference throughout the World; i.e. the implementation of the new protocol SAC could be largely promoted through this project and proposed for Europe and out of Europe. It will allow the promotion of European standards and European industries.

The Digital Agenda sets out the EC's strategy for addressing the main challenges and developments in the information society and media sectors up to 2020. It aims to improve efficiency, modernize administration, reduce bureaucracy and enable citizens to communicate with the various administrative authorities more easily. Once citizens have a secure national ID card and e-Passports, they will be able to gain access more easily to services in an expanded eAdministration.

The consortium has developed data structures and new security chip architectures that are being integrated into the latest globally applicable standards for travel documents. In addition to the ID holder's biometric data, the newest electronic travel documents can electronically record visa data and arrival and departure stamps. This also makes it possible to update ePassports and similar documents during their relatively long period of validity, rather than replacing them e.g. in the case of a name change due to marriage or an address change after a move.

Given citizens' increasing mobility and the constant availability of electronic services, the secure use of digital identity documents for smartphones and tablets was also researched. The experts considered open architectures and tested new security mechanisms at both software and hardware levels. The primary focus was placed on contactless communication with an eID card, secure mobile user authentication and confidential data input and output within a protected computing environment.

The "NewP@ss" research project had a total volume of about Euro 30 million, half of which was covered by business and industry partners and the other half by the governments of five member states of the European Union. The German share was about Euro 8.7 million.

Biometric travel documents are currently issued in all 28 EU states with its approximately 500 million residents. Electronic identity cards are used in 23 European countries. Other European states have already announced that they will introduce electronic identity cards in the next few years or begin issuing the next generation, which this research project helped to develop. A total of 120 states have distributed around 500 million electronic travel documents since 2006. ☒

Wibu-Systems AND Infineon *get* SERIOUS

By Oliver Winzenried, Wibu-Systems

The numbers that characterize the Industrial Internet of Things are staggering: $15 trillion added to global GDP over the next 20 years[1], an annual economic impact of $2.7 to $6.2 trillion by 2025[2], an installed base of IoT units reaching 28.1 billion units in 2020[3]. This revolution is thrilling and alarming at the same time, as jobs, technology, trends, and ways of living are going to be revolutionized. The mission is to make the industrial ecosystem more efficient, sustainable, and responsive to buyers' demands; the risks for security and safety could, however, spread like wildfire, and disrupt not just single businesses, but entire cities.

How to prevent these dark repercussions and enjoy the fruits of the transformation? Modern industry is moved by a constellation of systems that include personal computers, industrial PCs, embedded systems, mobile devices, tablets, programmable logic controllers, and microcontrollers. Along the line, the computational power of these devices decreases, which also makes the implementation of security measures a quite complex task. Additionally, intelligent device manufacturers cannot be expected to offer constant training in security, especially with all the novel threats we are facing every day. The challenge was therefore twofold: Bringing about innovations in a way that would be feasible even under unfavorable conditions and in ruggedized environments, and making them easy to integrate.

1 *Source: General Electric*
2 *Source: McKinsey Global Institute*
3 *Source: IDC*

> *"CodeMeter µEmbedded offers users of our XMC4000 Cortex M4 microcontroller a secured solution for updating the firmware of their already installed embedded systems in the field and for releasing new functionality through licensing.*
>
> *Maurizio Skerlj, Senior Director responsible for the Industry Microcontrollers business unit at Infineon.*

> *"By working with Infineon, we have mastered the challenge of implementing a DRM system in a microcontroller. CodeMeter µEmbedded gives our shared customers a solution that protects their firmware against tampering, cyberattacks, and reverse engineering. And since CodeMeter µEmbedded is fully compatible with CodeMeter – our security solution for PCs and embedded devices – and with DAVE, they can immediately start protecting and licensing their software.*
>
> *Ruediger Kuegler, VP Sales and Security Expert at Wibu-Systems*

Based on the popular and widely accepted CodeMeter® solution for protection, licensing, and security, the German security specialists at Wibu-Systems have developed CodeMeter µEmbedded, which addresses the specific needs for firmware updates or upgrades to microcontroller-based systems: code integrity, license controls, reverse engineering protection, and code copy protection. As if the technological benefits were not enough, Wibu-Systems has also provided a means to monetize the economy of the future.

To reach such an unprecedented level of sophistication, Wibu-Systems has partnered with Infineon Technologies to enable secure update functionality in Infineon's range of XMC4000 microcontrollers. In its first release, CodeMeter µEmbedded is set to enhance the standard tool chain and provide secured firmware updates and functional upgrades in embedded systems built around XMC4000 microcontrollers.

As controllers are being used more and more in demanding and control-based tasks such as pump controllers, motor controllers, sensors with fieldbus connections and the like, secure loading solutions become a critical factor. The job of CodeMeter µEmbedded is to facilitate the loading of updates into the Infineon XMC4000 microcontroller series and enable additional features in any insecure environment. In a highly connected smart system, several factors need therefore to be taken into account:

1. Only code from a trusted source must be loaded in the controller. The code has to be encrypted during transport and loading, and decrypted inside the controller, based on a controller-bound, individual keyfile in the boot ROM.

2. There should be measurable and verifiable license controls over the controller loading the code, with the ability to unlock (activate) additional features of the microcontroller.

3. The code must be loaded and decrypted only in an authorized (licensed) controller. Its use on non-licensed controllers or in an emulator should be prevented and discouraged.

CodeMeter µEmbedded aims to protect the firmware of the controller during updating in the field against tampering, reverse engineering, and copying. Furthermore, it becomes possible for OEMs (the developers of the software that runs on the controller) to expand the functionality of the hardware or software, so that their client (the user) can take full advantage of the product solution.

With CodeMeter µEmbedded, the user can now import an encrypted file into the OEM firmware file from an external environment. Encryption is triggered via the development environment – DAVE® 4.0 from Infineon. For this purpose, ExProtector is run via a plug-in installed in DAVE to encrypt the firmware

“CodeMeter µEmbedded does not just safeguard intelligent device manufacturers against external threats coming from unknown violators. It also protects customers against subcontractors’ malpractice; manufacturing devices equipped with XMC4000 can inherently control production volumes and prevent illegal batches of goods from ending up on the grey market. We see a double advantage in this partnership: Infineon and Wibu-Systems have streamlined a complex security process and help eradicate product counterfeiting.

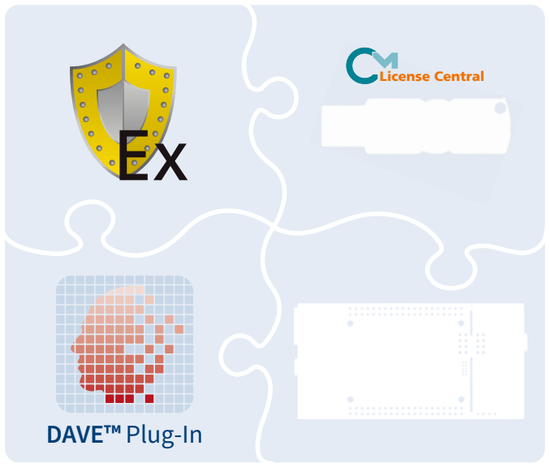
Oliver Winzenried, CEO and Founder of Wibu-Systems

file. After transfer into the XMC4000 controller, the firmware is decrypted and stored in the flash memory, while decoding is handled by the XMC4000 controller.

For optional later upgrades, the microcontroller can generate a request file with the fingerprint of the controller. This encrypted file is transmitted to the manufacturer (by email or online) and a license update is generated and returned. This license update can be transferred to the controller to provide new licenses or make new features available within the microcontroller.

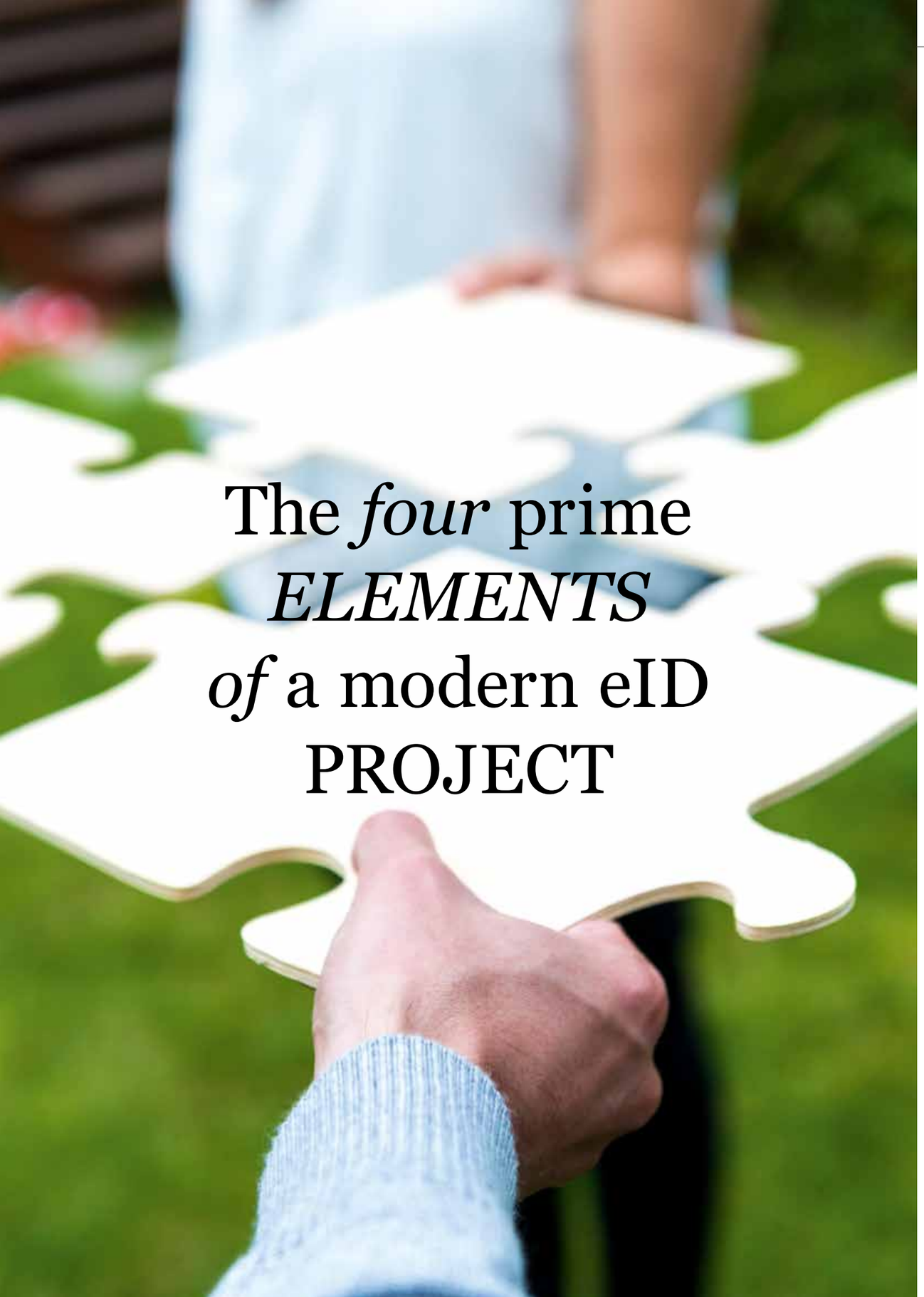
CodeMeter µEmbedded has an extremely small footprint, amounting to less than 60 kBytes. To accomplish this, Wibu-Systems has streamlined its functions to a minimum. The licenses generated are fully compatible with all CodeMeter variants and CodeMeter License Central. They are bound to the unique ID of the microcontroller and can be activated directly during manufacturing. Additionally, Features-On-Demand can be enabled later via remote file updates.

CodeMeter µEmbedded is license-compatible with CodeMeter Runtime. Transferable licenses can be moved onto a device from a CmDongle or a CmActLicense. CodeMeter µEmbedded can also be used to securely store symmetric and asymmetric keys. The keys themselves are located in a protected memory area and can only be used on a device with matching ID.



Utilizing the outlined approach allows multiple use cases with a single technology and tool-chain, while guaranteeing effective firmware protection against copying and reverse engineering. Functional upgrades can take place without any changes to the firmware, and secure firmware updates are now possible even in insecure environments. Fundamentally, this is a user-friendly security solution with state-of-the-art cryptography technology.

CodeMeter µEmbedded has now been successfully integrated into the XMC4000 Infineon microcontroller family. Starting in Q4/2015, developers can fortify their application code against piracy and license it in XMC4000. All tools for protecting the code are now fully integrated in Infineon’s development platform DAVE. ☒



The *four* prime *ELEMENTS* *of* a modern eID PROJECT

By Lutz Feldhege, cryptovision

Modern eID document project requirements often ask for a variety of elements, but can be distilled into the four prime elements of multi-application, multi-segmentation, secure in-field application loading and data management. Each has its own set of unique challenges and care should be taken to cover each requirement adequately enough.

For a start, the idea of the card being able to carry multiple applications is vital, as so many eID projects are extending usage and are using smart cards for secure storage of document validation data and incorporating additional applications like ePKI for digital signature, electronic driving licenses, mass transit ticketing, or even payment applications.

The element of "multi-segmentation" – different secure containers on the card for different authorities – is also becoming just as important as multi-application but for slightly different reasons. By utilizing a trusted eID credential as a root for other services, different government ministries can utilize a multi-application document rather than issue their own document. Instead of having a single purpose voter identification card, a social security card, and a taxpayer ID card, each of these relevant ministries could leverage one eID card.

Facilitation and management of eID documents in the field is a topic that has garnered a lot of interest recently. Back-end data management in a secure environment is an accepted scenario within the secure document world but more and more it is a necessary requirement for both data management and application loading to be done in-field in a secure manner.

Take, for instance, secure in-field application loading after the document has been issued. Unlike electronic passports which are intended to be static documents with long effective lifetimes, and which are written once and read many times, eID cards are much more dynamic documents which may require both, changes to the cardholder data (update of current address, change of contact information) and additional card functions. Applications can easily be added as eID usage grows and the issuing authority manages deployment of new eID services. With a flexible card operating system, adding new functionalities can be accomplished in-field, even on previously issued eID cards.

As with secure in-field application loading, secure in-field data management (both read and write) is of paramount importance. Historically, when an eID document was to be updated with new cardholder demographic data or new applications, the document needed to be re-issued or even replaced. However, using existing standards like EACv2, allows for setting fine grained permissions for the card content, which allows a delegation model where certain data on the card can be read by one agency but restricted to others. For example, a single eID card can hold data specific to two different ministries, as a voter identification card it might hold sensitive data such as party affiliation and voting jurisdiction as well as a tax payer identifier. By employing certificate-based authorization mechanisms, tax authorities could read the taxpayer ID, but not the voter information stored. Further, the permissions can be set in such a fashion where some information can be updated on authorized terminals such as change of political party affiliation made at an established voting location.

These factors can best be best achieved by an access certificate-based infrastructure composed of:

- A PKI backend system
- Authorized terminals
- A suitable certificate and terminal management system
- A flexible eID document solution

This is all based on existing standards, such as EACv1 and EACv2. Latest standardization and interoperability initiatives (eIDAS) also underline the continuation of this trend. While these standards are already very mature and well established for machine readable travel documents, they are also ideally suited for other types of documents, such as a health care card which carries patient data securely, but still allows for update of heath conditions, or student campus cards that carry both enrollment data and allow for on campus payments.

Such a system outlined does not have to be as complex or as expensive as, for example, the German eID system. The combination of core security mechanisms and lean technology components can provide a flexible and scalable solution by using open standards and supporting open platforms reduce overall costs of the system.

Cryptovision has proved that this model is effective with SCalibur (as well as ePasslet and CAmelot) and has been successfully deployed in numerous international projects around the world. ☒

The first BIG STEP in eIDAS *implementation*

By Andrea Servida, European Commission

With the adoption of all the implementing acts, we have taken a concrete step to building and unleashing the potential of Europe's Digital Single Market. Less than a year ago, eIDAS Regulation entered into force. Today, we have completed the adoption of all the implementing acts due by 18 September 2015. This is a remarkable accomplishment, that makes the EU the first and only region in the world having a workable and balanced legal framework for cross border use of electronic identification and trust services.

☐ Operationalizing eIDAS via the recently adopted implementing acts is a concrete step to building and unleashing the potential of Europe's Digital Single Market. With eIDAS, the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access to services and do transactions online and across borders in just "one click". Indeed, rolling out eIDAS means higher security and more convenience for any online activity, such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments, bidding for online call for tenders, etc.

What does this mean?

Today, four implementing acts were published in the official journal: two for eID (on the interoperability framework and on levels of assurance) and two for trust services (on the formats of advanced electronic signatures and seals and on the technical specifications of the national Trusted Lists).

Let me briefly highlight what this means in practice. For eID, at the end of this month (September 2015) Member States could, on a voluntary basis, start the procedure to notify and recognize national eID, meaning that citizens and companies could use "cross border" to access online public services. This is because the EU now has a set of legal rules (the eIDAS Regulation) and tools (i.e. the level of assurance and the interoperability framework) to support the transparent and accountable mapping of the trustworthiness of existing and diverse national eIDs, together with agreed operational and security specifications for interoperability. Is this all? Not really. Under the Connecting Europe Facility (CEF) the European Commission and EU Member States are also rolling out the eID technical interoperability infrastructure and components to operationally support the cross border use of eID. This is a real premiere in the world!

But, are we done with all this? Not really. The journey has just started and everybody (in particular Member States, the private sector stakeholders and the Commission) has to get ready to fully benefit from EU-wide use of eID. A key enabling role is for MS which have the possibility to notify their eID means without waiting for 2018 when the cross border recognition of eID becomes mandatory.

For the trust services, eIDAS has significantly upgraded and improved the existing legal framework for e-signature. The newly published acts on the formats of trusted lists and of advanced e-signatures and e-seals to be recognized by the public sector, complete the set of tools to ensure transparency and efficiency for cross border use of trust services (i.e. e-signature, e-seal, time stamping, e-registered delivery services, website authentication). Indeed, it would be easier and more convenient for citizens and companies to use their e-signatures/e-seals everywhere in the EU, for transactions with public administrations as well as, we also expect, private sector businesses.

In addition, the establishment at National and EU levels of trusted lists of trust service providers, together with the possibility to differentiate qualified services by means of the EU trust mark, will greatly improve both the transparency of the market, as well as the user's understanding of the quality and security of the services they rely upon. To conclude, I emphasize that on 1st July 2016, eIDAS will apply and the existing e-signature directive will be repealed. By then, all Member States have to have a supervisory body in place as provided in eIDAS regulation. Such a body will have to be operational in order to allow market players to become compliant with eIDAS in due time. It is not only time for you to get ready, but also for us.

What would come next?

We, at the European Commission, are working and will continue to support you in this last phase of eIDAS implementation. Through the technical solutions deployed under CEF, we foster interoperability of eIDAS tools such as e-ID, e-Delivery and e-Signature by linking up Member States' infrastructures.

Besides this interoperability layer, we also design activities to ensure continuity of our engagement actions, as well as support a permanent exchange and discussions among stakeholders.

Building on the key messages gathered in the past events and the suggestions that we're receiving on our online participatory platform, we are also working to:

- Set up an eIDAS European Observatory to boost online trust, security and transparency in the DSM as a virtual network of stakeholders to exchange ideas and good practices, as well as recommend actions and initiatives to ease the uptake of electronic identification and trust services.
- Launch a series of high-level roundtables to define strategic lines to foster eIDAS as an enabler for market digitization.

Much more to come. Stay tuned! ☒

Bundesdruckerei finds COMMON GROUND for Berlin *and Bavaria*

By Silicon Trust

Berlin-based Bundesdruckerei GmbH has acquired a majority share in the German IT security specialist, genua Gmbh, based in Kirchheim near Munich. genua specializes in network security solutions and focuses on customers with special IT security requirements – above all mechanical engineering companies and public authorities. Its product range includes firewalls, virtual private networks (VPNs) for secure data exchange on the Internet, remote maintenance solutions for machinery and IT systems, as well as solutions for mobile security.

> *"We are happy to have found, in Bundesdruckerei, a strong partner who follows the same philosophy as we do: high-security solutions made in Germany.*

☐ "genua's portfolio rounds off Bundesdruckerei's product range perfectly – this acquisition is part of our strategy as a provider of full IT security solutions for public authorities and SMEs", Ulrich Hamann, CEO of Bundesdruckerei, explained.

genua gmbh was founded in 1992 by Dr. Michaela Harlander, Dr. Magnus Harlander and Bernhard Schneck. All its products are developed and manufactured in Germany. It has a staff of 200 working at its main site in Kirchheim and branch offices in Berlin, Cologne and Stuttgart. Bundesdruckerei is acquiring a 52 percent share. The remaining 48 percent will remain with the company's founders, who will continue to be responsible for the company's executive management.

"We are happy to have found, in Bundesdruckerei, a strong partner who follows the same philosophy as we do: high-security solutions made in Germany. Our solutions complement each other ideally and we see considerable business potential in public authorities, government agencies and, above all, in the industrial sector", Dr. Michaela Harlander, co-founder and managing director of genua, stated. The company will continue to operate independently on the market.

Bundesdruckerei offers innovative solutions relating to full IT security management. These are aimed primarily at companies and institutions. "We have made significant progress in the past few years: from a printer of passports, ID cards, banknotes and stamps, to a provider of comprehensive security systems for both the analogue and the digital world", said Mr. Hamann. Here, the company sets its main focus on secure identities – i. e. the question of: Is this person really the person he/she claims to be? As Mr. Hamann underlined: "Our solutions focus on security, efficiency and customer benefit – allowing companies and authorities to concentrate on their own core processes". ☒

2015 ID4*AFRICA*: The *inaugural* EVENT

By Joseph Atick, IBIA and Greg Pote, APSCA

Development agencies are bullish on Africa's prospects. The World Bank's June 2014 Global Economic Prospects report lists sub-Saharan Africa as one of the fastest-growing regions globally. According to a recent report by the African Development Bank, average growth was 3.9% last year and is expected to accelerate in 2015. An article in The Economist in May this year stated that foreign direct investment (FDI) is expected to reach $55 billion in 2015, 20% higher than in 2010. In contrast to inflows of capital in previous years, recent investments are increasingly targeting the less resource-rich countries and Africa's booming middle classes. According to the same article, the amount of investment into technology, retail and business services in Africa increased by 17 percentage points between 2007 and 2013.

Although European states spearheaded trade with Africa, today Asia is increasingly playing a larger role in the growth of African GDP. Chinese investment and development projects in Africa have been a significant driver of economic growth for several years. Anyone who has taken a recent flight from Shanghai to Africa would have found it packed with Chinese blue-collar workers going to work as middle managers in construction and mining projects in East and West Africa. Despite the inroads already made by China, African trade with India is now growing at a faster rate than Chinese trade and is projected to reach $100 billion in 2015.

However, while Africa's economic growth is accelerating, the benefits are still by far unevenly distributed. For social development to match economic growth and generate long-term gains, inclusiveness is essential. There is a clear need for robust national systems that provide digital identity to all Africans, ensuring that everyone can access government services and benefits, prove their eligibility and be included in Africa's economic takeoff. This is why the recently launched ID4Africa event held in June this year, was an event whose time had truly arrived.

The idea for ID4Africa was motivated by the need to change the current situation of identification systems in Africa, where large segments of the population continue to suffer from the lack of robust and accessible ID. In many cases they are not documented in the civil register and as adults they do not hold identity credentials that enable them to exercise their rights and participate in society. As a consequence, they remain in the shadows of society; excluded, burdened and unable to benefit from the fruits of development.

This clearly has to change.

ID4Africa was conceived to promote the responsible adoption of modern digital identity systems as drivers of socio-economic development. It is a forum designed to allow African nations to compare experiences, share knowledge and pool resources to build capacity related to developing identity systems. It is a movement of empowerment where Africa would take matters into its own hands and would dictate how it will respond to its identification needs.

In June 2015, the unprecedented ID4Africa – 1st Government Forum on Electronic Identity, brought together over 300 regional and international representatives of four key stakeholder groups in the identity space in Africa: the identity authorities and users, the international development agencies, the solution providers and the domain experts. The convergence of these four groups in a focused forum created unique opportunities for networking and exchange of ideas, experiences and funding sources. It united all the necessary ingredients for enabling the right ecosystem to emerge for the adoption of e-ID in the service of socio-economic development.

The forum featured an exciting lineup of government and identity experts that presented on real experience relevant to Africa, on topics that are hot today. Many discussions were held on the subject of establishing central databases, biometric enrolment and verification, as well as the different services that could be offered through national ID systems. Most importantly, this was the first forum in Africa that brought together under one roof over 30 global identity industry leaders, to exhibit their latest innovations related to digital identity and secure credentials. It created a unique opportunity for identity experts to demonstrate and explain to senior African government decision-makers responsible for national identity systems, how these solutions can be used to build identity systems that will support socio-economic development in Africa.

While developments in digital identity systems are being undertaken in a number of African countries, many of these systems are still a far way off from ensuring that the benefits they were designed to provide are being received by the citizens who need it most.

At the end of the first day, Forum Chairs Joseph Atick and Greg Pote highlighted a number of key issues, which had quickly surfaced during the presentations and discussions. It was clear that while developments in digital identity systems are being undertaken in a number of African countries, many of these systems are still a far way off from ensuring that the benefits they were designed to provide are being received by the citizens who need it most, and that this would hamper all efforts in having citizens view their national IDs as a fundamental part of their existence.

Another vital issue expressed throughout the forum was the stifled level of investment given to developing civil registries (which include birth, death and civil status records), particularly when one considers they are the wellspring from which all other identity systems grow. However, what became certain was that Africa has a united resolve to make the best investments forward to improve on, and provide sound and effective national identity systems that will equally benefit all citizens.

ID4Africa calls for an annual meeting to allow the movement to define the agenda year after year and to achieve the stated objective. The inaugural event was proudly hosted by The National Identification Authority (NIDA) of the Ministry of Home Affairs of Tanzania, and organised by APSCA and the Identity Counsel International (ICI).

ID4Africa 2016 will be held on May 24-26, 2016 in Kigali, Rwanda and will be hosted by the National Identification Agency of the Government of the Republic of Rwanda.

SILICON TRUST DIRECTORY 2015/2016

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 USbased 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 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 protect- ed. Based in Orange County, California, it is a technology-driven company with significant experience in diverse markets, and is uniquely equipped to address the needs of customers worldwide in an evolving technological landscape.

www.identive-group.com

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 multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

OPEN LIMIT

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

www.openlimit.com

OVD KINEGRAM

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

www.kinegram.com

PAV

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

www. pav.de

PRECISE BIOMETRICS

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

www.precisebiometrics.com

PWPW

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

www.pwpw.pl

REINER SCT

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

ROLIC

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

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

UNITED ACCESS

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

WATCHDATA TECHNOLOGIES

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

WCC

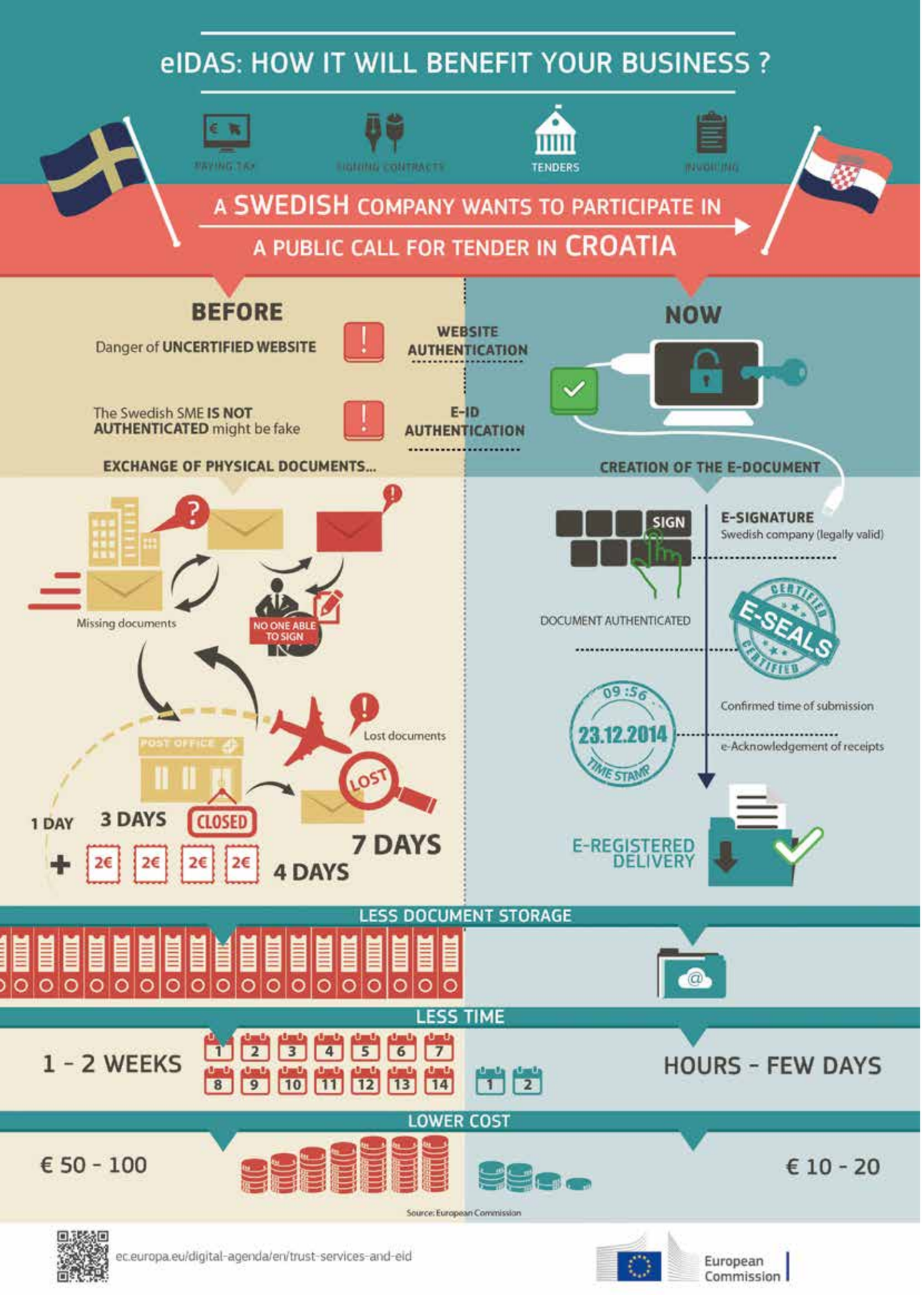
Founded in 1996, WCC Smart Search & Match specializes in the development of enterprise level search and match software for identity matching. Its software platform ELISE delivers meaningful identity matches using multiple biometrics and/or biographic data from a wide range of sources at sub second response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

WIBU-SYSTEMS

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

X INFOTECH

X INFOTECH 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



FIND
WHAT LIES BEYOND THE EXPECTED

Border Control
Justice & Public Safety
Civil Identity

SMART SEARCH & MATCH

www.wcc-group.com