NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

OCTOBER 2014 | #15

The VAULT

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

THIS EDITION'S CONSULTANTS: Ingo Liersch, Robert Bach
EDITORIAL CONTRIBUTIONS: Robert Bach, Eric Billiaert, Oliver Winzenried, Frank Schmalz, Veronica Atkins, Rob Haslam, Antonia Maas, Christian Wagner, Urs Fawer, Dave O'Connor
PHOTOS: Veronica Atkins, Infineon Technologies, WIBU Systems, The Hunger Project, istockphoto, Bundesdruckerei GmbH, A. Bedoy (CC BY 4.0), iStockphoto
PRINTING: Druckerei Häuser KG, Cologne
EDITION: Autumn 2014

eID + 1 + 1
A *PERFECT* match?

By Robert Bach, Infineon Technologies

Is there such a thing as the perfect recipe for a good relationship? Online portals argue that algorithms go a long way in finding a suitable match out of a large pool of possibilities. But what if there is more than one variable? It could get tricky. It's not too different in the world of smart cards: Multi-application and the convergence of services on a government-issued identity card have been on the horizon for some time, with some early adopter schemes in Asia. In theory, coupling high use applications, such as health, transport or insurance with a government-issued secure token has always been attractive. In reality, however, the complexity of implementing such schemes, the discussions of data ownership, privacy and liability, meant that multi-application remained more of a theory than a reality. But in the last year, the benefits of using the security and scope of governmental ID schemes to bring further services to citizens have been the driver behind some new schemes on the African continent: The South African National Electronic ID Card and the Nigerian electronic ID card, in roll-out since August. These schemes have the potential to kick-off a whole new phase of multi-application schemes.

Public Transport applications are considered a good multi-application match

What was the motivation of secure government ID card schemes in the past? From when the implementations of secure electronic ID documents started rolling out about ten years ago, the focus has been on security. With the possibilities of advanced chip technology, increasing memory and faster processing power, the security of the overall ID system became pivotal: Secure enrollment, using different biometrics, secure central or de-central data processing, secure population databases as the basis of a functioning ID backbone. A secure database infrastructure was and still is the heart of any government-issued ID scheme.

In terms of applications, some government documents, given their form factor, are designed to host single applications, for example the electronic Passport. Based on ICAO specifications and other regional frameworks, the key driver behind electronic Passports scheme is to secure travel throughout the world. After the terrorist attacks in the United States in September 2001, and the security vulnerabilities within the international travel sector that became apparent, an international effort went towards securing both the travel document and increasing the security when verifying the validity of these documents. Many airports now feature Automated Border Control systems, making use of the biometrics function in ICAO-compliant travel documents.

Beyond international security and safety concerns, the rise of national ID schemes using chip technology meant that additional applications were incorporated beyond travel. With the advantage of only national legislation regulating these additional uses of an electronic ID card, now citizens using these cards enjoyed further benefits of the additional applications. Especially APAC countries were fast to pick up this trend, with Europe and now Africa following. So, what kind of applications are suitable to be added to national ID documents? It seems that local schemes, such as transport and micropayment are faster and easier to integrate than worldwide payment schemes, such as EMVCo and are therefore the main driving application to go into convergence. First examples for this kind of convergence are the MyKad card in Malaysia, which has been shipping for 10 years and the new South African National Electronic ID Card.

In terms of market volume, ABI research, in a recent study from August 2014, expects to see the volume of converged cards in circulation to increase to 2.03 billion units in 2019, penetrating 26.9% of the total worldwide population. ABI expect EMV to be a good standard also due to its familiarity with end-users and reckons Africa is a focal point for convergence due to widespread financial inclusion schemes.

Positive market trends suggest that the move to convergence is a natural one. However, it is not quite so. In fact, the deployment of multi-application schemes based on government-issued documents is very complex for the issuers. All relationships, i.e. from the government to its citizen, the government to the private sector partners, the private sector to the citizen and the relationship a citizen has to both, his or her government and the, say, financial institution offering services, need to be defined and standardized. However, the rewards can outweigh the risks when it comes to multi-application schemes: After spending a massive amount of resources, most governments are keenly interested in high deployment rates of their new electronic ID documents. Offering additional and helpful services to citizens can significantly increase the take up and use of these documents. It has become apparent that the government responsibility does not end with setting up a secure system and issuing the cards to the population. Usage of the issued documents is the key factor that makes ID schemes a success or not. Getting the population to actually use their cards as opposed to carrying them for personal identification is a massive task. eGovernment services, such as online tax declarations and online registrations are often not sufficient to change the citizens' habits. In this situation, convenient and high frequency applications, such as public transport and access to financial services can help to increase the usage of electronic ID cards.

Depending on whether the citizen had to pay for his or her ID card, additional services primarily mean better value for money. Often mandatory, fees for government-issued ID documents are always debated and in many countries translate into a being a covert tax burden. Additional services would educate the population on the advantages of smart card and mobile technology, for example by using a contactless card for public transport or mobile payment.

In order to implement successful multi-application schemes it is important to start discussions early. Advantages have to be worked out for all parties involved, which can lead to significantly longer decision and project management phases. Technically, the document lifetime is a major challenge. While Government documents have an average lifetime of 7 years, payment cards have a lifetime of max. 3 years, transport cards have an even shorter renewal cycle. A secure removal and update of applets has to be possible, as well as a strict, hardware supported separation of governmental electronic functions and additional private sector applications. For those certified upgrades and application exchanges, Java is an ideal solution. Also, there is growing need for larger hardware: More memory for applications to run, increased performance, advanced security concepts to safeguard secure and certified applet upgrade mechanisms. For those future scenarios, suitable hardware and software solutions are already available. Governments and project implementers should make sure, that their value-chain is future-proof and uses established industry standards, such as EMV for payment or FIDO for authentication. Standards make the implementation and deployment easier.

So, what are the key references in the market at the moment that governments can look to when thinking about implementing their own schemes?

After spending a massive amount of resources, most governments are keenly interested in high deployment rates of their new electronic ID documents. Offering additional and helpful services to citizens can significantly increase the take up and use of these documents.

Malaysia's MyKad is one of first multi-application national electronic identity card projects implemented worldwide with approx. 2 million units issued per year. With nearly 20 million MyKad cards in circulation, it is a good example of how a scheme can evolve and be improved over time. Recently the card was upgraded, featuring a high security polycarbonate card with an integrated dual-interface crypto controller, to enable contactless payment, which is used as a Tap-n-Go or RapidKL transportation card. The MyKad card offers as many as 50 applications, such as travel, eDriving License, eHealth, eSignature, ePurse and Transport.

Another valid example is the South African National Electronic ID Card. The rollout of the new eID started in summer 2013 and it will take nearly eight years until all 51 million South African citizens have enrolled in the scheme. In South Africa, the polycarbonate smart card securely stores the citizen's personal data including a digital photograph and fingerprints. Citizens can rely on the eID as a single card for multiple applications: Firstly for secure identification and registration for voting and other e-government services, secondly it can also serve to give access to banking services. As a result the government can meet more than one objective: By increasing electronic transactions in the country, it starves fraud and corruption of cash. The transparency that comes with such financial inclusion schemes helps stabilize the country's economy and, at the same time, it increases the efficiency of the government's own administration.

In order to implement successful multi-application schemes it is important to start discussions early. Advantages have to be worked out for all parties involved, which can lead to significantly longer decision and project management phases.

The recent launch of the NIMC, the National ID card of Nigeria, caused quite a stir. For the first time, a national, government-issued, ID card featured a brand logo of a private corporation: MasterCard. All in all, the card will have a total of 12 applications, the launch kicked off with 5: Travel, ePKI, EMV, Biometrics (Match on Card) and ePurse. The NIMC project is considered the largest financial inclusion project on the African continent, giving citizens the capability to receive social benefits, pay and withdraw money from ATMs.

Taking a look at the supply-side of multi-application capable hardware, selected security controller families are already supporting the specific requirements previously discussed. Take for example Infineon's SLE 78 SOLID FLASH™ dual-interface and contactless 16-bit controller family, certified according to Common Criteria up to EAL6+ (high) level.

With its 16-bit dual CPU, the digital security concept Integrity Guard with fully encrypted data path, and a total memory size of up to 700 kByte, it reflects the requirements of the multi-applicative future already today.

Governments and project implementers should make sure, that their value-chain is future-proof and uses established industry standards, such as EMV for payment or FIDO for authentication. Standards make the implementation and deployment easier.

The digital security concept Integrity Guard enables the SLE 78 family to perfectly match governmental targets in security, reliability and privacy protection. Integrity Guard is ideally suited for a secure but nevertheless easy implementation of multi-application schemes as the underlying hardware itself strongly supports Software Providers in a secure and certified implementation.

The integrated Memory Management and Protection Unit serves as a hardware firewall to enable the secure separation of adjacent applications, i.e. governmental and private sector functions.

The integrated SOLID FLASH™ memory offers sufficient space to host plenty of multi-application use-cases on one card. It permits efficient loading of applets. Post-issuance of additional applications – even if the card is already field-deployed – now becomes easily manageable.

However, the limited number of references worldwide still put A bit of a damper on the topic. While there are some interesting developments, both in Europe and beyond, implementing multi-application schemes remains a tall order. Russia, France and Poland are all currently debating or beginning to implement some sort of convergence ID project and it is yet to be seen whether it is, in fact, an unstoppable trend. ☒

“SECURE ID systems *require* *vision* and *COURAGE*”

Silicon Trust met up with Eric Billiaert of Gemalto
for a Fireside Chat on the topic of Identity.

Identity management is key for the secure development of the Internet. The term “the internet of identities” is echoing more and more in conferences I attend. It comes from a clear awareness and requirement to remove the problem of not knowing for sure to whom you are talking, dealing or transacting with. The underlying challenges for security in relation to official, legalized and guaranteed forms of identification are the fight against cyber-crime and the creation of a framework of trust for the digital world.

☐ Primarily, it is about the efficiency between citizens, business and governments to foster greater economic growth within the country and the only way to help achieve that goal is to fundamentally make sure that you are dealing with the right person and the right organizations in a simple and effective way. These questions of national eID, the set up of a framework of trust for the Internet, protection of every citizen's identity and privacy in a state of law are approached throughout the world by each country in a different manner and with different timelines in mind.

Is the eID topic as much a private business topic as it is a governmental topic or for the newcomers is it primarily more public sector orientated?

Public Authorities have somewhat unwillingly been caught up in this proliferation of dynamic change in the tertiary economy and personalized services oriented towards the citizen or the consumer.

However, the sovereign bond is not just an archaic relic of the centralization of yesteryear – it is first and foremost the emblematic and identity-laden vehicle for collective trust and thus for the social cohesion of any given territory. So for me, it is up to the authorities to set up the pace: set the governance framework, the legal framework and encourage operators and banks to work together. This requires vision and courage. If you look at Estonia, it was clear that the government there wanted to leverage the internet opportunity. In their constitution, there is the right to access the internet for each citizen. All the ministries are filled with people in their thirties promoting transparency in Government. Even the Prime Minister is explaining how IT is a tool to transform the country. When such vision and will exist, then the process goes much faster.

Having said that, it's also true that in a Government environment everything can take about ten years to fully roll out. Expecting a clear ROI three years after can be disappointing. It's like building a highway and trying to justify return on investment based on the first twelve months of traffic load. It can be very, very frustrating.

Maybe over a period of twenty years or so can one see benefits and growth through haulage and tourism or better connections to other regions, or the spread of business but not in the immediate time after completion of the project. So we have to be very cautious when trying to measure return using facts and figures based on short-term deployment. Luckily, there are already some positive examples of national achievements.

In summary, a national e-Government program is primarily about infrastructure planning and modernization on a national scale. Wanting to achieve irrefutable and quantifiable gains in terms of sustainable development (growth, health, education, and dematerialization) from such a program is often a source of disappointment and the reason for the failure of many such projects.

What would you say are the key motivations for introducing ID solutions?

Each country has its own pace and motivations. Some African countries, for example, want to set the pace for a better infrastructure with more transparency to bring strength into the processes and affirm their commitment to democracy. They want to ensure that those who say they are 'Nationals' are indeed 'Nationals' through setting up a National Register with vital statistics for their populations. It usually starts from there. Once you have such a system there is usually a big push for biometrics to ensure that individuals have their own identity, so that in the future they will have their rights and duties clearly defined.

Something I read in an Indian newspaper a few years ago was a revelation; I saw a portrait of nine people and quotes such as "with this new identification system, I will be able to get buried in a place that is marked out with my name" or "my kids will be able to attend school", "they will even vote." This is such a basic assumption for us here but only made possible in India because of a National Registry! You can also fight corruption and fraud and make documents more secure. Once you have these documents you can help the population and businesses move online. You have not only created a strong physical identity, you also create a strong digital identity. I believe that the state is the best place to leverage this – perhaps working closely with telcos and banks because they also have credibility to exchange IDs and data or making transactions secure.

And it's a basic need for the unbanked.

That's true. This triumvirate between the government, banks and telcos is intertwined within this entire process, with telcos even trying to create their own IDs and spread them within the public sector.

> *"Public Authorities have somewhat unwillingly been caught up in this proliferation of dynamic change in the tertiary economy and personalized services oriented towards the citizen or the consumer.*

Where is France in this process?

France has implemented a smart identification badge for civil servants (Police and Gendarmerie). Electronic signature based on the 1999/93 EC directives is used by many companies in online processes such as TeleTVA.

French health professionals have been using strong authentication for more than 15 years for the SESAM-Vitale process. Over 1 billion claims are dematerialized per year slashing red tape and creating a better healthcare system for all. Banks are using OTP systems, LA POSTE is issuing e-ID based on login/password ... So there are many initiatives.

However, there is currently no National eID or mobile ID framework in place as yet.

Is there a reason for this?

Currently in France the idea of eID is not popular at all – the same was true in the UK – and consequently no politicians will stick their necks out to push this idea through. It is simply not a popular idea. There will be no political return by doing it. But things are changing. The new inter-ministerial organization decided in August 2014 may speed up things.

For the country with the biggest amount of expertise in this field – it must be frustrating.

Very frustrating. But in the country of Descartes, where method is key, a lot has been done for back office applications as pointed out by the 2014 UN study on eGovermnent, where France is now ranked #4 after Korea, Australia and Singapore. With these efficient on-line integrated applications, a robust e/m-ID policy could be a boost for the nation.

For the Silicon Trust, the logical next steps are multi-application and Mobile ID schemes. Would you agree?

It seems that Mobile ID could come to the rescue of National ID programs. That's why many countries are watching very closely pioneers such the Emirates, Qatar, Oman, the Baltics, Scandinavian countries, Korea, Singapore to name a few.

Authorities around the world are very eager to learn how they can leapfrog from their current system to the very latest systems without losing too much money or getting caught up in dead ends.

> *Set the governance framework, the legal framework and encourage operators and banks to work together. This requires vision and courage.*

There is a certain logic that says everyone already has their own phones and the telecom infrastructure exists. This must make things easier for Mobile ID, surely?

This has been said for many years. With Mobile ID, the two first barriers – the reader and the middleware – have already been overcome. And as NFC is backed up by Apple, I clearly see things moving even faster.

So the focus falls upon the process of delivering the Mobile ID and how to leverage the Mobile ID to get clever applications that give you a great service and make administrations more efficient, but also the delivery of new services. This is what I am expecting as a taxpayer from my government.

Who, would you say, are the up-and-coming nations that will do a lot with this topic?

I am surprised by the ambition and means of the Middle Eastern countries. They are spending a huge amount of effort on restructuring their administrations, making them leaner and more efficient as well as delivering new services. They are listening closely to what their nationals want and are looking to see how fast they can make them happen.

South Korea has also started to use their Mobile ID system a few months ago and as you may know, the country has been at the top of the list for Asian eGovernment-based countries for many years. It will be very interesting to see what happens there. Singapore too is a lighthouse for eGovernment administrations.

Scandinavia and the Baltics should also not be ruled out. These countries are set apart by the trust their citizens have in their Governments. They should also not be taken lightly as they introduce more eGovernment services and Mobile ID. There you will find the most innovative applications in the short term.

Thank you very much, Mr. Billiaert. ☒

Securing *financial* operations

By Oliver Winzenried, WIBU Systems

For decades, the conventional way for a corporation to protect its intellectual property has been to patent it. For the inventor, this provides legal protection and it is the basis of many business cases: if others want to use it, it comes at a cost. There is, however, a problem with the patent process: to receive a patent, it needs to be published, which, in turn, makes the idea visible.

"With CrypTA we are able to guarantee a high level of security to protect our intellectual property and can implement a high degree of flexibility in our processes at the same time."

Guido Walther,
Director Technical Support at Wincor Nixdorf

"CrypTA uses various security elements of CodeMeter simultaneously, thus offering the users of the Wincor service platform a convenient and restricted access to service documents with the highest possible security."

Oliver Winzenried,
CEO and founder of Wibu-Systems

Therefore, many companies are keeping their most valuable ideas a secret hidden within the internal systems. This turns these corporate systems into very desirable targets for specialized hackers and organized industrial espionage experts. No one knows how many trade secrets companies keep, or how much they are worth. Some, like customer lists, are generated during day-to-day operations. Others are kept secret because patents typically last only twenty years. A survey by ASIS International, a security-industry body, estimated the annual value of stolen corporate intellectual property at $300 billion in America. Another put it at over $1 trillion worldwide. Once the IP has been compromised, products and ideas are copied, reverse-engineered, and thrown back into the market, causing immense damage to the legitimate proprietor.

Most intellectual property thefts involve insiders. These are typically employees or contractors given access to sensitive information, which they steal via flash drive, mobile phone, or e-mail.

Most intellectual property thefts involve insiders. These are typically employees or contractors given access to sensitive information, which they steal via flash drive, mobile phone, or e-mail. The German company and one of the world's leading providers of IT solutions and services to retailers and retail banking Wincor Nixdorf realized the potential of this threat as early as 2007 and started a development project in order to protect test software and documents in the service environment against unauthorized use. A key aspect of the project was the secure authorization of technical maintenance staff at the company's self-service terminals. Wincor Nixdorf was looking beyond the scope of a standard security solution for software protection, identity, and access control. Access was to be secured via two-factor authentication, i.e. to gain access to the network users must possess both a user ID and the mechanism itself. In addition, the solution needed to be easy to use, flexible, and mobile: one password to start all protected applications, suitable for heterogeneous system environments and for the technicians performing their necessary maintenance applications. In terms of the back office, the security system had to be integrated into existing help desk processes and administered via the Wincor Nixdorf Global Customer Care Center in Paderborn.

The result of the development project was CrypTA (Cryptographic Technician Authentication), introduced in 2009 by Wibu-Systems. CrypTA ensures authorized access to test and diagnostic functions and is based on a USB dongle, which is used essentially in the same way as a key.

The basic technology for document encryption is the password protection function of the PDF document, which is included in the Adobe offering. Within CrypTA, the password is part of the key with which the document is saved. The critical point is the password: too simple and it can easily be hacked or phished; too complex and the password becomes hard to type and remember. In either case, it can be passed on to others. For these reasons, CrypTA uses password protections only for a few selected documents and to a limited extent. With the vast amounts of documents that need to be generated, accessed, and distributed, Secure Key Management is vital. Within CrypTA this is solved with a plug-in for Adobe Reader and Acrobat. The CodeMeter stick, distributed to every service technician, is an award-winning solution containing the most powerful encryption algorithms in combination with a smart card chip where the encryption keys are stored, away from all types of local and remote attacks. This way the technician only has to remember one individual password – the one that accesses his CodeMeter dongle.

Within CrypTA, the password is part of the key with which the document is saved. The critical point is the password: too simple and it can easily be hacked or phished; too complex and the password becomes hard to type and remember. In either case, it can be passed on to others.

After five years and with the experience of running such a successful system Wibu-Systems and Wincor Nixdorf have come to a point where they want to share their know-how in this field. Both companies are expanding their long-term collaboration and are now offering their respective expertise in the area of Digital Rights Management, IT Services and Service Desk solutions to the international market. Possible target markets are banks, manufacturing companies and suppliers, everybody that has know-how worth protecting. ☒

NEW perspectives for eID & *financial* INCLUSION

By Frank Schmalz, Giesecke & Devrient

The status quo of financial inclusion is a large, international problem with two thirds of adults in most developing countries having no access to formal financial services. Globally, 2.5 billion and 76% of the population in sub-Saharan Africa are unbanked with no possibility to receive micro credits, insurance or securely store personal savings. The national economics in the affected countries still largely depend on cash and struggle with the accompanied drawbacks of fraud, corruption, black economy and operation costs. Many emerging and developing countries have acknowledged the importance of the problem for bringing stability, wealth and perspectives to their countries' citizens. National eIDs with payment functions can offer secure and efficient infrastructure schemes to support these efforts and to overcome many of the challenges.

Financial inclusion is at the core of many regional development projects. For example, The Hunger Project's Microfinance Program in Benin addresses a critical missing link for the end of hunger in Africa: the economic empowerment of the most important but least supported food producers on the continent – Africa's women. The picture shows Louise Lagni from Zakpota, who, after attending workshops, now consults fellow-villagers and is the leader of the women's credit group. Together, they have taken out a loan at the Credit Bank, which is divided to finance their income-generating activities.

© The Hunger Project

> With match-on-card, the biometric feature never leaves the card and can serve as identification means in online and offline scenarios. This special characteristic of match-on-card and the fact that the biometric feature is only accessible by well trusted government institutions storing this information in well protected and offline vaults, could be the general enabler for biometric in payment applications.

In an attempt to significantly increase the unsatisfactory level of financial inclusion, 35 central banks of the world's emerging and developing countries committed themselves to financial inclusion programs in 2014. These international efforts and resulting frameworks are overdue and highly commendable. However, many of the affected countries are struggling to finance changes in the systems. Tax income is low due to corruption, shadow economy, organized crime and inefficient tax fraud investigation.

Cash, of course, is still the number one payment method in developing countries throughout the world. Cash is extremely flexible, however vulnerabilities are apparent: Corruption, black market transactions, illicit commercial activity and organized crime all feed off the traceability of cash badly damaging the country's economy. Billions of dollars are lost every year. It is this money that could be used to change the nature of the financial infrastructure and make it accessible to as many citizens as possible.

A shadow economy requires cash to prosper. The most efficient way to counter this hidden sector of the economy, where private cash transactions go unreported, is the increase of electronic transactions. (Fig. 1: Shadow Economics and Electronic Transactions). This is especially applicable to developing countries, where the poorest of society are both marginalized because they don't have access to financial services and, at the same time, exposed to existential risks of losing their cash savings, be it through natural disaster or crime.

In 2012, David Wolman, editor at Wired magazine, writes in his book The end of money Counterfeiters, Preachers, Techies, Dreamers – and the Coming Cashless Society: "Although predictions about the end of cash are as old as credit cards, a number of developments are ganging up on paper and metal money like never before: mistrust of national currencies, novel payment tools, anxiety about government debt, the triumph of mobile phones, the rise of virtual and alternative currencies, environmental concerns, and a wave of evidence showing that physical money is the most harmful to the billions of people who have so little of it."

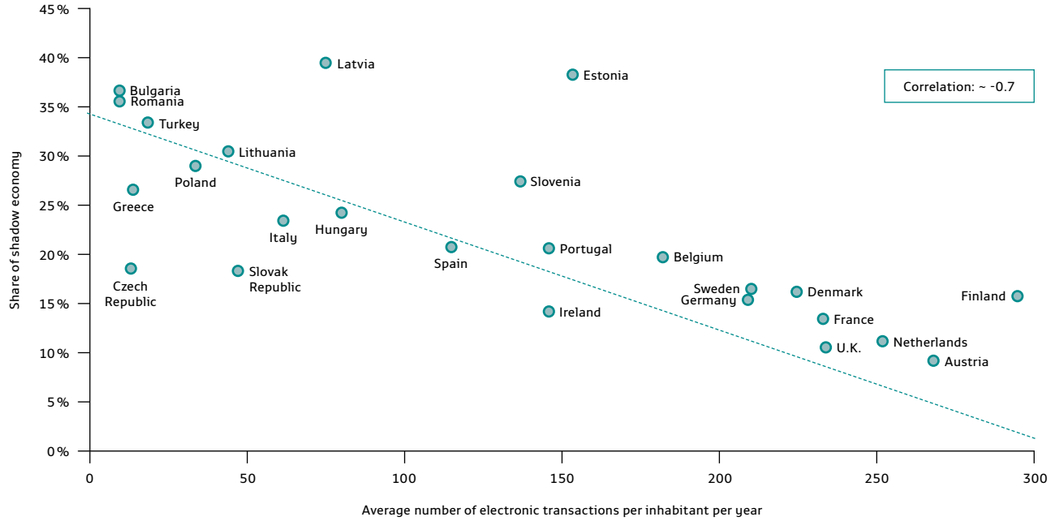
The introduction of a comprehensive electronic payment and transaction infrastructure has been an essential tool to improve law enforcements related to financial crimes in developed countries. Electronic transactions can be verified and traced, providing a solid basis to combat corruption, organized crime, tax evasion and fraud. Emerging countries, especially, suffer from fraud in the health and welfare system due to the cash nature of these systems. Fraudulent collection of salaries or welfare benefits due to dual employment and phantom jobs can pose a serious financial threat. Dual employment occurs when a person holds two jobs in the public sector, both civilian and military, while non-existent individuals hold phantom jobs, created by others to earn additional income, or by individuals who do not perform their duties but receive salaries.

Electronic transactions can be verified and traced, providing a solid basis to combat corruption, organized crime, tax evasion and fraud.

Electronic payment schemes are an efficient way to make financial transactions traceable. However, it does not solve the problem of multiple or false identities. Governments try to force financial institutions to thoroughly identify their customers. They are imposing Know Your Customer rules (KYC) and financial regulation laws, however, these actions are bound to fail without the means for reliable identification.

Reliable Identification requires nationwide registration and enrolment of citizens followed by biometric deduplication. The deduplication process compares a biometric feature, like a fingerprint, with the same biometric feature of all other registered citizens. This identifies fraudsters trying to apply for more than one official identity.

Deduplication has to be done on a nationwide level and is therefore unavailable to private companies like banks. Obviously, private companies are usually in competition with other companies. A fraudster would just have to apply for two accounts under different names in different companies. The companies have no means to identify this scam since customer data exchange with another bank often constitutes a privacy rule violation.



Source: The Impact of Electronic Payments on Economic Growth, Moodys Analytics

Nationwide registration and enrolment of citizens is typically done in a national identity card project resulting in the issuance of a national identity card which serves as government approved proof for one single identity. Countries with properly carried out national identity card projects resulting in high quality documents, have significantly less problems with false identities, multiple identities or identity theft.

Countries with properly carried out national identity card projects resulting in high quality documents, have significantly less problems with false identities, multiple identities or identity theft.

Nations with identity cards provide the right tools to comply with 'Know Your Customer' rules – what remains is the ability to check the document. Thorough training of clerks is required to avoid false identities based on fraudulent documents. Combining national identity cards with payment features move this task from the private company clerk with sometimes questionable training and motivation to the public officer issuing the national ID card. In addition, this officer can be equipped with biometric identification solutions at issuance.

But missing reliable identification means are not only a problem of financial institutions having to fulfil government rules. Governments are suffering terribly from fraud in the health and welfare systems. The lack of identification means is exploited by people keeping up benefit payments for deceased relatives, redirecting disbursements or stealing benefit checks. When used for disbursement schemes, biometrics verification ensures that people are still alive when they receive payment and that they are the valid beneficiaries.

South Africa is a prominent example of potential. The country has been able to reduce social benefit fraud by 186 million dollars with the introduction of biometric checks.
In addition, the use of benefit checks or cash in government disbursement schemes produces significant operation costs. Service, support and security are major cost drivers. Electronic IDs with debit payment functionality can serve as reliable targets for disbursement payments. With the introduction of an electronic system for social benefits disbursement, the US were able to save 1 billion dollars in ten years.

Critics claim that the introduction of electronic payments in developing and emerging countries is missing the target. People are not used to these systems and many are illiterate. For sure, improvement cannot be achieved without change. And this of course includes adapting to new technologies. The important challenge is to make the transitions possible. Fatai Amoo, head of Sterling Bank Plc, Nigeria said: "We have over 30 million adults who are unlettered and whenever they want to use their ATMs they would tell anybody around their PIN. We all know that, that is risky and a lot of people have fallen victim."

Biometric ATMs have been rolled out, for example in Japan.

In the past, the financial industry has been interested in introducing biometrics as account holder identification. Apart from addressing the mentioned challenges of illiteracy further benefit would be the reduction of fraud and service costs due to stolen or forgotten PINs. However, implementation had been proved difficult due to people's reluctance to give biometric information to private companies, the protection of this information is a hassle for banks and the proper enrolment is a huge investment.

These are the challenges that have to be addressed. Some developing countries already started by introducing biometric enabled ATMs connected to biometric background database systems. These ATMs can be accessed without PIN and just by biometric identification. The solutions require online connectivity and pose a certain risk of proliferation. A successful hack of such a database would make the future use of this biometric feature impossible. Again national eIDs could solve this problem by providing match on card capabilities usable to the payment systems. With match-on-card, the biometric feature never leaves the card and can serve as identification means in online and offline scenarios.

This special characteristic of match-on-card and the fact that the biometric feature is only accessible by well trusted government institutions storing this information in well protected and offline vaults, could be the general enabler for biometric in payment applications.

In many developing and emerging countries mobile payment solutions are on the rise leaving the classic Point of Sale (POS) and ATM centered electronic schemes behind. These solutions have significant advantages when it comes to deployment and usability. However, certain challenges discussed in this article cannot be addressed by these systems. The most prominent would be the issue of reliable identification. The eID with payment functionality can serve as the identity seed to these systems. Combining eIDs and mobile payment solutions would lead to a perfect match of secure and user-friendly electronic payment systems.

Payment enabled identity cards provide a bank account for every citizen to push financial inclusion, a verified target for government disbursement payments, biometric identification capabilities to counter fraud and can serve as an enabler to push the development of cashless transactions bringing its benefits to governments and citizens. These multi-application cards go beyond the topic of reducing the amount of cards issued. The combination enables new use cases not available to multiple single application cards.

The eID with payment functionality can serve as the identity seed to these systems. Combining eIDs and mobile payment solutions would lead to a perfect match of secure and user-friendly electronic payment systems.

However, the implementation of such a solution is still a daunting task. Payment enabled identity cards have been in discussion for many years. The problems arising from bringing privately owned financial institutions together with public authority driven national identity programs, as well as the different technical specifications and concepts, have been preventing successful implementations for a long time. Recent developments and pilot projects have started to overcome these problems. Reliable, trustworthy and competent partners, being aware of the requirements from both payment and ID projects are required. Drawing on years of expertise in the government and financial sector, Giesecke & Devrient is able to provide turnkey solutions to the individual needs of our customers. Thanks to these cross-industry insights, we have carved out a unique market position – as a trusted trailblazer and dependable partner that is able to combine best case approaches from all our markets. ☒

The WORLD
looks to *NIGERIA*.

And *to*
GELSENKIRCHEN.

By Silicon Trust

There was a strange occurrence in the western German city of Gelsenkirchen in the summer of 2014. A Nigerian delegation in company of their German partners got visibly emotional. Bystanders would have seen that they were holding Euro notes from a local ATM. Also noticeable would have been the pride in the faces of the whole group. The reason? A Nigerian citizen had just used a German ATM using his new multi-application identity card. It was, on many levels, an outstanding moment.

☐ It is no coincidence that this event would take place close to the headquarter of cryptovision, one of the leading providers of secure electronic identity and digital information protection solutions. Founded as a spin-off of Essen University, the company specializes in modern cryptography methods and public key infrastructures (PKI) for government authorities and private commercial sectors. cryptovision was commissioned by the German Federal Office for Information Security (BSI) to participate in developing the EAC (Extended Access Control) standard for electronic passports and played a key role in this project.

Beyond Germany, cryptovision also has a growing influence and continues to buck the trend of the international ID market looking for alternatives to turnkey solutions by a single vendor. Especially in emerging and developing countries, governments and their agencies are starting to invest in national IT expertise to reduce later dependency from outside system integrators and the associated costs. Small and flexible experts, such as cryptovision, working in different consortium constellations, are able to work onsite and with the national teams to help them achieve this objective. The company has developed products that attract high international demand, such as cv act ePasslet suite, a comprehensive collection of applications for sovereign electronic documents and the PKI software CAmelot. Cryptovision's products are integrated, for example, in the eID card schemes of Rwanda and Armenia and electronic passports of Moldova and Ecuador.

And Nigeria. With over 170 million inhabitants and more than 250 ethnic groups, Nigeria is the most populous country in Africa. Sometimes referred to as "The Giant of Africa", Nigeria made some rather large waves in the international ID community this summer. After several years of preparation time, the National Identity Management Commission of Nigeria (NIMC) launched the first national electronic identity card with a payment application, representing one of the most comprehensive multi-application ID deployments worldwide.

At the end of August 2014 the first residents of Nigeria received their copy of this multifunctional eID document, a contact-based (as opposed to contact-less) polycarbonate smart card, with a form factor similar to a traditional credit card. To make the card usable, a sophisticated eID infrastructure had been deployed, including registration authorities, identity management systems, and secure card production facilities. Mobile devices for enrolling, reading and even updating some data stored on the card will be added to the infrastructure components.

In the first phase, the Nigerian eID will be used for three applications: as a proof of identity, for digital payment (based on the EMV standard), and for digital signature with biometrics. With this truly innovative concept, the Nigerian eID is the first national project in the world that combines eID functionality with a payment system. To facilitate financial inclusion in the country, this feature gives millions of Nigerian citizens first time access to electronic payment. In the next project phase, the functionality of the national eID card will be extended to support additional electronic applications, like driving license, health information card, tax record and voting. Other technical aspects of the Nigerian eID project are impressive as well. With full card issuance, it will represent one of the largest and most complex Public Key Infrastructures (PKI) deployed worldwide. This PKI is comprised eight certification authorities and will issue over 300 million certificates. This infrastructure is necessary to protect the eID system and the card itself from hacker attacks. The various applications that run on the Nigerian eID card have been implemented with Java Card technology. This open standards-based approach delivers a high level of transparency and independence for the customer. In addition, the modular architecture easily enables future extensions and changes. A new card profile was developed especially for the Nigerian identity card in order to support this functionality. Within this framework it was possible to implement such a large range of applications on a single smart card.

And Gelsenkirchen? Well, all aforementioned core software components (PKI, card applications, and smart card middleware) in the Nigerian eID scheme are delivered by cryptovision, acting as key part of a consortium consisting of leading technology companies. "We are thrilled that our entire solution range is applied in this unique project. We are also greatly indebted to NIMC because they are not only a reliable partner, but also have the expertise and courage to implement such an innovative approach." says Markus Hoffmeister, CEO, cryptovision.

"An excellent mixture of international partners and clients. The Mindshare 2014 agenda did not only focus on the technical aspects, it went further to give insights on what happens when the technological concepts are actually applied."

Dr. Kim Nguyen, Managing Director, D-Trust

Sharing, caring, learning – Mindshare 2014

During the 2014 cryptovision summer event "Mindshare", the Nigerian delegation was part of large group of clients, partners and employees. In front of a full house of ca. 120 attendees from over 15 countries, the keynotes of the first day included Kim Nguyen's explanation of FIDO and it can help to bridge authentication and identification. Markus Hartmann of HJP Consulting presented an overview of ICAO, which was especially topical, as the he had just returned from the EC-initiated ICAO Interop test that had taken place in Madrid the week before.

The second day delivered some excellent insides into some of the upcoming ID projects including Estonia, Austria, Ecuador, Nigeria and Ghana. Many Silicon Trust Partners were present, including Trueb, Giesecke, Identive and many more. Highlights were the presentations be the Ecuadorian on lessons learnt from past mismanage as well as the presentations by Merecedes Jativa and Xavier Pazmino of IGM.

Delegates were invited, weeks before the official announcement, to get some firsthand information from Barr. Chris 'E Onyemenam, Director General of the Nigerian NIMC, on the Nigerian eID project and from Moses Baiden and Sanjay Patel on the developments in Ghana.

"Mindshare 2014 presented weighty security topics in a very light wrapping. Its unique how all attendees, including the international VIPs, aren't brought to a 5* hotel but at the end of the day join into a family and friends cryptovision summer festival."

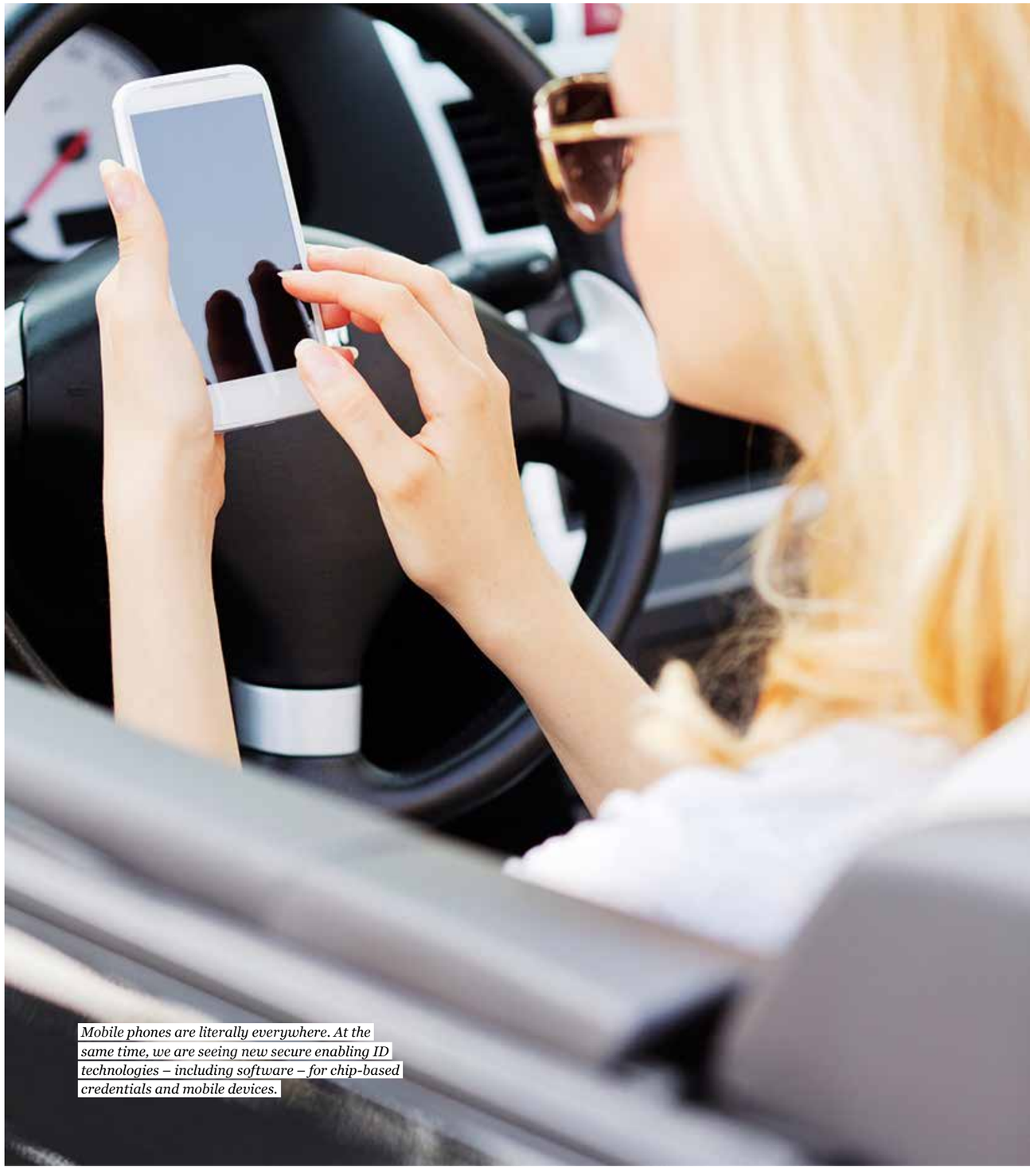
Markus Hartmann, CEO, hjp Consulting

So, the content was there, the right people, interesting topics but it was the Sommerfest at the end of the first day that gave the Mindshare 2014 event its special flair. The weather turned out to be glorious and the mindshare delegates were joined by the friends and family of cryptovision on the vast company grounds which were transformed by the man in charge, Lutz Feldhege, to resemble a cryptovision summer festival, with bouncy castle, BBQ, live music and oversized lounge chairs. The atmosphere reminded the delegates that, after decades of working in the same area, on the same projects and often in and out of the same companies, they too are a kind of family, albeit a very dysfunctional one at times. ☒

Mobility fuels ADOPTION of multi-application *eIDs*

By Rob Haslam, HID

For years we have been talking about the increasing use of multiple technologies in major government-to-citizen-ID programs to address a growing array of applications and services. As the applications have increased so has the sophistication of the technology. Looking ahead to 2015 we anticipate a number of trends impacting the use of multi-application, multi-technology ID cards. According to Gartner, Inc. innovation in the government sector is being driven by four powerful forces: social, mobile, cloud and information. In this paper we will focus on the trend toward mobility and related innovations in government-to-citizen-ID programs.



Mobile phones are literally everywhere. At the same time, we are seeing new secure enabling ID technologies – including software – for chip-based credentials and mobile devices.

While mobile phones and readers are increasingly present in commercial transactional environments such as renting cars, retail shopping and ticketing, large scale mobile applications have been far more limited in Government ID programs. However, the tide is changing. The first signals of a paradigm shift are here.

Innovations in mobile ID technologies are beginning to emerge allowing secure identification and authentication as well as instant access to critical information. The strategic adoption of secure mobile eID applications may be found first in less mature markets where mobile phone usage is extremely high, and government-to-citizen ID programs have been transitioning to electronic IDs (eIDs) for some time.

Historical perspective: The evolution of multi-application, multi-technology eIDs

Over the past five years, governments around the world have made a dramatic shift to national eIDs. Two imperatives have led this shift from static paper IDs to multi-application, multi-technology eIDs:

1) the need to provide effective defenses against large-scale forgery attempts; and
2) the opportunity to take a holistic approach to solving national ID challenges.

According to Acuity Market Intelligence, by 2018, 127 countries will be issuing 740 million national eIDs annually. Approximately 3.5 billion people, nearly half of the world's population, will have a national eID card. The success of these programs will be measured by the degree to which they are adopted and utilized within the context of country specific objectives. While some programs are as basic as creating a secure, forgery-resistant voter ID card, increasingly we are seeing complex, multi-application national eID programs. With regard to the latter, these programs are leveraging the latest technology innovations and provide the greatest return on investment.

Heightened security concerns, high traffic border crossings, and growing requirements for streamlined government services delivery are just some of the factors influencing this change. Governments and national organizations are now increasingly likely to leverage National eID programs as an opportunity to increase efficiency as well as protect and ensure the identity of the holder. This has given rise to projects calling for powerful multi-purpose ID credentials that operate on many levels, maintaining the highest levels of security while addressing additional objectives such as entry to secure facilities, faster border crossing, or access to health, education and other social services.

Mobility: Driving innovation in Government-to-Citizen ID programs

Mobile phones are literally everywhere. At the same time, we are seeing new secure enabling ID technologies – including software – for chip-based credentials and mobile devices. Governmental organizations will finally be able to reap the rewards of mobility (flexibility, real-time access to information, confident interaction with citizens) and multi-function ID, while reaching the required levels of security and updateability for confident ID authentication. These innovations are particularly helpful to government agencies out in the field such as the police and border control.

One such example is the Nigerian National Police which has embraced the latest innovations in mobility to improve the security and effectiveness of the government's vehicle registration program.

The Nigerian National Police Force

Nigeria has a huge population of 170 million people (nearly 1/4 of Africa) with an estimated 50-60 million vehicles on the road. The challenge is found in the fact that one organization – the Federal Road Safety Commission (FRSC) – collects driver and vehicle data to issue drivers licenses and vehicle documents while another organization – the Nigerian Police Force – monitors and protects drivers and vehicles. The information collected by the FRSC is not sufficient or readily available to the police out in the field.

To remedy this situation, the Nigerian Police adopted a mobile Biometric Central Motor Registry (BCMR) to provide real-time access to biometrically verifiable information plus ongoing access to accidents/crimes. Currently in its pilot phase, the BCMR has the potential to be the most advanced vehicle registration program in the world. Vehicles and owners are now being registered into a biometric central database and issued a biometric RFID credential. When an officer approaches a vehicle, he/she can use the card's most advanced visual security for a confident visual check, plus leverage the secured data storage that allows the Nigerian Police to access all credential and accident information in real-time via a handheld mobile device.

At full deployment it is expected that the police will have more than 10,000 mobile readers distributed nationwide. With the advancements made by HID the next generation mobile reader could be your smart phone. Using smart phones as readers can significantly reduce infrastructure costs – by an estimated $10M-$15M.

The secure and timely issuance of cards will be a secondary, but nevertheless important aspect of the program. Each organization will benefit from the more cost effective use of a shared infrastructure for encoding and printing. This shared infrastructure will be able to issue more sophisticated RFID cards that include highly advanced visual security features.

In addition to improved communications and security, the new approach to vehicle registration will also help prevent car theft, provide forensic evidence and be a tool in the growing fight against terrorism. Looking more broadly at the world, new mobile operating systems are enabling agnostic ID authentication and security for truly integrated, multi-functional secure mobile programs.

Real-time communications has resulted in improved security and government effectiveness plus significantly reduced infrastructure investments in the long run.

What's next?

Beyond the four forces identified by Gartner as driving innovation – mobility, social, cloud and information – advancements in materials, manufacturing processes and issuance systems are also paving the way for increased adoption of multi-application eIDs worldwide. In addition to providing higher levels of security and functionality, these more sophisticated systems also deliver an increased return on investment for governments. At the same time, such advancements enable the delivery of more efficient and convenient services for cardholders. General technology trends, including the growing use of mobile devices, software as a service, and access to the "cloud" by individuals will continue to drive innovation and increasingly "citizen-centric" programs. ☒

A SOUND platform for GOOD IDEAS

Society has never been as networked, as flexible nor as mobile as it is today. We can delve into a sheer endless world of information, no matter where, no matter when. In just a short space of time, smart phones, tablets, etc. have permanently changed how we interact and consume. But users who fail to protect their data can quickly fall prey to fraud and misuse.

By Antonia Maas, Bundesdruckerei GmbH

Almost every day we hear news of data theft and misuse. Attacks are not only increasing, they are also becoming more intelligent. These developments affect both private individuals as well as companies and governments, as demonstrated by information regarding NSA activities leaked by Edward Snowdon.

Computer crime has been a billion dollar business for some time now and is considered to be today's scourge of mankind. According to the German high-tech association BITKOM, 2013 saw a sharp rise in the number of officially reported cases of computer sabotage and extortion of Internet users. Following a temporary decline, phishing has returned with increasingly more sophisticated methods. Cecilia Malmström, European Commissioner for Home Affairs, estimates that one million people fall victim to crimes like these every single day around the globe. According to the European Commission, the resultant damage world-wide amounts to around 290 billion euros annually – and the trend is growing. Cybercrime has now become more lucrative for criminals than trading in drugs, explains German IT expert Arne Schönbohm.

Dr. Michael Littger,
CEO of Deutschland sicher im Netz e. V. and member of the eIDEE jury

> What we can see is that IT security – and that also means security of the digital identity – can fail if demands on users are too high. I am convinced that innovative ideas for smart management of identities are the key to greater convenience and can hence pave the way for greater IT security. With this in mind, I expect eIDEE to deliver innovative and realistic ideas for practical application.

Identity theft is lucrative

Criminals usually attack digital identities and personal data using Trojans which they place unnoticed on computers. They sell their haul via the virtual marketplaces of the underground economy. For 2011 alone, Spanish IT consultancy firm PandaLabs counted around 50 online stores for illegal trading with electronic identities. According to the Norton Cybercrime Report by software supplier Symantec, 90% of data theft is already directly committed by criminal bands.

It is still extremely difficult to put a stop to identity thieves. Almost a third of those polled for the above Symantec report stated that their case had not been solved. From invoices for goods that they did not order to entries of debt with the Schufa credit rating organisation right through to arrest warrants for crimes which they did not commit – the consequences for the victims are serious. On average, these victims of online crimes had to invest 28 days and 250 euros in order to deal with the consequences of their identity theft.

With initiatives like the European Union's Cybercrime Centre, governments are now bundling forces in the fight against online fraudsters. But in order to pull the rug from under their feet, Internet users will have to act and protect their computers as well as they can against attacks from the net, for instance, by being more careful before disclosing personal data. According to a media use survey by BITKOM, almost half of all Germans published personal data on social networks in 2011 even though these forums are a veritable goldmine for identity thieves.

There is now growing awareness among citizens and companies with a view to data protection and security for communications and identities. Terms such as cloud computing, smart living, smart grids, M2M communication and NFC are becoming household words. However, preventive measures, greater care, regularly changed passwords and an anti-virus program on smart phones are not enough when it comes to reliable data protection. Doubt-free proof of identity is the only way to ensure effective protection against fraud in the online world. Trust is the foundation for secure transactions – both in the analogue and digital world. But how can optimum protection be achieved?

The first good ideas – beyond user name and password – are already available today, like fingerprint iPhone access, voice-activated door opening or payments using biometric facial recognition. But if we are to be able to pay, shop, sign and communicate online in a secure manner, we need concepts that work quickly and in just a few steps, that can be operated intuitively, do not cost the earth, are available everywhere and can be used in mobile systems. These technologies must mean added security and they should work in such a way that the user hardly notices the underlying processes.

More than e-mail encryption

Three years ago, Bundesdruckerei came up with the idea of not just gathering experts together to work jointly on implementing solutions, but also to ask users for their ideas. This led to the "eIDEE – Contest for the Digital Handshake". Today, the measures needed to protect the secure identities of individuals, objects and processes involve much more than just encrypting e-mails or securing IT infrastructures. That's why Bundesdruckerei's eIDEE Contest is an appeal to think about the integration of secure identities into digital processes.

The winner of last year's eIDEE Contest was POLYAS GmbH. This company offers online election solutions for non-profit organisations and educational institutes. The idea of using the online ID function of the German ID card to enable even more secure and anonymous elections over the Internet impressed the jury in autumn 2013. "POLYAS eID" is now undergoing intensive testing on the reference system using test ID cards. As soon as this phase of testing has been completed, the system will go live. "POLYAS eID" together with the German ID card should then enable greater co-determination and promote direct democracy, for instance, through referendums or opinion polls. "Digital participation via the Internet is a useful and future-enabled means of reducing political disenchantment and of improving participation in the opinion-making process. Today, POLYAS is already a good supplement to traditional postal voting which is much more expensive and prone to error," emphasizes Amita Sarup, Project Manager at POLYAS, during the 2013 award ceremony in Berlin.

The competition is being held for the third time in succession

Up until 5 October 2014, this year's applicants were once again able to submit their ideas, concepts and projects related to secure and user-friendly identity management in the digital future. "This issue is very diverse, topical and literally crying out for innovative solutions," says blogger Falk Hedemann writing about the competition. For blogger Cornelia Dietrichs, eIDEE offers a huge benefit "because it allows a certain amount of participation in the shaping of our future". During a celebratory award ceremony in mid-November in Berlin, a jury of eight headed by Professor Dr. Thomas Schildhauer, Director of the Institute of Electronic Business (IEB) at Universität der Künste Berlin, is to choose the winners in five categories:

The best entries from companies and start-ups will receive material and consultancy support to implement the idea. The winner of the secure identity prize for private individuals will be chosen by the audience. Students are to draft creative contributions on the subject: "What will my identity look like in 2034?" and the winner will receive a company traineeship and 2,500 euros for their school class. Under the motto "Identity tomorrow – a secure and simple life in the digital world", designers can submit concept work, such as interface and interaction concepts, designs, prototypes and products which form a bridge between design and technology. 2,500 euros will be awarded to the best work which will be on show during the award ceremony in November.

Lena-Sophie Müller,
CEO of Initiative D21 and eIDEE jury member

> For users, security must be a matter of course – it must be second nature. The applications have to grow in line with technical progress while the German ID card – and even perhaps identities too – will have to be "mobile ready". The aim must be to reduce the complexity of systems and to integrate security in an almost playful way – above all, on mobile devices too. I hope that the eIDEE Contest will pave the way for these kinds of applications. We need a kind of "one-click security" which will not bother people with technical terms and processes. Instead people should be able to immediately recognise the benefits offered by this and load security as easily as an app.

Professor Dr. Thomas Schildhauer,
Director of the Institute of Electronic Business e. V. (IEB)
at Berlin's Universität der Künste and
chairman of the eIDEE jury

> German start-ups already have considerable innovation capacity. But many good ideas are never developed to full maturity in Germany because often one important condition is missing, for instance, money or skilled staff. The innovation process could be stepped up if Germany's traditionally closed innovation processes, i.e. the closed shops, were opened faster and ideally already during the development process. Really good innovation ideas need a certain stickiness factor. It is vital that they fulfil a "must-have" function, generate real benefits and are fun. Pricing, performance and quality have to be right and should not disappoint.

Users often have the best improvement ideas

With this year's new categories, Bundesdruckerei is aiming to make more people aware of the important topic of identity protection. We are convinced that good ideas already exist and want to be heard – a fact that was confirmed in previous years' competitions. Start-ups are often founded because they have a great idea. Private people discover gaps when they surf on the net. Company employees work in their field on special topics and they can easily make specific proposals for improvements. This year's student prize is explicitly designed to make the next generation of Internet users more aware of this topic. The designers are to contribute new perspectives with a view to design, for instance, for processes, applications or apps.

Incentives for one's own work

Greater security with the same convenience – that's what Internet users want for modern online structures. The innovation department at Bundesdruckerei is also working on possible scenarios for the future in order to create solutions for this. For years now, the company has been recognised the world over as an innovative force in the Secure ID industry and is pursuing innovation through around a dozen co-operation projects with scientific institutes. Dr. Ivonne Scherfenberg, Innovation Developer at Bundesdruckerei, is currently working on the Trusted Service Platform which provides different security levels as required in a multi-level concept. Service suppliers and Internet users can thus reduce the risk of misuse. "We hope that the eIDEE Contest will also provide momentum for our innovation work: We can envisage very good ideas from start-ups which supplement our platform as a technology partner. Or also application partners who wish to connect to our platform in order to offer their services. We are, of course, always looking for innovative applications which make life simpler for Internet users, especially with a view to user-centric innovation," Dr. Scherfenberg explains her expectations for the contest. ☒

ABOUT THE eIDEE – CONTEST FOR THE DIGITAL HANDSHAKE

With its eIDEE – Contest for the Digital Handshake, Bundesdruckerei GmbH is searching for innovative ideas in identity management. eIDEE addresses companies, start-ups, institutions, private individuals, designers and students. The contest has the backing of numerous partners (biw Bank für Investments und Wertpapiere AG, Design Research Lab, Deutschland sicher im Netz e. V., e-commerce Magazin, Fraunhofer "Next generation ID" innovation cluster, Initiative D21 e. V., Institute of Electronic Business IEB, Project A Ventures und Verein Sichere Identitäten Berlin-Brandenburg e. V.) and supporters (blau Mobilfunk GmbH, Fraunhofer FOKUS Institute, Fraunhofer Institute for Reliability and Microintegration (IZM), ReinerSCT and TeleTrusT – Bundesverband IT-Sicherheit e. V.).

NEXT Generation *Contactless* eID CARDS

By Christian Wagner, Smartrac Technology Group

☐ In order to support the next generation of highly secure and durable contactless eID cards, the inlay industry is facing new fundamental technical challenges. The main drivers for Research and Development in this regard are dedicated to meet the following major requirements:

- Provision of a 10-year lifetime functionality in the field
- Integration of enhanced security features and components
- Support of the highest possible field strength and data transmission performance on different frequencies
- Prevention of micro cracks especially in brittle materials like polycarbonate
- Easy handling of chip transponder inlays and pre-laminated inlays during card production processes
- Provision of incorporated security features preventing fraud and counterfeiting.

Consequently, the inlay generation of tomorrow has to provide utmost ultrathin, durable, flexible and flat product characteristics.

SMARTRAC's Product Family SMART-SL (SLIMLAM)

In order to meet these targets, SMARTRAC's new SMART-SL product family provides a reduced inlay thickness of 200µm with a homogenous flat inlay surface. SMART-SL utilizes SMARTRAC's unique wafer processing and chip die bonding technology. The robustness of the assembly is assured by a special in-house wafer process, granting the grinding, dicing and bumping of the chip dies at the highest standard. Thereby, the chip die reliably bonded to the CCL-carrier receives complete flexibility and stress resistance enabling a 10-year lifetime. Conventional packaging technology is made completely obsolete where traditionally the chip module is the major alien element in the card material environment causing the limitations to the possible inlay dimensions today. Moreover, the flat and homogenous surface of the SMART-SL assembly prevents the application of stress to the ambient card material in the chip area. So, the root cause for the appearance of cracks due to the wear and tear of the card material is eliminated.

As the SMART-SL chip inlay takes up only very little space on ID-1 cards, customers have more flexibility on the card body and can incorporate modern card security features like optical variable devices, threads, hidden core printing or others. The rising trend of multi-application cards also increases the need for space on the card, for example for additional features such as displays, number pads or buttons for One Time Password (OTP) applications or for the visual display of specific document bearer's data, such as the current living address.

Further aspects are the specific requirements of eID cards in the area of data storage and data transmission performance. The former being based on the requirement to store all document master data like bearer's name, birth date, issuing authority, issuing date and validity data but as well the Machine Readable Zone (MRZ), electronic certificates, and last but not least biometrical data as fingerprint images with 15 kilobytes per finger and the facial image with approximately 20 kilobytes.

The data transmission performance is a prerequisite to enable border crossing transactions reliably and at the highest speed possible. So, as state-of-the-art the standard transaction speed of eID reader devices and documents is supporting 848 kbit/s at present. However, current developments in the industry already prepare for a reading performance of contactless transactions of more than 5 Mbit/s. This implies highest physical challenges to the antenna technology as well. In order to be prepared for these developments, SMARTRAC's SMART-SL family already today uses a patented copper wire embedding antenna technology providing the highest reliability and best ISO resonance frequency characteristics of the antenna for eID applications. This performance is available for all applicable frequency ranges used in the eID segment.

eID documents commonly operate at high frequency (HF) which is outlined in ISO standard 14443. Ultra high frequency (UHF) is a standard emerging especially in Northern America for driving license cards or border crossing and residence permit cards.

Requirements of Next Generation Dual Interface eID Cards

In regard to dual interface cards, the requirement of a 10-year lifetime has not been sufficiently addressed since eID applications demanded this technology for the first time. Especially the connection of the dual interface module to Radio Frequency (RF) antenna for the contactless interface has been always the weak point.

SMARTRAC has developed a new manufacturing process in order to meet the physical durability demands of dual interface eID cards. The overall solution consists of the SMART-HERA® machine for implanting the module and a special SMART-HERA® inlay based on SMARTRAC's copper wire embedding technology.

Key values of the SMART-HERA® solution are

- 10+ year durability for high security eID cards (PVC, PC, Composite)
- No ageing of sensitive materials like flex bumps or conductive glue due to a soldered metallic interconnection between module and antenna pads
- Best resonance frequency performance due to proven wire embedded inlay antenna
- Highest assembly yield rate of the SMART-HERA® machine
- Low consumable costs

As a first step of the value chain, SMARTRAC provides PVC, PC or composite PRELAM® sheets to the card manufacturer who can laminate additional layers on to the pre-laminated sheets before punching out the cards. The PRELAM® contains the proven embedded SMARTRAC copper wire RF antenna which is connected to copper pads at its ends.

It is quite obvious that applications in this segment demand the highest level of data storage capability and data transmission performance.

The single cards are placed in stacks for fully automated dual interface module implementation by the SMART-HERA® machine. To begin with, the module cavity is milled with high precision. During the next step, the dual interface module is connected to the pads of the embedded antenna. The applied technology is based on a soldered wire connection between the antenna and the chip module contacts. This metallic interconnection guarantees very high stability against mechanical stress and also long-term bending and torsion durability. Finally, the module is cured in the cavity by means of a hot press station. Quality assurance options, like antenna continuity test, ATR- test, ATS- test, an electrical parameter test and an optical inspection, can be offered upon request.

Beside the business of selling the SMART-HERA® machine and inlays, SMARTRAC today has installed SMART-HERA® implanting services in three high security facilities around the globe. This enables customers to use the SMART-HERA® solution for qualification purposes, ramp-up volumes or projects with a lower volume of cards. ☒

eID – KEY ENABLER for *eGovernment*

By Urs Fawer, Trüb

The success of electronic governmental programs depends, amongst others, on the trust in and availability of digital identities. The eID, as the classic electronic identity document, can be seen as a key element in this context. This article also introduces alternative solutions based on mobile phones or tablets, which are becoming more and more popular. For illustration purposes, Estonia is presented with its leading position regarding eGovernment. In Estonia, citizens and residents can access more than 700 eServices with their eID and, alternatively, with a mobile ID.

The Prime Minister of Estonia, Taavi Roivas, speaking at the Plenary Session 'The Digital Sector as Key for a High Value Economy in the BSR' at the 2014 Baltic Sea Days.

☐ eGovernment refers to electronic government where public authorities interact over the Internet with citizens or businesses. With such eService offerings, nations can communicate with their citizens in a very convenient way, facilitate service offerings, and, at the same time, implement significant cost savings. On a global basis, the Secure Identity Alliance (SIA) has identified a saving potential of 50 billion US$ for governments by enabling trusted digital identities by 2020. The eServices are accessed typically using an eID. Such electronic identity documents host a chip for securely storing the digital identity of the document holder. Mobile ID refers to yet another approach where the data is stored in the secure memory of a mobile device like a smart phone or a tablet. The following sections address implementations of government services in more detail. The second part of the article describes the success story of the Estonian eGovernment solutions followed by concluding remarks.

eGovernment services are generally associated with an innovative country, which provides fast and convenient services to its inhabitants. Nations often find themselves in competitive situations amongst each other like with respect to their economic performance, or regarding acquisition of new industries. As a matter of fact, governmental interactions on a cost efficient and convenient level can turn out as a differentiating factor. Prerequisite for eGovernment services is a data-sharing layer for securely exchanging data over the internet between government agencies and optionally with private service providers.

To name just a few, the following list shall give an idea on possible eGovernment services: eTax, eSchool, ePension, ePolice, eHealth, eSignature, eElections, and eTicketing. eVoting, as another favorable service for example, has been introduced first in 2005 by Estonia, followed by mVoting in 2011, based on identification and authentication by means of a mobile device.

The eID contains a chip as an element to securely store the electronic card holder credentials used for “electronic” identification and authentication. Optionally, travel functionality is implemented on the chip based on biometric data of the document holder and in accordance with ICAO Document 9303. Here, the chip acts as a security element and can be used to pass the gates of an automated boarder control scheme.

Normally, eIDs are issued by governmental organizations. The credit card sized documents typically serve for physical identification purpose, too. With the inherent touch and feel of an official document and with the personalized portrait, document holders quite naturally perceive such documents as trustworthy with a strong tie to their own identity. Citizens easily comprehend where the digital identity is stored, especially if the eID is equipped with a contact based interface as is familiar from banking cards. This link of trust is a good starting point towards the successful implementation of eGovernment services.

Prerequisite for eGovernment services is a data-sharing layer for securely exchanging data over the internet between government agencies and optionally with private service providers.

The eID sample cards above illustrate two cards with a contact based interface (Hong Kong and Estonia with the chip on the back) and one with a contactless interface (Macau).

The Council of the European Union has adopted very recently the so-called eIDAS regulation which lays down conditions for cross-border recognition of electronic identification, creates a legal framework for trust services and electronic signatures and defines the rules for secure electronic interaction between businesses, citizens and public authorities. This regulation requires member states to mutually recognize their electronic identification schemes and is expected to come into effect by 2018.

The new regulation governs with Identification, Authentication and digital Signature the basic so-called IAS functionalities of an eID (see box on IAS). The so-called “advanced electronic signature” must be uniquely linked to the signatory, identify the signatory, be under his sole control and linked to the “signed” data and protect against subsequent changes. Furthermore, the “qualified electronic signature” addresses a higher security level with the additional requirements that the signature is based on a qualified signature, and is created with a qualified secure signature creation device.

The eIDAS regulation lays down conditions for cross-border recognition of electronic identification, creates a legal framework for trust services and electronic signatures and defines the rules for secure electronic interaction.

Smart card chips are the devices of choice for implementing legally compliant IAS functionality, since they are designed for implementing cryptographic operations and securely storing cryptographic keys. Credit card sized smart cards can be considered as the classical physical carrier. As discussed earlier, document holders intuitively comprehend the link between the physical and the digital identity and perceive a high level of trust in such governmental eIDs.

Alternative implementation forms like dedicated USB sticks with smart card hardware components or memory-based solutions have also gained in popularity. Memory-based solutions refer to configurations where the relevant cryptographic keys are stored in the cloud or on the computer hard disk or solid state drive. Such solutions may be challenged by the legal requirements for advanced or qualified electronic signatures, which state that the signature must be under the sole control of the signatory.

A mobile ID shall refer to a mobile device like a phone or a tablet that is utilized for identification and authentication services based on a secure hardware element and using network connectivity. The secure element (SE) can be implemented in four different configurations with different underlying ownership models:

- eID / NFC: the mobile device acts as a reader and connects by means of near field communication (NFC) to a contactless eID with smart card chip;
- SIM: the SIM hosts a dedicated SE, controlled and owned by the mobile network operator (MNO);
- integrated: the SE is an integral part of the mobile device’s hardware with the device supplier in a key position;
- SD-card: a separate secure digital (SD) card with an SE is inserted, supplied by the application provider.

Mobile ID users will experience convenient eServices using their mobile device which is virtually always at hand. It could yet be a challenge to sign a multi-page document using a mobile ID. With the limited screen capability, a “coupled” third device with larger display may be required for verification purpose.

IAS FUNCTIONALITY

Identification
process of using claimed or observed attributes of a person (or a thing) to deduce who the entity is

Authentication
corroboration of a claimed set of attributes or facts with a specified, or understood level of confidence

Digital Signature
data created through a cryptographic transformation, and appended to a data unit that allows the recipient to prove the source and integrity of the data unit

As the landscape of technical mobile ID solutions and ownership models is diverse, it is rather difficult to predict which solution will be successful and eventually dominate the market. The interests of the various stakeholders are not same. The success also depends on the level of trust which citizens associate with IAS services provided by MNOs or hardware manufacturers.

Mobile IDs and eIDs have a common ground as they are both based on a secure smart card chip, and they both support application with digital identification and authentication. Yet, these two forms of implementation also differ as only the eID is typically issued by governmental authorities and can serve for physical identification. Generally, the mobile ID is considered to offer a higher level of flexibility and convenience with a few limitations like in the case of generating electronic signatures.

The terminology e-Estonia has been introduced to describe Estonia's emergence as one of the world's most advanced e-societies.

Multiple forms of electronic identities have already been implemented in some states or may soon be reality. The eIDs take the anchor position for digital identities, as only eIDs are strongly linked with governmental authorities. Mobile IDs with different ownership and provisioning models implement a complementary service offering.

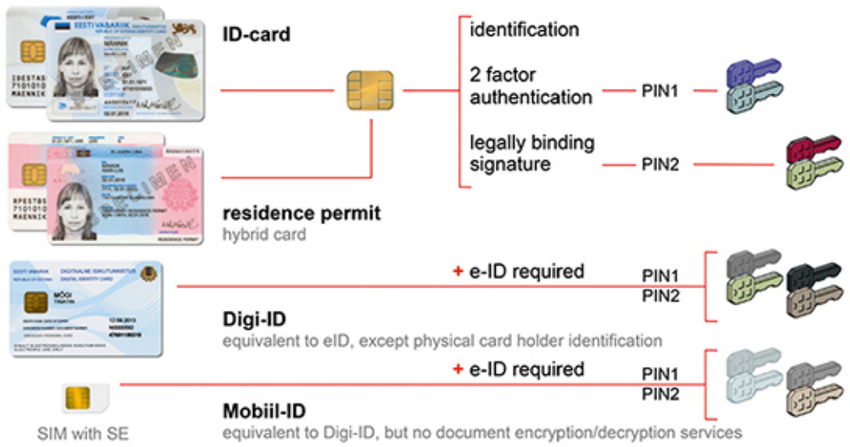
Estonia, the Baltic country with a population of 1.3 million, introduced its national eID in January 2002 and the mobile ID in 2007. As of today, the ID portal www.id.ee records 170 million electronic signatures and close to 300 million electronic authentication events. There are many reasons why Estonia takes a leading position with respect to eGovernment; one of them is that the eID is mandatory for all residents aged 15 or older. Another one is the vast amount of over 700 eServices offered by governmental and private organizations. These services can be accessed by the following types of digital identities shown in the figure below.

Estonian authorities offer with Digi-ID an alternative eID which can be issued on the spot, being particularly useful to quickly recover from a lost or stolen eID. It is also an attractive offering for professionals who need their eID functionality in a closed or hazardous environment. With Mobiil-ID, the brand name for the Estonian mobile ID, another option is available in cooperation with all three MNOs. All the above digital identity tokens store 2 asymmetric key pairs protected by dedicated PINs for enabling IAS services.

In Estonia, the eID acts as the anchor document since the alternative digital identity documents Digi-ID and Mobiil-ID are only issued on the basis of a valid electronic ID card or residence permit. As Estonian governmental institutions, private organizations and companies are very successful in offering eServices, the terminology e-Estonia has been introduced to describe Estonia's emergence as one of the world's most advanced e-societies.

Trust in identity schemes is a key element for a successful launch of eGovernment programs. Equally important is an attractive portfolio of service offerings together with a large-scale deployment of digital identities.

As an alternative to traditional eIDs, implementations with mobile devices are becoming increasingly popular, yet with competing technical approaches and different ownership models. It will be very interesting to observe initiatives in this business field, and how mobile IDs and related services will evolve. It is expected that mobile IDs will play an important role as an additional and convenient means for accessing eServices. This will have a positive impact on the usage of eServices with eIDs in a key enabling position. ☒



SECURITY meets *INNOVATION*

The Story Of The Irish Passport Book Design

By Dave O'Connor, DLRS Group

In September 1923 an Irish delegation, led by President Cosgrave, travelled to Geneva to seek admission for the Irish Free State to the League of Nations. The Irish Times of September 08, 1923 reports that the party were travelling on Irish passports, the first occasion on which Irish passports had come into use. The report continues that the passport was printed in Irish, French, and English and encased in a green cover. Whereas little further detail is reported about these passports, which would not be made available to the general public for a considerable time, the security features of the documents were considerably different to those, which appear on the modern Irish passport.

Ninety years later, the Irish Passport Service launched the latest incarnation of the Irish passport book. In this version the Passport Service worked with a group of commercial partners, led by the Irish based DLRS Ltd., to release a book that delivers enhanced security features but with a distinctive Irish identity. The passport may not be encased in a green cover but the design and development story is one with an Irish twist on security meeting innovation, resulting in the award of Regional ID Document of the Year 2014 and most importantly an enthusiastic reception from Irish citizens around the globe.

On opening the book your eyes are immediately drawn to the triple spiral drawing in the colour shifting ink Spark technology, one of the first occasions Spark has been used on an international travel document. This representation of the entrance stone to the passage grave of the Neolithic site Newgrange in County Meath – the entrance point to the new passport book. The Royal County theme continues with the use of the font "Meath" for the request page, a throwback to the type of fonts used on Irish passports from the 1940s.

Ireland's world renowned literary tradition is beautifully represented in the passport.

Dave O'Connor, Sales Director at DLRS Ltd, explains that the use of innovative security printing techniques continues through the book. "Shining a light through page 21 of the book towards the natural light, a shamrock appears through the elegant background surrounding the Aviva Stadium. Image perforation has been used in security documents, such as motor tax disks, in the past, but this is the first occasion the approach was taken in an international travel document."

Perhaps one of the most striking features of the Irish passport is the use of interesting celtic figures in half form on each of the visa pages. O'Connor explains that the Passport Service was looking for a simple feature that individuals could use to test the authenticity of the book. Fold the pages in on themselves a celtic God emerges in full. In 1781 James Gandon commissioned Edward Smyth to sculpt a series of figures to appear on the façade of Dublin's Custom House. Images of Smyth's river Gods, which continue to adorn the landmark building in Ireland's capital are used on the passport, a different half figure on each page. O'Connor continues "The Passport Service experimented with a range of images to be used on the pages and ultimately settled on these hand drawn images, which had last appeared on the "c" series of Irish banknotes, last seen in 2002".

WB Yeats

Images of Irish landscape, heritage, culture and modern Ireland, which adorn each visa double page were carefully chosen to resonate with Irish citizens. From the opening breath-taking landscape of the Cliffs of Moher in County Clare, to the stone ringfort of Grianan of Aileach in County Donegal, Croagh Patrick in County Mayo and the Rock of Cashel in County Tipperary.

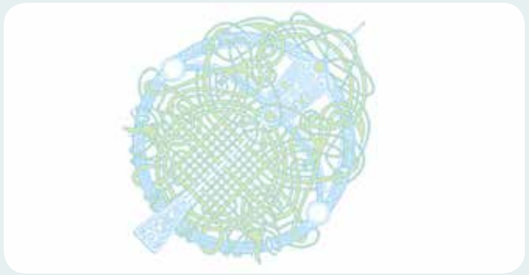
O'Connor confirms that the design was an evolutionary process. "Enhancing the security features of the passport was at the heart of the preliminary design stages. Our early discussions focused on the possibilities and limits of the range of security techniques to be used. The discussions then broadened to consider how each individual technique could be represented in a suitably Irish manner. The Passport Service had identified in advance a range of images to be tested for use on the visa pages. However it was only when the images were laid down on paper printed using security inks that real decisions could be made on whether or not individual images would be used or not. The Aviva Stadium image on page 14 of the book is a case in point. At first a photograph of this representation of modern Ireland was considered, but in the end a hand drawn sketch worked better on paper."

O'Connor points to some of the tricks used to capture the essence of locations while straying slightly from the visual reality. The image of Cork's Opera House is clear but is the foreground an exact representation of the site on Cork's Emmet Place?

It is the attention to detail that is striking throughout the new book. Wil Byrne, Techinical Director of Absolute Graphics, chief designer for the book says that Ireland's world renowned literary tradition is beautifully represented in the passport. Images which embody three Irish poems are used. Byrne takes out a magnifying glass to showcase the true minute detail of the drawings. In one of these, Yeats' Lake Isle Of Innisfree, pages 22 and 23 of the book, the poem's nine bean rows align along the cabin of clay and wattle and hovering around you can see the honeybee.

As the landscape images cross two pages, early design samples showed that it was necessary to find a suitable printed element to tidily close the image on each left hand page. To address this issue, an intricate design of two intertwined trees was used. Wil Byrne also explains that the trees represent the two traditions on the island. The birds, which make up part of this design are depicted dispersing seeds in the same way that our diaspora carry Irish values and traditions with them, as they travel the globe. The birds face outwards, suggesting that the sharing of values and traditions is a two-way process, which enriches us all.

ELEMENTS OF THE IRISH PASSPORT



Celtic Brooch
The Celtic Brooch is taken from Irish history. This original illustration not only shows the brooch design but also is placed at the traditional angle that this item of clothing was used representing care and security for children.

Bird Knot
The bird knot is used to tidily close the images on each two-page spread. It features an intricate design of two intertwined trees and two birds. The birds are depicted dispersing seeds in the same way that our diaspora carry Irish values and traditions with them as they travel the globe. They face outwards, suggesting that the sharing of values and traditions is a two-way process, which enriches us all.

Spark
The entrance to the passport sees a depiction of the entrance stone to one of Ireland's oldest monuments – the 5000 year old passage tomb at Newgrange.

Landsdowne Road

Ireland's lush green landscape and Irish nature are appropriately represented throughout the book. Ogham was an Irish alphabet in use up to about the tenth century, where essentially names of trees were given to letters of the alphabet. An ogham character appears on the bottom right hand corner of the datapage, printed in thermo-chromic ink, i.e. the colour of the character changes when heat is applied. On each left hand page a different ogham character is also used. However, a new dimension to the passport emerges and when the passport is inspected under UV the name of the tree associated with the individual ogham character and a hand drawn trace of each tree leaf, lights up under ultra-violet inspection.

O'Connor is keen to emphasise how attention to detail was so important to the Passport Service. Other examples of this detail include the celtic brooch pattern, used on each right hand page, containing small green dots indicating the page number; and the microtext printing of articles of the Irish constitution used to create the musical staves of the Irish national anthem.

The design of the polycarbonate datapage, which holds the personal data and the RFID chip within the passport, created other challenges advises Rory Noone of HID Global Ireland, who manufacture the datapage in their Galway factory. "The printing techniques and security features available on a plastic card are markedly different to those used on the paper visa pages, so it was important to design a data page, which maintained the Irish character and feel of the rest of the booklet, whilst ensuring high security and adhering to the international standards, which govern the layout of such pages. The Celtic knot motif and the harp symbol are quintessentially Irish, but we needed a theme, which would run through the whole book".

At the start of the design process, the focus was inevitably on improving the security features of the Irish passport book. This was undoubtedly achieved. However, at the same time a book was designed that brings together so many aspects of the rich Irish identity. O'Connor says this was achieved by the client

Polycarbonate Datapage

and service provider, spending the time up front to understand and be sensitive to national identity, and to innovate by building on this identity. The smiles on the faces of Irish citizens, who proudly show off their new passport when travelling, are testimony to the achievement of this aim. ☒

DLRS Group Security Concepts is Ireland's largest security printer. Established since 1976, DLRS is the market leader in vouchers, revenue stamps, cheques, passports and other security solutions.

David O'Connor, Sales Director
DLRS Ltd, Pinewood Close,
Bray Industrial Estate, Bray, Co. Wicklow
P: + 353 (1) 2768600
E: salesdlrsgroup@smurfitkappa.ie
W: www.dlrsgroup.com

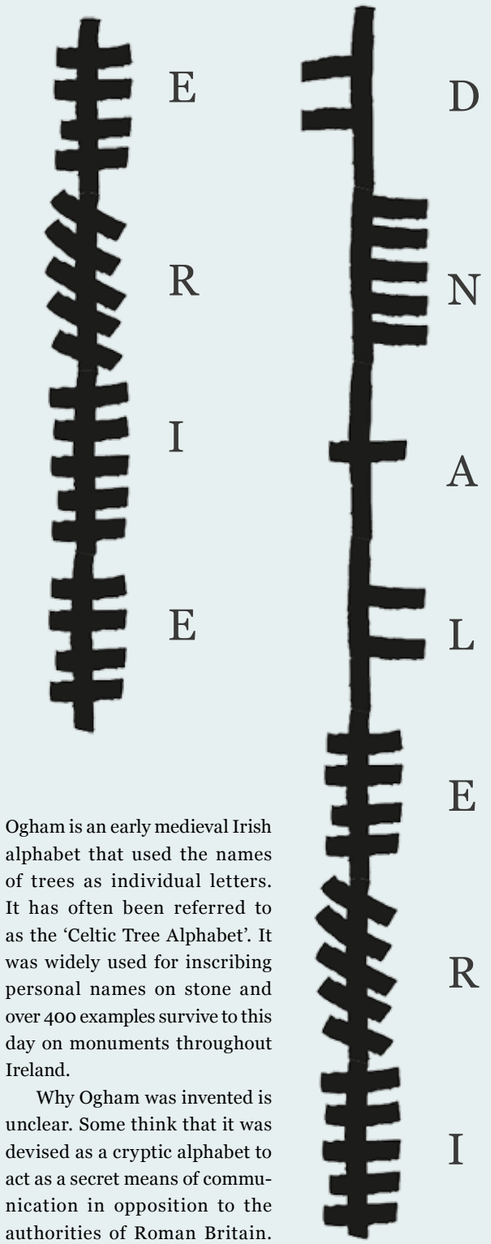
HID Global is the trusted source for innovative products, services, solutions, and know-how related to the creation, management, and use of secure identities for millions of customers around the world.

Rory Noone, Operations Director
HID Global Ireland Teo, Pairc Tionscail na Tulaigh,
Baile na hAbhann, Co. Galway
P: +353 91 506 904
E: RNoone@hidglobal.com
W: www.hidglobal.com

Absolute Graphics is the market leader in the design of security and anti-counterfeiting print solutions in the Republic of Ireland.

Wil Byrne, Technical Director
Absolute Graphics Ltd, Screentech Building,
IDA Business Park, Southern Cross Road, Bray, Co. Wicklow
P: +353 1 276 8100
E: wil@agraphics.ie
W: www.agraphics.ie

OGHAM ALPHABET



Ogham is an early medieval Irish alphabet that used the names of trees as individual letters. It has often been referred to as the 'Celtic Tree Alphabet'. It was widely used for inscribing personal names on stone and over 400 examples survive to this day on monuments throughout Ireland.

Why Ogham was invented is unclear. Some think that it was devised as a cryptic alphabet to act as a secret means of communication in opposition to the authorities of Roman Britain. Others think that it was invented by early Christian communities to write short messages in the Irish language.

eIDAS: HOW IT WILL BENEFIT YOUR BUSINESS ?

PAYING TAX · SIGNING CONTRACTS · TENDERS · INVOICING

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

BEFORE

Danger of **UNCERTIFIED WEBSITE**

WEBSITE AUTHENTICATION

The Swedish SME **IS NOT AUTHENTICATED** might be fake

E-ID AUTHENTICATION

EXCHANGE OF PHYSICAL DOCUMENTS...

NOW

CREATION OF THE E-DOCUMENT

DOCUMENT AUTHENTICATED

E-SIGNATURE
Swedish company (legally valid)

Confirmed time of submission

e-Acknowledgement of receipts

E-REGISTERED DELIVERY

LESS DOCUMENT STORAGE

LESS TIME

1 - 2 WEEKS

HOURS - FEW DAYS

LOWER COST

€ 50 - 100

€ 10 - 20

Source: European Commission

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

European Commission

SILICON TRUST DIRECTORY 2014/15

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, Neubiberg, Germany, offers semiconductor and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2013 fiscal year (ending September 30), the company reported sales of Euro 3.84 billion with close to 26,700 employees worldwide.
Infineon's semiconductor security technologies protect digital information from misuse: They guard over virtual money and sensitive electronic documents. Nowadays chips capable of processing encrypted data without converting it into readable text beforehand are used for the purpose. Infineon resolves the incompatibility of communication requirements and privacy. By combining hardware security and encryption technology, Infineon's chip solutions form the basis for data protection and data security while upholding the freedom of the individual and supporting modern, convenient communication media. 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

GIESECKE & DEVRIENT

Giesecke & Devrient
Creating Confidence.

Giesecke & Devrient (G&D) develops, produces, and distributes products and solutions in the payment, secure communication, and identity management sectors. G&D is a technology leader in these markets and holds a strong competitive position. The Group's customer base mainly comprises central and commercial banks, mobile network operators, business enterprises, governments, and public authorities. Protection of identity is becoming increasingly important in the digitally connected world. G&D has already established major milestones with Mobile Security, Government Solutions and Secunet AG. G&D combines its activities in the field of cyber-security across all business units to form a comprehensive solution and target new markets.
www.gi-de.com

GEMALTO

Gemalto is the world leader in digital security with 2013 annual revenues of €2.4 billion and more than 12,000 employees operating out of 85 offices and 25 research and software development centers, located in 44 countries. The company help 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.
Acting as an independent supplier, AdvanIDe has a long track record in interpreting evolving needs by the smartcard industry in the different regions of the world, thanks to our world-wide presence. AdvanIDe concentrates on proactively identifying emerging trends in order to anticipate rising demand and guarantee prompt availability of the required component in adequate volumes via cost-effective mode.
www.advanide.com

AGFA

Agfa is commercially active worldwide through wholly owned sales organizations in more than 40 countries. In 2011 the Group achieved a turnover of 3,023 million Euro. 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 (Societas Europaea) is an international information technology services company with 2013 annual revenue of € 8.6 billion and 76,300 employees in 52 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. With its technology expertise and industry knowledge, 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 applications like loyalty, e-purse etc.
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. With iEnigma®, charismathics re-invented the smart card, requiring only one set of credentials for a digital identity, whether in the office or on the road. The charismathics Smart Security Interface CSSI© is a comprehensive and agnostic PKI client framework. It supports all computer platforms, myriads of smart card operating systems and token profiles, various technologies and third party 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. All products are continually provided with state-of-the-art cryptographic algorithms. In addition, the implementation of forward-looking technologies, such as elliptical curve cryptography (ECC), for example, ensures the products already comply with many future requirements.
Technology from cryptovision forms an integral part of many different kinds of industry-specific devices, such as bankcards, passport control systems, control units for automobiles, military command systems, eBilling, ePayment, satellites, speed cameras, and many other applications. What is more, cryptovision PKI products secure the IT infrastructures of diverse sectors of the economy, as the range of our references from private enterprise to government agencies attests.
The highly qualified consultancy services provided underpin the effective integration of the security products. 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. Furthermore, strategic partner Matica System provides cost-effective, flexible solutions for industrial card personalization and card mailing systems.
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. Our company was established in 1926, primarily for the production of domestic banknotes.
Over the past decades our product range has become more and more diversified. Currently, we produce passports, visa, ID documents, driving licences, securities, duty and post stamps, tax stamps and banderols, paper- and plastic-based cards, with or without chip, and are aiming to provide complex system solutions.
www.penzjegynyomda.hu

HID GLOBAL

HID Global Government ID Solutions is dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide. HID Global Government ID Solutions offers government customers an end-to-end source for their most demanding state and national ID projects. With Genuine HID™, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Genuine HID solutions are designed and built in ISO 9001 certified facilities; include worldwide agency certifications; and are backed by global product warranties. Government ID Solutions offerings in-

clude expert consulting services, data capture, credential management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelaminates, LaserCard® optical security media technology, and FARGO® card printers.
www.hidglobal.com

HJP CONSULTING

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

THE IDENTIV GROUP

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

MICROPROSS

Microprass is a leading company in the supply of test and personalization tools for the smartcard industry. Active since 1979, the company features an in-house R&D center as well as production facilities The cornerstone of Microprass activity is the design of solutions for engineers looking for tools to qualify, or certify their products and prototypes against a given specification. Microprass 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.microprass.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. In 2012 the company opened Mikron GmbH /Munich to serve the market in EMEA and the US.
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 and certified Common Criteria – EAL 4+ on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multi-applications OS, used in more than 40 eID projects worldwide.
www.masktech.de

OVD KINEGRAM

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

PAV

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

PRECISE BIOMETRICS

Precise Biometrics is an innovative company offering technology and expertise for easy, secure, and accurate authentication using smart cards and fingerprint recognition. Founded in 1997, Precise Biometrics today has solutions used by U.S. government agencies, national ID card programs, global enterprises, and other organizations requiring multi-factor strong authentication.
The company is headquartered in Sweden and is listed on the NASDAQ OMX Stockholm small cap list (symbol:PREC). Precise Biometrics Inc., its U.S. subsidiary, is based in Vienna, VA. Precise Biometrics offers the Tactivo™ solution, a smart card and fingerprint reader for mobile devices. Also availalbe are related apps that use Tactivo for authentication using a smart card, fingerprint reader, or both.
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

SC2

SC2 is a broadcom company. The SC2 team is comprised of talented and experienced security architects and engineers, combining extensive experience with real world-implementations of smart card technology, including contact, contactless and dual-interface smart cards. SC2 solutions include e-health, e-ID, e-passport, citizen cards, signature cards, e-employee cards, e-banking solutions including worldwide credit card companies and transportation.
www.scsquare.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. SID-Consult also prepares expert opinions on fraud and counterfeiting.
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

The IT security association TeleTrusT Germany e.V. was founded in 1989 to provide a reliable framework for deployment of trustworthy information and communication technology. Today, TeleTrusT is a widespread competence network for IT security currently representing more than 110 members from industry, science and public institutions, with associated member organizations in Germany and other countries. TeleTrusT comments on political and legal issues related to IT security, organizes events and participates in conferences. TeleTrusT is the carrier of the "European Bridge CA" and the expert certification scheme "TeleTrusT Information Security Professional (T.I.S.P.)".
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. The corporate customers unit generated revenue of around EUR 9,5 billion in the 2013 financial year.

www.t-systems.com

TRÜB AG

Trüb AG is a leading company in Switzerland and internationally in the manufacture and personalization of national identity documents such as personal ID cards, driver's licenses, tachograph cards and data pages for passports as well as bank, loyalty and access cards. The company was founded in 1859 and has developed over the years into a world-wide leader for high quality identification solutions.

www.trueb.ch

UNITED ACCESS

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

www.unitedaccess.com

WATCHDATA TECHNOLOGIES

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

www.watchdata.com

WIBU-SYSTEMS

Wibu-Systems AG (WIBU®), a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market.

Wibu-Systems' comprehensive and award winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and intelligent device manufacturers who distribute their applications through PC-, embedded-, mobile- and cloud-based models.

www.wibu.com

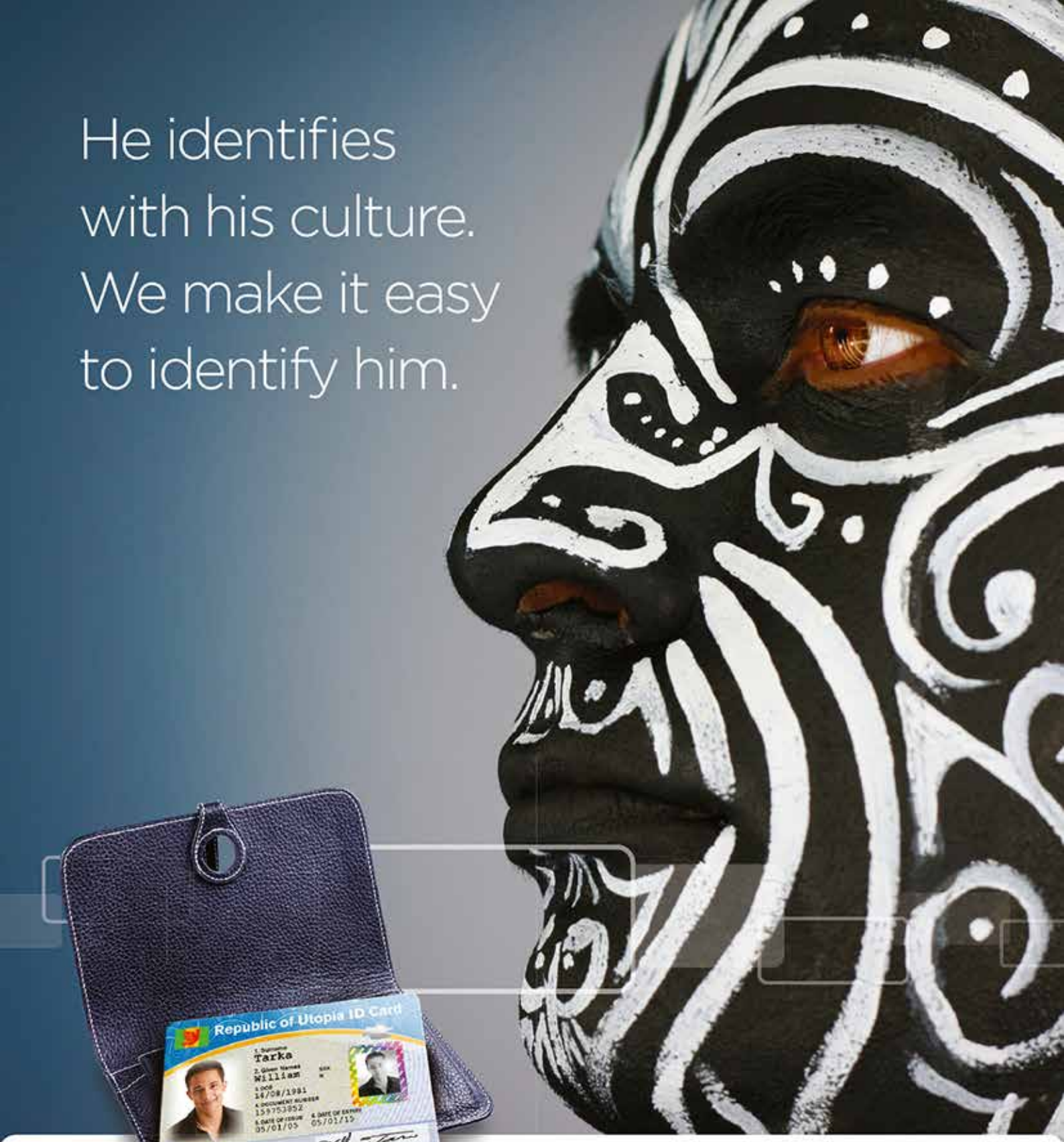
X INFOTECH

X INFOTECH is a leading system integrator and MultiPerso software developer, delivering security solutions to businesses across a wide range of industry sectors, such as financial, government, healthcare, retail, and public.

The company's portfolio supports all activities required for eID and payment card issuance, passport production and management, cryptographic infrastructure development, authentication solution integration, and other activities related to payment security and smart card technologies.

www.x-infotech.com

He identifies with his culture. We make it easy to identify him.



HID Global provides governments worldwide with highly secure, counterfeit-resistant ID solutions.

HID

Countries demand one-of-a-kind secure ID systems. HID Global delivers the field-proven brands and the solutions to create your unique system: LaserCard® Optical Security Media (OSM), ActivID® Credential Management System and FARGO® ID card printers and encoders. Field-proven brands, expertise, and trust–that's why HID Global powers the world's most innovative government ID programs. Let us power yours.
For more information, visit **hidglobal.com/citizen-ID**