

NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2014 | #14

The VAULT

SCORE!

JOIN THE
WINNING
TEAM WITH
MOBILE ID

CITIZEN 1

RED TAPE 0



Culture brings people together.
We'll help you tell them apart.



Only HID Global can create and deliver
a complete counterfeit-resistant ID solution,
custom designed to fit your country's needs.



Every country is unique. HID Global makes sure your Secure ID system reflects your unique needs. We have a stable of field-proven brands: LaserCard® Optical Security Media (OSM), ActivID® Credential Management System and FARGO® ID card printers and encoders. And our experts are ready to guide you in creating just the right system. Field-proven brands, expertise, trust – that's why HID Global powers the world's most innovative government ID programs, including the ultra-secure US "Green" Card. We're ready to power your nation's most important identity programs. **For more information, visit hidglobal.com/citizen-ID**

© 2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID logo and the Handshake logo are trademarks or registered trademarks of HID Global Corporation/ASSA ABLOY AB in the United States and in other countries.

Contents

ID goes mobile, one tap at a time... 4

By Joseph Haid, Infineon Technologies

eGovernment, the convenient way 10

By Marie Figarella, Gemalto

Europe leads the way in eID 16

By Veronica Atkins, Silicon Trust

Live from the drivers' seats 18

An interview with Oliver Winzenried and Marcellus Buchheit, WIBU-SYSTEMS

PersoSim – Simulator of the German ID card 24

By Holger Funke (HJP Consulting), Tobias Senger (BSI), Anke Larkworthy (HJP Consulting)

Turning to citizen-centric solutions for government ID 28

By Rob Haslam, HID Global

Securing sensitive data 32

By Marcel Hartgerink, WIBU-SYSTEMS BV and Tom Kevenaar, GenKey

Data security begins at the factory gate 36

By Thomas Löer, Bundesdruckerei GmbH

Multi-Access ID Card for every Russian citizen 40

By Andrey Golushko, JSC Mikron

The SwissPass – more than just a card 42

By Mario Voge, Trüb AG

Silicon Trust Partner Directory 2014 46

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: Heiner Fuhrmann, Detlef Houdeau

EDITORIAL CONTRIBUTIONS: Joseph Haid, Veronica Atkins, Michael Hegenbarth, Rob Haslam, Marie Figarella, Daniela Previtali, Holger Funke, Tobias Senger, Anke Lankworthy, Marcel Hartgerink, Thomas Löer, Andrey Golushko

PHOTOS: Infineon Technologies, Robert Brembeck/WIBU Systems, Genkey, iStockphoto

PRINTING: Druckerei Häuser KG, Cologne

EDITION: Spring 2014

No portion of this publication may be reproduced in part or in whole without the express permission, in writing, of the publisher.

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

ID goes mobile, *ONE TAP* at a time...

By Joseph Haid, Infineon Technologies

More than a billion electronic documents, such as eID cards featuring contactless functionality, have been deployed around the world. ABI Research reports more than 500 million NFC-enabled mobile handsets will be shipped in 2014. The fact that NFC-enabled mobile devices can interact with contactless identification documents – NFC-based Mobile ID – paves the way for innovative and secure services in the governmental and private sector. This article provides an overview on the basics of mobile ID based on NFC, use cases, the required technology and trends in the Mobile ID market.



□ What is the idea behind Mobile ID? Already the term provides a rough idea about the concept: a mobile device of any form factor – mobile phone, tablet, or laptop – is used to perform an operation based on the information of an individual person, i.e. electronic identification. The main difference between the implementations of this idea is where the credentials, e.g. name, date of birth, are stored and how they can be retrieved. Two basic concepts of Mobile ID can be distinguished:

- Credentials and security functions are stored on the mobile phone. They can either be physically located on the removable UICC ('SIM card') or on an embedded secure element soldered within the mobile device.
- Credentials and security functions are stored on a contactless ID card and are accessed via contactless NFC interface.

The latter approach relies simply on the requirements and environmental conditions in different countries around the world. Both have in common that individual credentials, e.g. fingerprints, and secrets, e.g. keys, do not leave the secure element of the certified eID card, thus they are not disclosed to the mobile phone itself. By its nature this solution benefits from hardware-based security as most eID cards are using certified security controllers. This article focuses on possibilities of NFC-based Mobile ID as it recently gains much attention around the globe.

Obviously, the mobile phone and its user are the central elements of Mobile ID use cases. The user downloads a mobile application onto the mobile device. To initiate the service, the user starts the application and selects the service to be performed, for instance signing a document digitally. The application requires certain credentials and secure functions to perform the task. All required functions/data are either provided by the contactless ID card or performed in collaboration with a background system. In extreme cases, the mobile device acts just as the user interface, while the function is performed only by the ID card and the background system. During the transaction, the user presents the contactless ID card on request to the mobile device. The mobile phone works now in reader mode, i.e. acts like any contactless reader holding a reader application. The security function is now performed, for instance, the ID card digitally signs the document or a strong authentication is performed. After the security function is finished, the data is sent back to the phone and/or to the background system. The application on the phone then closes and the eID card can be removed.

NFC-based Mobile ID is enabled by the increasing popularity of contactless ID cards within the population. In the past years, most Mobile ID systems were based on UICC-based approaches due to

practical reasons. The deployment of NFC-enabled mobile phones was simply too low to reach a significant portion of the population. Examples of UICC-based systems can be found in Estonia (Mobile ID) and Finland (Valimo Mobile ID).

The growing penetration of NFC-enabled phones together with the growing number of contactless ID cards has already changed this situation. Governments around the world are starting to think about Mobile ID services in order to simplify the public sector processes for its citizens. Furthermore, there are ideas to offer Mobile ID-based services to private services. One example is that a company could offer its employees the possibility to electronically sign internal documents using the contactless identification document. To integrate this functionality, the application on the mobile phone can be extended with a ready-to-use service offered by a government.

The growing attention on the large potential of the Mobile ID market is obvious at the many mobile industry conferences, trade shows and events around the world. One of the basic ideas, which are already being demonstrated in various products, is to transfer the processes already existing today, i.e. using a PC combined with a contactless reader, to NFC-enabled phones. This straightforward approach does not require the design of new contactless identification cards, but broadens the number of potential users for Mobile ID services.

Governments around the world are starting to think about Mobile ID services in order to simplify the public sector processes for its citizens.

It can also be observed in the market that mobile phones are considered as an attractive alternative to contactless readers. In this case, the mobile phone is connected to a governmental background system and performs the desired action, e.g. the identification of a cardholder. Thus, a number of freely available applications are available to read out contactless cards. In the government identification application segment several NFC-based ePassport readers are available.

So what kind of application scenarios are attractive and realistic? One possible use case is strong authentication using NFC-enabled Mobile IDs. Services provided via networks require a strong authentication mechanism for the user to prevent misuse and digital fraud. Authentication can be done in several ways, e.g. via user name, password, fingerprint, and/or secure physical tokens. The NFC-enabled eID card can serve as a secure token communicating conveniently



with the mobile device. In this case the eID card is an extension to typical user name/password authentication, and an alternative to dedicated physical tokens. The principle described is called "Second Factor Authentication": combining 'Something I know' (e.g. password, user name, pin) with a second factor 'Something I have' (e.g. eID card). This type of strong authentication is already used in many eGovernment applications, often still based on the contact interface of a smart card. ID cards support a secure authentication towards several eServices, e.g. tax declaration systems, and private/commercial accounts, e.g. banking systems in several countries, e.g. eCard/Austria, National eID card (nPA)/Germany. It is expected that a

growing number of contactless eID cards will be able to provide the strong authentication function together with an NFC-based enabled phone. A practical reason limiting the use of this authentication functionality is the relatively small number of smart card readers in the population. In the NFC-enabled Mobile ID use case, the mobile phones act as a smart card reader, thus overcoming this limitation.

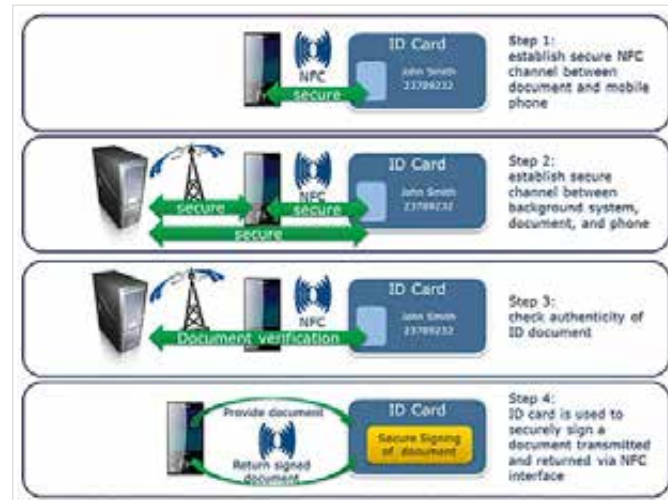
Another use case is signing documents using the NFC interface: Document signature in the governmental and private sectors is one of the most attractive use cases for NFC-based Mobile ID. Documents to be signed include legal contracts and income tax statements, but also documents of everyday life such as registrations of the kids to

kindergarten activities. In this use case, the eID card is presented to the phone and establishes a secure channel. In a second step a secure channel to the background system is established to enable secure exchange of data between the phone, card, and background system. In a third step the background system checks the authenticity of the eID card based on strong authentication. Based on a successful authentication, the card electronically signs the document and returns it (or a secure hash value) back to the mobile phone. Finally, the card can be removed from the phone and the process is finished. Exploiting the possibilities of mobile devices, the signed document can be sent via e-mail to the desired addressee. The described use case combines the hardware-based security of the eID card with the convenience of contactless technology.

So, with a demand for mobile ID solutions in the market and an increase in NFC-enabled mobile devices, what are the technical challenges that remain? As is so often the case, it is the matter of standards and interoperability. Despite the availability of NFC-enabled phones,

Despite the availability of NFC-enabled phones, not all specifications are finally released and tested yet. This implies that NFC-enabled devices may have different contactless behaviors. This situation results in a heterogeneous NFC infrastructure causing undesired interoperability issues between smart cards and mobile phones.

not all specifications are finally released and tested yet. This implies that NFC-enabled devices may have different contactless behaviors. This situation results in a heterogeneous NFC infrastructure causing undesired interoperability issues between smart cards and mobile phones. The challenge for contactless smart card IC vendors is to provide interoperable products beyond the functionality described in ISO/IEC 14443, and even NFC Forum specifications. Further challenges are multi-application scenarios, i.e. combining several applications on one eID card, such as secure transport application with governmental services. In order to be independent on any proprietary solution not available on all NFC-enabled devices, an open standard is the best solution to choose. The CIPURSE™ standard, developed by the OSPT (Open Standard for Public Transport) Alliance, fulfills these basic requirements.



Using Mobile ID for secure signing of a document. The signed document can then be sent via email to the addressee.

The strength of the NFC-based Mobile ID approach is the seamless combination of intuitive usability via NFC with the security using a contactless, security certified eID card. The large deployment of more than a billion contactless ID cards combined with the availability of more than 500 million NFC-enabled mobile devices in 2014 opens up a completely new space for innovative, customer-centric services and applications. It is expected that Mobile ID will not only evolutionally, but revolutionarily change the landscape of governmental services on mobile devices in the next few years. One important step will be the interoperability between NFC-enabled mobile devices as well as contactless documents, mostly designed with respect to ISO/IEC 14443. This is already addressed in all relevant standardization and specification bodies. The challenge for contactless smart card IC vendors is to enable interoperability within the known ISO/IEC standards, NFC Forum specifications, the installed contactless infrastructure, and mobile phones. The use cases described in this document – strong authentication and electronic signature – show the high attraction of NFC-enabled Mobile ID. The advantage of combining hardware-based security on eID cards with the convenience of contactless technology makes NFC-based Mobile ID a promising approach for use in governmental and private sectors. ☒



Discover the Innovation Driver for ID Management.

As a leading systems supplier in the high security segment, we offer a perfectly matched range of innovative Secure ID solutions. Our unique Full-ID Management reduces data to what's important, makes communication channels secure throughout and enables trusted authentication on the Internet for both you and your customers. Discover a system that is so much more than just the sum of its parts:

www.bundesdruckerei.de | www.full-id-management.de

eGovernment, the *CONVENIENT* way

By Marie Figarella, Gemalto

As government agencies and companies need to provide access to online services on mobile devices, they are facing the challenge to offer the same security level currently available with cards on desktops or laptops. Mobile Identity offers convenience and can pretend to reach a high level of security with the support of SIM cards, GSM networks and rigorous registration process for trusted issuance. It enables people to sign documents via mobile digital signature, perform business transactions, access medical records, submit taxes and engage in a wide array of personalized online services wherever they are, over their mobile network. Via mobile, there is one single device for authentication allowing the citizen the ease of accessing services via their mobile smart phones with the assurance that their personal information is secure.



□ Many country feedbacks (Spain, Estonia, Belgium, Portugal) showed that the availability of a card reader has been one of the main hurdles for citizens to use their eID cards to secure their eGov services online. We see the combination of contactless eID cards (such as the German eID project or ICAO compliant resident cards) with NFC-enabled mobile phones as a promising approach and simple first step to automatically read ID credentials.

Mobile authentication solutions for government programs

The vision of governmental modernization programs is usually based on a strong idea: to extend all traditional uses of identity cards to the digital world, as well as to generate all the benefits in terms of increased competitiveness, responsiveness, ubiquity, potential for improvement and innovation of public services which online trusted transactions can provide to the socio-economic activity of a country.

Public acceptance, measured by the use of the electronic identity, has however not met expectations in many countries.

Public acceptance, measured by the use of the electronic identity, has not met expectations in many countries.

One of the greatest assets of mobile authentication solutions is the ability to extend smart card based national eID schemes. They enable governments to put the citizen electronic ID into every pocket that can hold a mobile phone.

Complementing the national eID card, mobile authentication solutions add the true mobility factor into the eGovernment services.

A big challenge has always been the threshold in user acceptance. If the solution is too complex, the citizens may shy away from it. Using the mobile phone as a signing and authentication device is natural for almost all users, and using a SIM card, one can also see it as the most democratic method of all – it can be available to anyone who has a mobile phone. Now, with authentication solutions on mobile, citizens can access services from all over the world, the only thing needed is a working SMS connection.

SIM cards are also enabling network connected devices being able to receive push notifications and authentication requests without requiring any action from the user. Mobile authentication solutions can add even more integration and ease of use adding authentication services in the Embedded Secure Element (eSE, TEE) of many modern phones.

Gemalto leverages on its Valimo Wireless activities. It is the leading solution provider for mobile user authentication and digital signatures with over 20 on-going projects and enabling millions of users to start accessing government services with enhanced security. Among those projects, 8 are used specifically in national eID schemes to secure the access to eGovernment services.

Mobile ID and Finland: love at first sight!

Finland has been one of the pioneers in use of Mobile ID. Just a few months after its launch in the country, Mobile ID was already supported by all eGovernment services that required strong authentication. Mobile PKI offers a very strong security framework for all parties. The security related operations are done in the SIM card, a tamper resistant environment, making it almost impossible to misuse the users identity. Software that tries to steal the identity of the user or sniff out passwords or other credentials cannot penetrate the SIM security.

Using the mobile phone as a signing and authentication device is natural for almost all users, and using a SIM card, one can also see it as the most democratic method of all – it can be available to anyone who has a mobile phone.

Authentication and signature information travels through the SMS and back-end channels to the service provider and is verified by the operator, so even if the user is attacked at the browser level,

or the computer is infected, it does not matter. The data never goes through the Internet channel. To be successful, the attacker should also gain access to the mobile operator network to attack/infect the encrypted SMS messages.

A Finnish consortium offering a centralized authentication and authorization portal for eGovernment services, realized quite early that a flexible and independent method of authentication was of importance.

Mobile PKI was seen as a great alternative for strong and flexible user authentication and electronic signature services. The government services saw the opportunity because of the high rate of transactions of many on-line services and the need for a cost-effective way of strong authentication.

The mobile network operators also seized the opportunity to build new services and generate new revenue streams using the mobile PKI technology. From early on, the major Finnish telecoms operators decided to create a national specification based on the ETSI Mobile Signature standards, the international standardization that defined the mobile PKI.

Simplified registration process in Finland

With the legislation, it is now possible for the user to walk into any operator shop and register his/her digital identity on the spot. The user presents his/her ID document (passport, driving licence, ID card) to the shop clerk when requesting a Mobile ID. Thanks to well trained staff, the actual registration process takes only a few minutes and the certificate is valid for five years.

Gemalto leverages on its Valimo Wireless activities. It is the leading solution provider for mobile user authentication and digital signatures with over 20 on-going projects and enabling millions of users to start accessing government services with enhanced security. Among those projects, 8 are used specifically in national eID schemes to secure the access to eGovernment services.

The four rules of success according to Finland

The parties involved in the mobile PKI efforts were determined to learn from the eID lessons and take into account that many Finns

still clung to the bank issued OTPs. The Finnish mobile network operators focused on four rules when launching the Mobile ID:

1. Launch the solution with attractive services.
2. Make it easy to get.
3. Market the solution to the end users.
4. Make sure it is easy to use.

The current Mobile ID approach in Finland is successfully leveraging these four guidelines:

- As it is at the heart of the mobile network operator business, operators can leverage the mobile PKI and offer new services especially attractive to corporate customers.
- Acquiring the mobile PKI is very easy. The activation itself can be done in the operator point-of-sales in a few minutes, or even online.
- In order to get as many active users as possible, the operators are creating marketing campaigns to promote mobile PKI and to recruit service providers.
- Authentication is as simple as 1-2-3. When you need to authenticate, just type your PIN code that protects the private key into your mobile phone and press OK. That's it.

Derived identities

High assurance credentials such as cryptographic national eID cards can be cumbersome to use across various platforms such as tablets or mobile devices. Electronic identity schemes available to the public today need convenience in use and availability, two key features of mobile devices.

This has brought about the idea of derived identities which basically enables a citizen to generate additional identity credentials onto different platforms to engage securely with identification and authentication services using eID as common trusted root. For example, a citizen could use its secure eID to create a mobile ID. The derived credential could then be used to identify, authenticate or even sign directly via the handset. ☒



Oman: a multi-channel approach

In December 2013, Oman's Information Technology Authority (ITA) launched a new Public Key Infrastructure (PKI) system to help secure online transactions.

The secure infrastructure, now in live mode, enables multi-modal access to eGovernment services (eID cards or Mobile phones) with the highest identity assurance level (level 4). It addresses both the public sector to secure eGovernment services and the private sector and supports the national digital transformation program.

The new Mobile ID is derived from the national ID scheme and Oman's Civil Register. The national ID provides a unique and strong evidence of the subscriber's identity bringing trust to the overall eServices scheme in Oman.

Source: Gemalto



The face recognition company

Cognitec develops market-leading face recognition technologies and applications for enterprise and government customers around the world.

Face recognition technologies are constantly evolving in response to new applications and quickly changing biometric markets. Cognitec's leading-edge products efficiently implement the different processes involved in today's identity management systems using facial data:

- identity verification
- duplicate check
- background check
- management of identity information
- real-time identification in video streams
- acquisition of biometric facial photographs

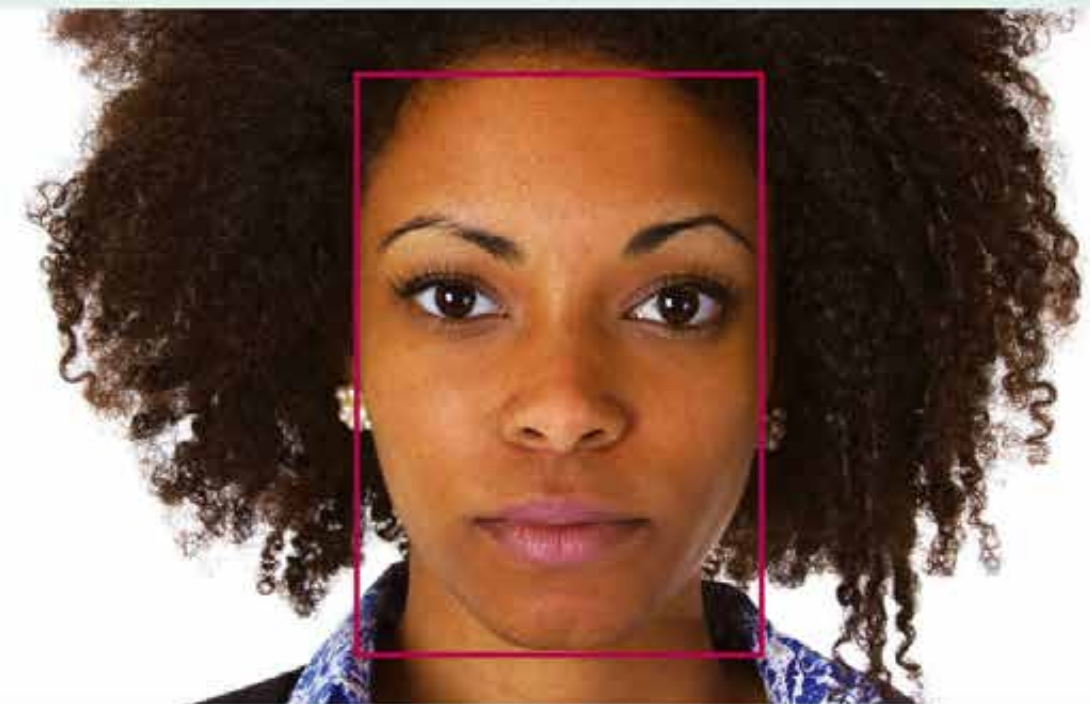
At the same time, Cognitec's products enable new commercial and consumer applications using facial data:

- analyzing people flow by count, age, gender and other measures
- recognizing VIP customers
- enabling digital signs to tailor advertisements
- logging in to computers, phones and banking machines
- indexing and sorting photographs in digital photo albums
- automotive applications for convenience and safety
- allowing humanoid/service robots to recognize faces and interact with people

Biometric performance has always been the focus of Cognitec's research and development.

Continued tests by government authorities and industry have validated Cognitec's leadership position within the face recognition market since 2002, resulting in a track record of successful reference projects worldwide.

With a clear focus on face recognition technology, we are committed to deliver the best performance available on the market.



EUROPE leads the way in eID

By Veronica Atkins, Silicon Trust

What would we do without the internet? It has become the backbone of our daily lives – we use it to work, to shop, to communicate. Today's service providers are making use of this rapid development and are providing more and more online and mobile services. Governments are beginning to catch up and so eGovernment solutions are on the rise. eID schemes with an integrated secure online functionality provide an infrastructure for the public sector to implement their eGovernment solutions. These solutions provide a more convenient and efficient way for the public to access their government services and reduce the frequency of the time-consuming visits to their local government offices. Prerequisite to use online public services with a secure proof of identity is an electronic identity card (eID) with security chip. While the trend towards secure national IDs is taking place across the globe, Europe is leading the way when it comes to using eID as a secure key to the online world.

150 *Million*

eID cards with online functionality have been issued in European countries by the end of 2013

Source: Eurosmart

70 %

of European states issuing eIDs with online functionality trust Infineon's security solutions

Source: Infineon

Infineon

With eID programs in place since 1998, the EU has accumulated

16

years of knowledge on eID

Source: Eurosmart

20 *among* **35**

countries worldwide that have introduced eIDs with online function are in Europe

Source: Infineon

EU Commission and Member States spend more than

€100 *Million*

for technical interoperability along eID, eHealth, eSignature and eServices

Source: Eurosmart

The sovereign documents market will grow by

14 %

in 2014

Source: Eurosmart

Live from the DRIVERS' SEATS

An interview with Oliver Winzenried and Marcellus Buchheit, WIBU-SYSTEMS

Photos: Robert Brembeck



1989-2014: “25 years propelling your business to new heights” is a bold statement that only exceptional company founders and top managers can make. In this interview, Oliver Winzenried, CEO of WIBU-SYSTEMS AG, and Marcellus Buchheit, CEO of WIBU-SYSTEMS USA, Inc., reveal some exclusive details about their personal journey and the ingredients of their special recipe which made them achieve a long-term vision and gain world recognition as one of the top three leading vendors in software protection, licensing, and security.

□ *You've started an entrepreneurial carrier early in life; how did you develop this idea and put it into practice back then?*

[Marcellus] Oliver and I first met at the Karlsruhe University while we were working on a mixed software/hardware project for the university's amateur radio station. Over the next couple of years, while still attending classes during the day, we developed several custom-specific projects at night. They were all successful and this made us confident that we could create a product that we could sell to the mass market. We soon realized that original software for PCs could be easily hacked and that security solutions on the market were still in a primordial stage. The plan took shape in 1987, when Oliver developed the WibuKey chip and its hardware, and I focused on the protection technology and tools on the PC.

WIBU-SYSTEMS has kept a unique vertical focus over the years. How did you spot this niche, and why have you not embraced additional technologies?

[Oliver] WibuKey 1.0 was released for DOS and already contained a basic version of the sophisticated automatic protection to come. Over the following years, the number of operating systems exploded – 16-bit Windows, OS/2, Novell, Linux, 32-bit Windows, MacOS, etc. We wanted to present a universal solution for all platforms to our customers. However, supporting so many platforms with a single architecture and one unique programming interface (API) was challenging, and our development resources were limited. Meanwhile the software protection market was growing worldwide, so we decided to keep faith to our original technological challenge. With a clear technological focus, we could listen to prospects' and customers' demands and provide them with an unprecedented advanced technology. We felt that to enter other security markets would dilute our core focus of software protection. At the end of the day, still in our niche, our solutions have gone through tremendous development: from IP "Protection" against counterfeiting and reverse engineering, to "Licensing" as an enabler of new business models, to "Security" to prevent tampering and cyber-attacks.

Where did the idea of CodeMeter originate?

[Marcellus] Before the Internet, software was burned on a CD and shipped in a box; adding a dongle was a no-brainer. In the Internet age, CDs became obsolete and software was all downloaded, which completely changed the rules of the game. Threats multiplied, allowing us in turn to grow our market share, but at the same time we had to rethink the concept of the product itself. We ended up envisioning a dongle which could be shared by many software publishers, but strictly programmable and upgradable at the end user's computer. After lot of brainstorming we came up with the idea that the name for this new product would be "CodeMeter" to express the purpose of the technology, namely that the "metering" aspect related to the use of software, so that the act of measuring could be used as an attribute of the source code.

Being the CEO of a company for 25 years is not an easy business; what is your way to keep a clear vision of the future strategies you want to pursue?

[Oliver] WIBU-SYSTEMS' first core value is to be of service to our customers so that their business can expand, once their assets are protected. And for that we listen closely to customers' wishes; they are an incredible source of ideas due to their diversity in their markets, cultures, and perspectives. Further, we try to anticipate the market trends, and that's where our active role in several international business organizations and standardization bodies lets our imagination flies to a different level. Last but not least, competition and new security threats challenge our brain and ensure we continuously evolve our products.

CodeMeter seems to be a complex product. How can it be described simply?

[Marcellus] In our early years our attention was fully taken by dongles as they represent the utmost security level when it comes to software protection. But we also knew that the criteria for adopting such a technology would sometimes include other circumstances, like at times the impossibility to connect to hardware at the end user's site, or a peculiar license distribution model, or a security solution so advanced that it was the most expensive part of the application. This is why we added CmActLicense to our portfolio. It still resides under the same CodeMeter umbrella, because licenses can actually be stored in a mix of repositories, all handled by the same core technology. CodeMeter is still involved when it comes to the creation, management, and distribution of licenses, but now it's a different layer of the CodeMeter technology – License Central. License Central interfaces with hard- and soft-license holders and streamlines the whole process in conjunction with the existing business ERP, CRM, and e-commerce systems in place.

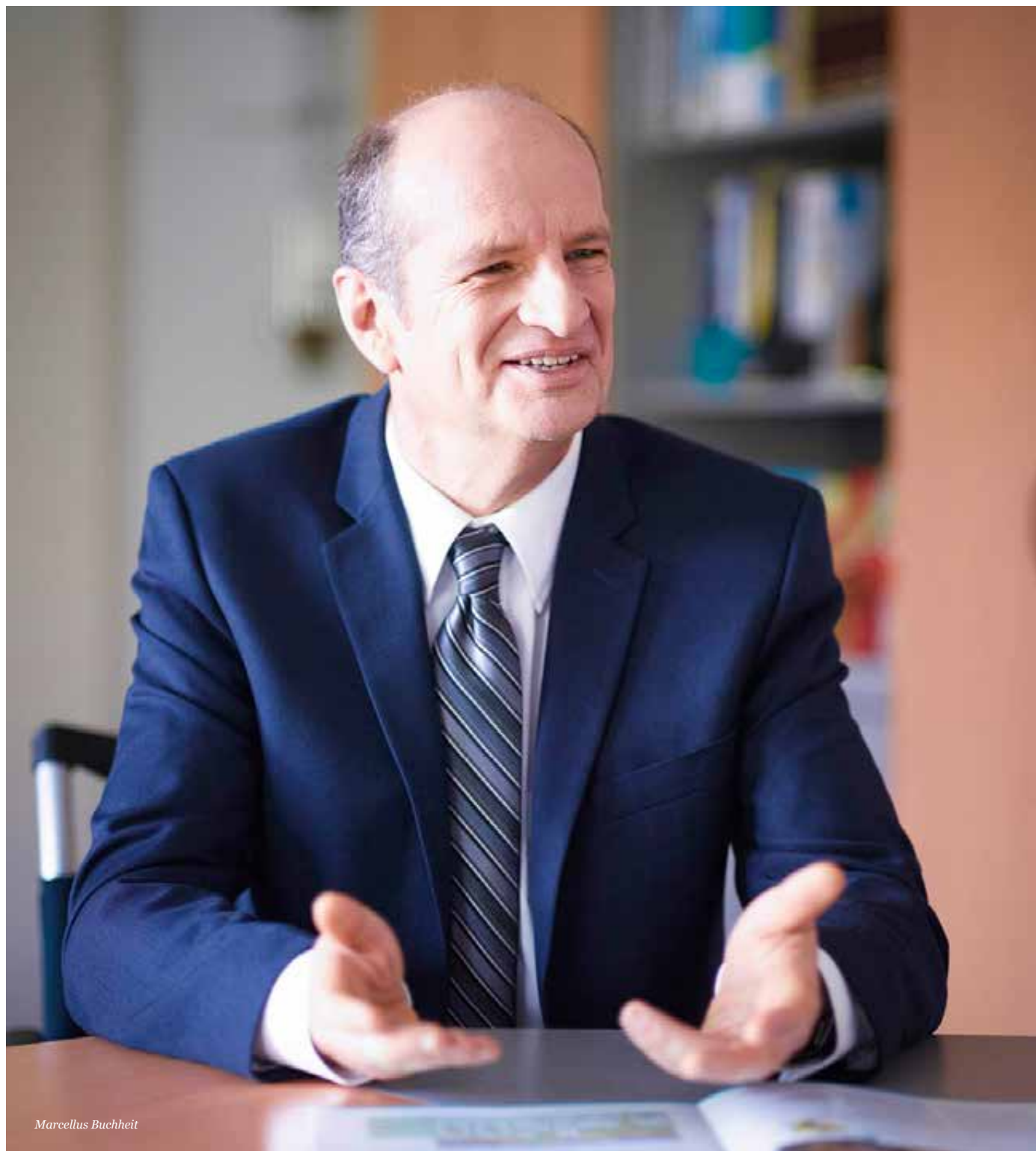
Who are WIBU-SYSTEMS' ideal customers?

[Oliver] Essentially we are coming across two main user groups. One uses PC software in office environments, while the other consists of manufacturers that deal with industrial applications and embedded devices. The former is gradually implementing a centralized license management solution to handle all new license models and automate the related processes. The latter is facing not just global counterfeiting but also sabotage, tampering, and cyber-attacks which are unprecedented in history, and therefore needs to become knowledgeable in security and to implement integrity protection solutions. In the case of ISVs, the product can easily be a standard package with optional customization features. For OEMs, the scenario is more complex for both sides, which is why we have begun forming strategic partnerships in order to generate facilitated solutions for developers. We are extremely satisfied with our customers and the long-term relationships we have with many of them testify to this mutual feeling.



Oliver Winzenried

"Wait until you have a bright idea, but when it comes to you and you've tested it, start pursuing it no matter what."



Marcellus Buchheit

"Employees are the engine of innovation and design. Their input is very respected."

The approach to market has changed as technology has pervaded our lives; are you a precursor of new trends or do you keep a more conservative attitude?

[Marcellus] We have always strived to be creative and develop innovative and proprietary solutions, and to support new emerging technologies since their early stage, whether it's a new operating system, a trend like the cloud, a revolution like connected systems in industrial automation, or the portability found in mobile technology. That's the approach we started with 25 years ago when we first began protecting Windows applications without requiring any source code modification, or later with Wibu-Box in the form factor of a PC Card, or later on with the USB interface, and even today with CodeMeter units available as μ SD cards or CFast cards, to today's support of PLCs and real time operating systems.

At the same time customers are right in asking for backwards compatibility and retrofitting, and we work hard to ensure our oldest dongles are still compatible with our newest technologies. This is a great benefit for their business continuity even though it somehow limits our possibilities.

You have opened other subsidiaries of Wibu-Systems across the world. What drove your decision to start a business in the US and in China? Are you considering further expansion?

[Oliver] The foundations of software development are pretty much identical around the globe – same platforms, computer models, development tools, etc. Other factors determine the success of a company abroad, like the completeness of the localization services, the skills of the local support team, and the training of the sales team. The liaison between the headquarters and the local realities are challenged by time differences, distinctive cultural approaches, linguistic barriers, diverse legal problems. We will definitely expand further on, but since we want to make sure we offer a tailored approach that meets the regional demands, we'll proceed progressively at a pace that allows us in the end to have a stable and competent foothold in each country.

We are very excited about our burgeoning growth into Latin America and Africa: these continents are amazing in terms of their economic potential and we would be excited to start local collaborations there.

Many of your co-workers have been with you for an exceptionally long time. What is the secret behind such a loyal team?

[Marcellus] Employees are the engine of innovation and design. Their input is very respected. Our company is growing in a stable fashion aiming at a broad ultimate picture; we are not the typical "hire and fire" business driven by short sighted financial results. At Wibu-Systems, the staff members of all departments contribute with their ideas and influence company's decisions. The atmosphere is cheerful, doors are open to invite dialogue, we

all enjoy a high level of reciprocal trust combined with a receptiveness to cultural interchange both within our headquartered team and with all our offices and partners scattered all over the world. The company promotes high ethical values which makes it easier for all to identify with them and pursue the common goals we set together. Last but not least, we invest in continuous training and education of our staff and share our commercial success with them.

You have achieved a proven track record of patents and awards. What is your role to this day with the educational world? And how much are you involved in training new students?

[Oliver] Yes, that's true, we own several trademarks, domains and patents in the US, Japan, and Europe. Patents are the true essence of the value of a company. And to make sure our innovations keep being top-notch, we are very active in research and development, and thus cooperate with, among others, the Karlsruhe Institute of Technology, the Fraunhofer organizations, and DFKI – the German Research Center for Artificial Intelligence.

Thanks to this constant exchange of knowledge, students are welcome for their internships in our headquarters or offices abroad while they complete their PhD. Moreover, we promote engineering, computer science, and other technology-oriented disciplines directly in primary schools, where we introduce pupils to these professions.

If there was something flattering you were to say about your top competitors, what would it be?

[Marcellus] We have a decent amount of competitors in the field, not too few and not too many, which gives us the right kind of encouragement to offer high-value products to our customers and spurs us to differentiate our offering. As independent analysts recently highlighted in a Hot Company Watchlist for our market segment, Wibu-Systems is actually one of the two top world leaders in hardware-based software protection and one of the three top global vendors in license management. Given that we have an innate tendency to over-engineer, the competition also plays a role in keeping us on track. With some vendors driven by sheer profit and others who have mainly turned their company from an entrepreneurial activity to a financial venture, we are happy to sit in the midst of all this and maintain our feet right on the ground and our minds in free rein mode.

What is the legacy that you'd like to convey to aspirational entrepreneurs?

[Oliver] Wait until you have a bright idea, but when it comes to you and you've tested it, start pursuing it no matter what. And then keep a good balance between external suggestions and your own insight. Patience and endurance are also top ingredients for a good mix. ☒

PersoSim – Simulator of the German ID card

By Holger Funke (HJP Consulting), Tobias Senger (BSI), Anke Larkworthy (HJP Consulting)

This article describes the advantages of an open source solution to simulate the chip card functions of a German electronic ID card.

□ Introduction

The electronic identity card (nPA) with its integrated chip provides a higher authentication strength than do other authentication procedures, such as username and password, and thus is expected to be used increasingly in both eGovernment and eBusiness applications. An electronic ID card holder can use the eID card to register for online services, while service providers can ensure that the user is who he or she claims to be. This principle of mutual authentication is the core element of the German electronic identity card.

Prior to the introduction of the new ID card in 2010, an extensive application test was conducted. In addition to being given access to different eID servers that were necessary for the test, participants received various sample ID cards. Using the sample ID cards, interested service providers were able to test their services prior to activating them online once the first eID cards were issued.

The sample cards used in the application test turned out to be too inflexible, however. The open source project "PersoSim" works around this issue by providing a simulator for the smart card functions of the new eID card. Although test cards continue to be an important component of evaluating and testing new eID services, a software-based simulation such as PersoSim has the advantage of being available free of charge at any time and can quickly be adapted further to meet new requirements. PersoSim¹ simulates all mechanisms and cryptographic protocols described in the technical guideline TR-03110 [1] of the Federal Office for Information Security² (BSI). The simulator is available to users who are looking for a versatile alternative to previous sample cards, such as service providers who would like to verify their implementations using the simulator. Furthermore, developers of eID clients, who can use the simulator to test their interpretation of the technical guidelines, will benefit from PersoSim. The simulator will also be of interest to anyone who intends to evaluate the protocols of the eID card in more detail. The source code of the simulator will be provided as

an open source project, allowing interested parties to investigate the cryptographic protocols of the electronic ID card.

The BSI hired HJP Consulting GmbH³ to develop the open source simulator. PersoSim is aimed both at developers in the open source area who want to actively participate in the further development of the simulator and at users who are seeking a ready-to-run sample card simulation. The BSI's additional objective for the simulator is for PersoSim to be used for upgrades of existing security protocols as well as for prototype implementations of new security protocols. Upgrading existing security protocols and evaluating new and stronger protocols for use with physical chip cards is a very time-consuming and costly process. It requires the involvement of several external parties, including manufacturers of semiconductors, COS, and chip cards as well as application developers. These restrictions do not apply when using a software-based simulator, because the protocol under test can be directly accessed. After changes have been made, the protocol is executable through a simple compilation of source code.

The authors first publicly introduced the project PersoSim during the Open Identity Summit in September 2013. In April 2014 the German magazine *Datenschutz und Datensicherheit* published an article focusing on PersoSim as part of a series of open source security articles [8].

The simulator

The simulation of a complex smart card such as the German ID card requires the implementation of a variety of chip card commands in accordance with ISO/IEC 7816, including the protocols of the BSI TR-03110. HJP Consulting was able to provide a fast introduction to the project because of their long-term experience in developing simulators in the area of official ID documents. The first version of the simulator was therefore already published on the project's website in December 2013.

Simulation of a Java Card

The simulator mainly consists of two different modules. One module describes the actual card application; the other module describes the interface between card application and the outside world, meaning that commands are received from the card reader and forwarded to the simulator. The card application represents the actual simulation of the electronic ID card. All cryptographic protocols described in [1], which are essential to the functions of the electronic ID card, are implemented within this module. A detailed description of each protocol and security mechanism can be found in [3]. Below are the protocols of the Extended Access Control (EAC) protocol family, which are relevant here:

- Password Authenticated Connection Establishment (PACE)
- Terminal Authentication (TA)
- Chip Authentication (CA)
- Restricted Identification (RI)

All of these protocols are implemented in the simulator, which allows a complete simulation of the eID function. This includes all cryptographic methods of the TR with all possible key lengths, starting with Triple-DES to AES with 256-bit keys.

Aside from the protocols, the actual data on the eID card play an important role. There is a differentiation between document-specific data such as the indication for cryptographic methods or associated key lengths, and owner-specific data such as the name or place of residence of the document holder.

The simulator already contains a data set with plausible sample data ("John Smith"). The preconfigured cryptographic methods and key lengths are consistent with the ones chosen for the current eID card. Therefore, PersoSim can be used out-of-the-box with reasonable and plausible data. To access the real electronic ID card, the service provider needs the appropriate certificate, which must be applied for at the Federal Office of Administration (Vergabestelle für Berechtigungszertifikate, VfB). It is not possible to gain full access to the stored data without one of these certificates. Within the PersoSim project it is also planned to use test certificates. In this case, the simulator will contain test certificates derived from the corresponding test PKI by the BSI. Thus, the PersoSim standard configuration already includes certificates, allowing the service provider or the user to access the data.

The current simulator is part of the product family GlobalTester. The GlobalTester basic version is also an open source project to test smart cards⁴. GlobalTester has been successfully used for many years, and the experience gained through this use is now incorporated into the PersoSim project. The simulator of the GlobalTester product family was also used to reproduce an example of the protocol sequence of the electronic ID card [4]. With the simulator both sides of the communication are represented (terminal and chip). The simulation allows the provision of the information and keys calculated inside the chip, which are usually not accessible. The simulator of the PersoSim project has

been implemented using Java programming language. Specifically, it comprises a reduced Java version⁵, which allows the execution of Java Card applets. The Java Card Platform had been chosen to enable an implementation close to smart cards. As Java is very well known, software developers gain a fast and cross-platform introduction to the PersoSim project.

The simulator has previously been connected through special hardware, which provided the communication via the radio frequency interface for contactless smart cards according to ISO/IEC 14443 [7]. The use of this dedicated hardware (Comprion CLT One) is impossible or difficult to finance for the typical user of PersoSim. Therefore, an alternative communication interface has been developed within the PersoSim project: a virtual card reader.

Connection via virtual card reader

As already described, the use of additional hardware to directly access the simulator is not foreseen in this project. For this reason, a virtual card reader is provided in order to communicate with the simulator. After the virtual card reader is installed on the user's system, it acts as an actual card reader for the operating system. This "card reader" is merely a driver that registers itself as a new card reader in the operating system.

Figure 1 (below) shows the relevant layers that a command has to run through when using hardware on the one hand and a virtual card reader on the other.

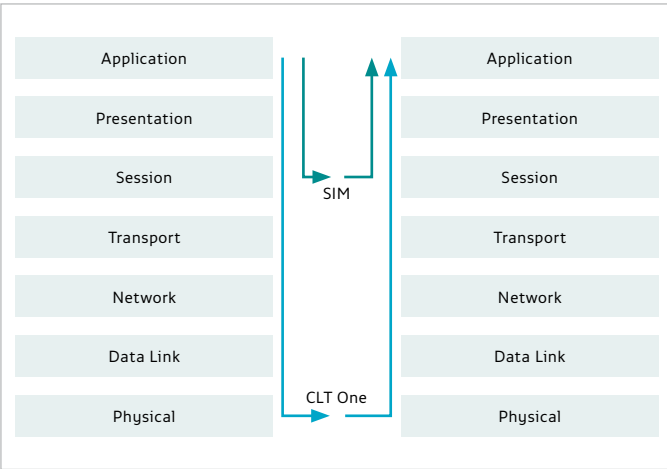


Figure 1: ISO-Layers of the simulators

Today PersoSim supports the following operating systems:

- Microsoft Windows 7 (32 and 64 Bit),
- Microsoft Windows 8.1 (32 and 64 Bit),
- Ubuntu Linux 12.04 LTS (32 and 64 Bit).

The source code of each driver is provided as well, to allow users to compile suitable drivers for other Linux derivatives on

¹ <http://www.persosim.de>

² <http://www.bsi.bund.de>

³ <http://www.hjp-consulting.com>

⁴ <http://www.globaltester.org>

⁵ <http://www.oracle.com/technetwork/java/javacard>

their own. The virtual card reader enables the use of the simulator in any application that uses a connection to a card reader. In the context of electronic identity cards, these are primarily the eID clients, which are locally installed by users and implement the communication between the chip and the eID server. The following eID clients are currently available:

- AusweisApp⁶ (Bund, BSI)
- AutentApp⁷ (Governikus)
- Open eCard App⁸ (Open eCard Team, ecsec)
- PersoApp⁹ (Fraunhofer SIT, TU Darmstadt, ageto)

The virtual card reader enables the user to simulate all three reader types relevant to the electronic ID card — basic, standard, and comfort reader. For this purpose, the drivers have access to an additional Java package that supports the functions of the card reader. This approach gives all virtual drivers a way to access a library with additional functions that is independent of the operating system being used. The driver of the basic reader can simply forward the commands to the simulator. Standard and comfort readers offer additional functionalities beyond forwarding commands. The technical guideline TR-03119 [5] describes all the functions that the card reader needs to support in the context of the electronic ID card, such as the functions of a PIN pad to enter passwords. Furthermore, [5] requires that this extension delivers the status information of the driver. This package also includes necessary commands, such as EstablishPACE. The great advantage of this approach is that the logic of the additional functions can be encapsulated in a single package available on both operating systems. Thus, the virtual driver only has to keep information specific to the operating system, and the logic can be developed and maintained in one single location.

Figure 2 (below) illustrates the structure of the virtual card reader:

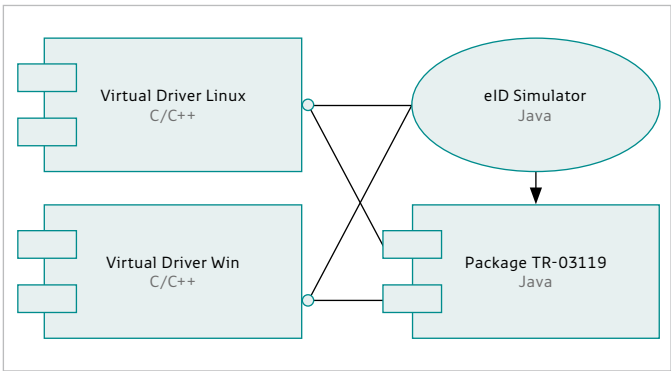


Figure 2: Architecture of the virtual driver

The simulation of a PIN pad can closely model the typical characteristics of a standard or comfort card reader. Since the drivers described here are primarily used in combination with the simulator for test purposes, the input of a password such as PIN or

CAN via the virtual PIN pad appears to be somewhat cumbersome. For this reason, a configuration option for the driver is available that allows passwords to be stored instead of entering them each time the simulator or the card reader is addressed.

The Open Source Community

Building and maintaining a community is an important part of an open source project. We differentiate between the user community and the developer community. The success of an open source project relies heavily on the participation of users and developers. Only through the collaboration of different users and developers with quite different interests does the open source project become alive. The PersoSim project released the source code under the GNU General Public License v3.0 (GPLv3), so that any extensions that are based on the original version are in turn made available to the community. The GPL is the first Copyleft license for general use, which ensures that modifications or derivatives of GPL-licensed works may be published only under the same license terms.

Advantages of Open Source

The savings in license costs and the possibility of customizing the software according to user needs are, from a user perspective, two of the most important reasons for choosing open source software (OSS). Furthermore, in addition to the open standards — especially important when using a simulator such as PersoSim — vendor independence is an important argument in favor of using OSS. PersoSim provides a simulator platform that can be used by other firms as the basis for their developments in the field of smart cards. Performance and technical quality are other arguments often used to promote OSS, because the principle of “more eyes see more” applies here as well. The worldwide developer community has access to the source code and can detect and solve problems if necessary. These reasons, as well as the positive experience of HJP Consulting with the OSS test tool GlobalTester, led to the decision to set up the PersoSim project as an open source project.

User Community

A dedicated website has been created for PersoSim users (www.persosim.de). In addition to a brief introduction to the PersoSim project, the user has access to all of the information needed to operate the simulator. The website provides the latest version of the simulator and the appropriate virtual driver. Besides the common documentation describing the use of the simulator, the user will also find a list of frequently asked questions and the contact details of the people behind PersoSim.

The BSI and HJP Consulting inform the community about news and updates through this site. The website therefore serves as an introductory page for the PersoSim project, with a primary focus on the user.

Developer Community

In addition to the user community, a developer community has been established. Interested developers will find in-depth information beyond the operation of the simulator. A developer can view and download the source code. Information about compiling the source code should enable the developer to translate the code. Since the simulator is implemented in Java, compiling is no great challenge. It is more difficult, however, to translate the driver for the virtual card reader running Microsoft Windows. To compile Windows drivers, the commercial development environment from Microsoft itself is needed. Test versions of the development environment are available online. In the PersoSim project all necessary files for the Windows drivers are provided, so that developers can translate those themselves.

To promote the exchange among developers, different options are offered:

- documentation (architecture of the simulator, instructions for compiling, etc.)
- wiki (short descriptions of functions, etc.)
- bug-tracking (detection and management of errors in the simulator or the drivers)
- coding guidelines (promotion of consistent source code)

PersoSim provides the developer community with an infrastructure that encourages the further development of the simulator. Employees of HJP Consulting took over the moderator role for the community and deliver the source code for the project.

Simulator on NFC device

In the next stage of the simulator’s development, the entire functionality of PersoSim shall be implemented on mobile NFC devices such as smartphones. Instead of the virtual card reader, the NFC interface of the device is used for the communication of the card reader with the other components (see Figure 3).

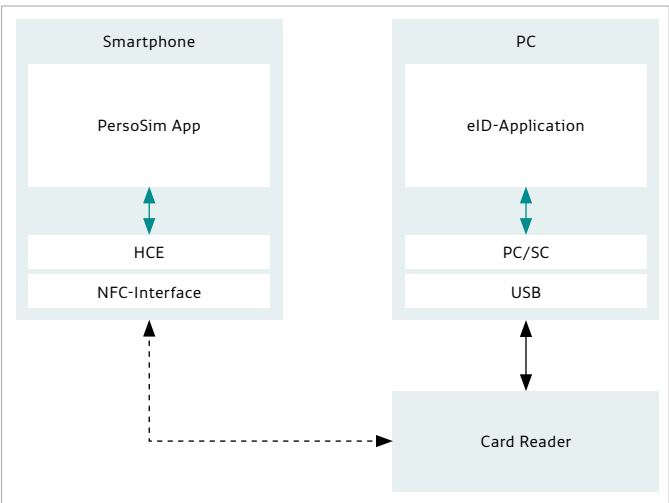


Figure 3: Architecture of NFC-Smartphone

The use of PersoSim on smartphones opens up more application areas — for example, its use on stationary terminals or machines with eID-support that do not allow access in order to install the virtual card reader. NFC-capable smartphones with the Android operating system are currently most suitable for this implementation, as they offer a well-documented API in order to access the NFC interface. Open source projects such as androsmex¹⁰ or the mobile versions of the abovementioned Open eCard App and PersoApp already use the NFC interface in Android to communicate with the German ID card. These apps use the NFC interface in Reader/Writer-mode. For the simulation of the smart card on an NFC-capable smartphone as planned in PersoSim, the Card-Emulation-mode will be used. With the Android version 4.4 (KitKat),¹¹ the "Host Card Emulation" API has been introduced (HCE), which is a service on an Android device that allows the user to generate a virtualized smart card. HCE emulates an ISO/IEC 7816 [6]–based smart card that uses the contactless protocol ISO / IEC 14443-4 [7] (ISO-DEP) for communicating via the NFC interface of the device.

Since PersoSim is already implemented in Java, the program code can be ported onto the Android platform with little effort. Adjustments will be necessary, especially in the GUI, as well as in the connection to the NFC interface. Instead of connecting via a virtual card reader, under Android the HCE-API will be directly accessed.

Conclusion and Outlook

PersoSim offers interested users an uncomplicated way to simulate the electronic ID card and thus verify their own implementations. In addition, the simulator enables users to understand the cryptographic protocols on the integrated chip.

Although the simulator is currently limited to the electronic identity card (nPA), it can be extended to other protocols in the future without any problems. Ultimately, the simulator can simulate all smart card protocols using common commands from the ISO/IEC 7816 [6]. It has the potential to create a universal open source platform that can simulate a wide variety of smart card applications in the near future. Such a platform could increase and enhance possible applications for smart cards even further. ☒

Literature:

- [1] BSI: TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1 – 3
- [2] Tobias Senger, Holger Funke: An open source eID simulator. Proceedings of Open Identity Summit 2013, GI-Edition, 2013
- [3] Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD – Datenschutz und Datensicherheit 32(3), 2008
- [4] BSI: Worked Example for Extended Access Control, Version 1.02, 03.08.2011
- [5] BSI: TR-03119: Requirements for Smart Card Readers supporting eID and eSign Based on Extended Access Control, Version 1.3, 22.03.2013
- [6] ISO/IEC 7816 Identification cards – Integrated circuit cards
- [7] ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards
- [8] Holger Funke, Tobias Senger: PersoSim. DuD – Datenschutz und Datensicherheit 4/2014

¹⁰ <https://code.google.com/p/androsmex>

¹¹ <http://developer.android.com/about/versions/kitkat.html>

Turning to citizen-centric solutions for government ID

By Rob Haslam, HID Global

The trend towards citizen-centric electronic ID (eID) and ePassport solutions has been growing in popularity over the past several years. Governments are increasingly recognizing the need to address the very real and specific needs of their populations. In 2014 we expect to see this movement transition from a trend to being the norm. At the heart of this trend is the need to meet citizens where they live. No longer can governments expect remote populations to expend the time or money to travel to city centers to secure new ID cards. While the general population has become more mobile, governments around the world are also learning to be more flexible and mobile in the delivery of IDs and services. Mobility in the secure issuance and delivery of ID cards can take a variety of forms. Some government are implementing distributed issuance systems, others are leveraging hybrid programs combining elements of centralized issuance with decentralized issuance and in some cases, governments are implementing successful mobile issuance systems to meet the unique needs of its geographically dispersed citizens.

□ Social dynamics driving the need for flexible issuance solutions

As citizens in more mature markets increasingly bring a “consumer” mindset to their everyday lives, governments are looking for identity solutions that meet growing expectations for easier, more convenient and more accessible services. Beyond the accessibility of services, citizens today also expect the instant issuance of secure IDs for faster processing, added convenience, and time- and cost-savings. The good news is that a new wave of distributed identity personalization technologies is capable of replicating the output of large centralized facilities with greater efficiency and economies of scale.

From a global perspective, large population pockets often exist in remote or outlying areas far from a central ID issuance

facility and for those citizens, it is neither feasible nor economical to travel what can be hundreds of miles to enroll or renew an ID card. Whether in smaller city centers, geographically remote locations, or dispersed areas, the value proposition of ‘instant on-site issuance’ through the decentralization of enrollment and issuance solutions is real. 78% of professionals surveyed in a recent study by Secure Document World believe that decentralization will make life easier for citizens; 53% believe that it will enable cost-effective delivery of IDs. The majority cited convenience, scalability and flexibility as key reasons this trend is taking hold. Adding to this equation is the opportunity for governments to create new revenue streams and at the same time offer new, local employment opportunities.

This paper provides an insight to how governments around the world are adopting a mix of mobile, distributed and centralized issuance solutions to meet the demand for citizen-centric services.

Angola: Flexible and modular approach



The Republic of Angola provides a great example of a country that puts its citizens at the forefront designing an eID program that addresses the needs of a geographically dispersed population.

Angola, facing the challenges of providing counterfeit-resistant proof of identity to a large and widely dispersed population, implemented a nationwide program that addresses this complex need. Central to the success of this program is a mobile card issuance system that reaches all citizens, even in the most remote rural areas.

In the mid-2000s, Angola began its search for a replacement for its paper-based citizen ID document. The use of false documents and ID theft exposed the nation to increased security concerns at a time when its new democratic government was being established and global insecurity was on the rise. The government’s vision was to provide one legal identity per person as a cornerstone of citizenship. And with its citizens’ interest front and center, the Angolan government decided to design the card for additional functions including proof of the right to vote, and possible access to multiple government services.

To meet the needs of Angola’s widely dispersed and predominantly rural population, the government needed a solution that would allow for distributed data capture and issuance. HID Global delivered a decentralized card personalization solution, deployed in approximately 60 fixed and mobile personalization centers throughout the country.

With a focus on the safety and security of its citizens, the new Angola National ID card meets multiple criteria. Angola’s National ID card contains state-of-the-art high resolution and multi-color security offset printing, including covert features and special links. The card also features optical security media, a highly secure, machine-readable technology. The absence of any communications infrastructure required the ability to instantly read the card’s data without access to a network plus modular and mobile data collection and card personalization systems.

From the start, HID Global worked closely with the government of Angola and its contractors to fulfill the nation’s vision for a sophisticated ID program that meets the on-the-ground realities of its population, climate and security challenges. The close collaboration resulted in a well-managed and effective system, with stable and reliable mobile card issuance.

Costa Rica: A citizen centric foundation



Costa Rica is an unusual example of a country for which ‘citizen-centric’ was at the core of its national identity programs. Costa Rica’s rapidly developing economy represents a strong attraction for regional economic migrants. With a population of over four million, Costa Rica is host to some 200,000 legal foreign residents. Easily counterfeited, paper-based foreign resident credentials had created social, economic and security problems. With hundreds of thousands of illegal workers placing heavy demands on the nation’s social welfare system, Costa Rica decided not only to replace insecure ID documents for legal residents, but to revise its legislative and constitutional framework to include one legal identity per person as a human right. Today the rights of citizens and legal foreign residents are protected through the secure issuance of identity cards to legal residents.

Specifically, Cost Rica’s citizens’ rights and legal privileges are now protected while legal foreign residents are assured access to the country’s social services.

To address the needs of Costa Rica’s geographically dispersed population of legal residents, applicant data for enrollment/renewal is captured at multiple local and remote locations. In order to provide foreign residents with maximum convenience, time and cost savings, the government turned to HID Global to implement a complete ID management system to control the entire process, from data capture to credential issuance. The system remotely collects data for document authentication, adjudication and vetting; the data is then sent to a main system server database, where separate unique applicant check systems verify the authenticity of the information. This integrated, modular issuance management solution also provides biometric-based checks at every stage of data capture, enrollment and issuance to prevent tampering, duplication and interference whether at a local or remote location

The Costa Rican government selected proven credentials based on the same optical security media platform as the successful U.S. Permanent Resident Card (Green Card) program. The new Costa Rican Foreign ID card incorporated multiple counterfeit-resistant features, machine-readable biometrics and secure data storage to prevent fraudulent alteration and withstand multiple years of use.

Flexible, mobile issuance solutions around the world



In Argentina, San Luis State is a pioneer in leveraging technology to improve government services. San Luis State needed an issuance system that could produce 400,000 eIDs a year, help improve the government's revenue stream, modernize the State's services and establish a flexible and scalable services platform. The end solution effectively combined centralized and decentralized issuance consisting of 75 new printers featuring the latest in advanced printing technologies. The State's new eIDs offer multiple application capabilities as well as co-branding opportunities.



Another example is Mexico City's recent driver's license project. As one of Latin America's largest cities, Mexico City has a huge population spread across a wide expanse – 9,640 KM. To address this enormous challenge, the city set out to create multiple secure card issuance points within each of the city's 56 boroughs and municipalities. Mexico City now has 159 scalable, decentralized secure printing systems spread throughout the city that together form a future-proof infrastructure.

Citizen-centric innovations beyond card issuance

Beyond innovations in secure card issuance, we are seeing governments address the needs of citizens through multi-technology eIDs and related services. The 1990s saw the evolution of IDs from paper-based documents to electronic credit card-sized credentials that are capable of integrating a number of security features. By the middle of the 1990s, government projects increasingly called for powerful multi-purpose ID credentials that could maintain the highest levels of security while also fulfilling functions such as entry into secure facilities, faster border crossing, driver's license services, vehicle registration, ID for voting privileges, and health care services among others. eIDs and ePassports have gradually pushed the level of security and functionality to new limits, providing benefits such as greater convenience and time-savings to citizens and travelers. For example, the increased adoption of e-Gates, which automate the border control function, are currently operating in more than 40 airports across Europe and Asia. This citizen-centric innovation allows travelers to pass through gates in as little as 30-45 seconds while also lowering costs by significantly reducing manpower requirements.

Similarly, new advanced ID cards carrying one or more technologies are at the heart of the new more citizen-centric eID ecosystem. This complex ecosystem fulfills a number of interdependent objectives, many of which are directly or indirectly citizen-centric:

- Perform multiple levels and types of authentication
- Leverage an extremely secure transactional framework
- Integrate with existing IT infrastructures
- Achieve economies of scale and administrative efficiencies
- Enable e-government transactional services as well as secure identity through physical and logical access
- Future-proof to expand functions at a later stage in the program

The trend toward viewing citizens as consumers is only going to grow in the next decade. As citizens' experience with technology increases, citizens' expectations also expand. No matter the country... no matter the unique needs of the local population... the design and issuance of secure electronic ID solutions have evolved to reflect the needs of citizens. Governments are viewing citizens as consumers, patients and clients. As such we will continue to see increased security and mobility (in the delivery and authentication as well as the issuance of IDs), improved productivity, more time- and cost-savings and an overall emphasis on comfort and convenience for citizens. Governments throughout the world are rethinking how they protect their borders and deliver e-services to their citizens. Once the trend, citizen-friendly programs are becoming the norm. ☒



Secure identification systems
from Giesecke & Devrient

Creating Confidence. G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport and border control systems, ID card solutions and have become a trusted adviser and supplier to governments. We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. G&D will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards. ID system implementation by G&D – individual, international and secure. www.gi-de.com



Giesecke & Devrient
Creating Confidence.

SECURING *sensitive* DATA

By Marcel Hartgerink, WIBU-SYSTEMS BV and
Tom Kevenaar, GenKey

The use of biometric identification solutions are becoming more and more commonplace, delivering many advantages in the healthcare, financial, travel and immigration, government and many other commercial areas. The use of biometrics as a means to support fair elections is also becoming increasingly common, particularly in emerging democracies where often no up-to-date administration of citizens is available. It is for this reason that countries such as Ghana, Nigeria, Kenya and the Democratic Republic of Congo have adopted fingerprint-scanning technology to enable fair and transparent elections.

Polling Station
Here



□ Ghana, for example, successfully deployed biometric voter registration and verification in their 2012 general elections involving more than 14 million voters. Biometric technology, however, brings its own particular social and technological challenges. Because biometrics affects an individual’s privacy and misuse in a political election could have significant ramifications to its citizens, it is critical that personal information remains secure, data is protected and software cannot be tampered with.

Selecting the right technology partners

To address the concerns of double registrations, the Electoral Commission (EC) of Ghana selected GenKey as its biometrics technology partner. GenKey, headquartered in the Netherlands, specializes in delivering biometric solutions for elections, digital healthcare, and other large-scale identity management applications.

GenKey’s challenge was to contribute to fair and transparent elections in Ghana using biometrics while at the same time protecting the sensitive data that is used in the process. Their approach was to:

- Use biometric voter registration to capture biometrics and enroll prospective voters
- Use large-scale biometric-based deduplication to obtain a clean voter list
- Use biometric voter verification to ensure only eligible voters were able to cast their vote and to prevent multiple votes by the same person

GenKey’s unique privacy enhancing technology allows for storage of biometric information such that it is intrinsically privacy protected. GenKey ensured the security and integrity of its software and of the collected data by using the CodeMeter Integrity Protection and Licensing platform developed by Wibu-Systems AG, a German-based security technology leader in protecting digital assets, intellectual property, and embedded software, such as GenKey’s biometric software solution.

Biometric voter registration

Biometric voter registration was conducted at more than 23,000 registration centers across Ghana between March 24 and May 5,

2012. Over 32,000 temporary staff were trained to operate the mobile biometric registration kits containing GenKey technology. The registration kits enabled the electronic collection of biographical information, a facial picture, and fingerprints of all ten fingers from each voter. Immediately after registration, each applicant received a voter ID card, which included the person’s photograph and a bar code with a unique ID card number. Over 14 million voter ID cards were issued.

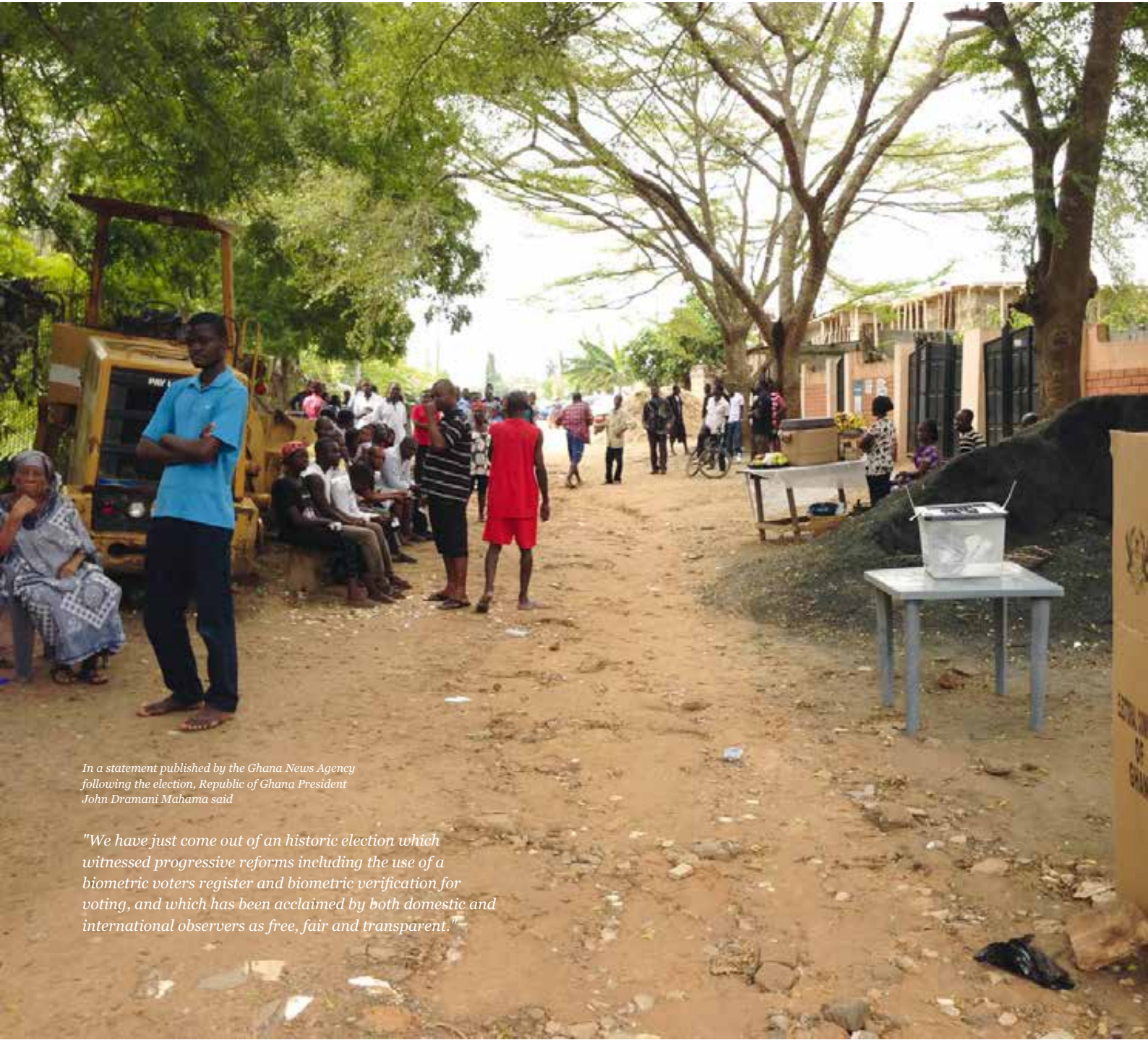
At the end of each registration day, the collected registration data (including the biometrics of the applicants) were sent to a central system, where a biometric duplicate check was performed by GenKey’s Automated Biometric Identification System (ABIS). The ABIS system detected a total of approximately 60,000 candidate duplicates, which were forwarded to an adjudication system to determine whether it concerned fraudulent cases or not.

Biometric voter verification

To verify the identity of eligible voters on Election Day, GenKey delivered 33,500 handheld Biometric Verification Devices to the polling places, where they were operated by 26,002 trained officers. Biometric verification of a voter started with comparing the Voter ID details on the card to a master voter registry, scanning the barcode to display the photograph, and comparing the picture on the device display with the voter. If they matched, the fingerprint of the voter was then scanned for final verification. If the verification was successful, the voter was issued a paper ballot to vote.

Protecting the device software and integrity of biometric data

To secure its software code against tampering in the field, GenKey integrated Wibu-Systems CodeMeter protection platform. Each verification device was loaded with GenKey software before it was shipped to a polling station. CodeMeter encrypted the code using both symmetric and asymmetric encryption. The program code was encrypted using symmetric 128 bit AES encryption. Upon starting the application, asymmetric encryption of the digital signature was employed. CodeMeter bundles the encrypted code with a license file so that when the system boots up, the embedded software calls this file, using a digital signature to verify its authenticity. A list of conditions is then verified such as the validity of the license, or the matching of the hardware features that were initially bound to the license during the encryption process, and



In a statement published by the Ghana News Agency following the election, Republic of Ghana President John Dramani Mahama said

"We have just come out of an historic election which witnessed progressive reforms including the use of a biometric voters register and biometric verification for voting, and which has been acclaimed by both domestic and international observers as free, fair and transparent."

thus protects the integrity of the device. To ensure privacy of the data, GenKey stores biometric information in an intrinsically private format so that the information is impossible to trace.

The combined GenKey and Wibu-Systems protection solution ensured a high level of security and integrity of biometric data. It also protected GenKey’s software against potential counterfeiting and misuse during the polls.

In a statement published by the Ghana News Agency following the election, Republic of Ghana President John Dramani Mahama said “we have just come out of an historic election which witnessed progressive reforms including the use of a biometric voters register and biometric verification for voting, and which has been acclaimed by both domestic and international observers as free, fair and transparent.” ☒



DATA SECURITY begins at the *FACTORY GATE*

By Thomas Löer, Bundesdruckerei GmbH

Something that just a while ago was completely inconceivable has now become second nature: smart phones, laptops and tablet PCs allow us to interact and consume no matter where, no matter when. But users who fail to persistently protect their data during all of these many Internet activities will soon fall prey to misuse and fraud. For years now, cybercrime has been growing continuously. Around one million people are affected by this every day and European Commissioner for Home Affairs, Cecilia Malmström, estimates that victims world-wide lose around €290bn each year.

□ Data theft on the rise

Stealing digital identities in particular has become a lucrative business as this data is traded via a well-organised underground economy. In its latest Norton Cybercrime report, software supplier Symantec demonstrates that around one third of all cases remain unsolved. Not only do victims frequently have to pay for goods they never ordered, they also have to deal with negative crediting ratings or even arrest warrants for crimes which they did not commit.

Insufficient data awareness among private users

German IT expert Arne Schönbohm estimates that more money is already being earned globally with cybercrime than with drug dealing. This means that political initiatives like the planned EU cybercrime centre are certainly correct and mark an important step in the right direction. But in order to put a lasting end to Internet crime, Internet users themselves must become more attentive and must do more to protect their private PCs and data. That being said, in Germany alone almost half of all social network users disclose vast amounts of personal data and have thus created the ideal situations for identity misuse and theft.

The private sector calls for new solution models

However, the danger of sensitive information, technology and knowledge falling into the wrong hands is growing not just in private homes, but also at companies, public authorities and institutions. Regularly changed passwords, encrypted e-mails or heavily secured IT infrastructures are no longer sufficient to protect organisations today against data theft.

What we now need are comprehensive solutions that already act at the factory gate and cover all organisational structures. Bundesdruckerei's new Full ID | Governance solution kit is the answer. After September 11, 2001, which completely changed the global perspective of security, the world-wide introduction of electronic travel documents already began driving the development of high-security technologies to protect secure identities. Today, in light of daily reports on stolen data or data misuse, we are once again experiencing dramatic change. Companies, public authorities and institutions everywhere have to arm themselves to fight cybercrime and would do well to protect their technologies and knowledge with new and flexible solutions.

Consistent concepts for improved data protection

With this claim, we have combined in our new solution kit a large portfolio of system modules which are specially tailored to the requirements of small and medium-sized companies and when combined actually begin to work at the customer's door.

Take, for instance, reliable visitor management. In order to ensure that guests are clearly identified and actually enter permitted areas only, we employ devices which enable security staff to check within a matter of seconds whether the ID documents presented are genuine and to issue smart visitor ID badges. These devices can of course be equipped with a host of additional functions and flexibly defined access rights. In order to avoid annoying waiting times, guests can enter their data at self-service terminals or in advance on their own PCs.

Once the first security gate has been successfully mastered, integrated building and infrastructure management can define precisely which rooms and technical infrastructures can be used by whom and when.

This also applies to a large extent to communication. Here, the system supports the use of electronic signatures, encrypted e-mails or files and also guarantees reliable VPN access, networks and servers. This ensures that information that is to be communicated

internally or exchanged with selected third parties only reaches the right address via secure channels. With supplementary user and rights management, we additionally create reliable protection, also for the company's own PCs, systems and machines, thanks to flexible control of use times and access rights.

The Full ID | Governance solution kit is rounded off by efficient document and workflow management which is used to control all release processes that occur in a process chain. This also benefits personnel management, for instance, which we provide with special tools for recording work and project times, for processing holiday applications or for updating master data.

If necessary, the complete solution can even be supplemented by bespoke eLearning systems for compliance management, by services in payments or by a state-of-the-art credit card function.

Advice and support included

With the vast amount of options on offer, it goes without saying that Bundesdruckerei also helps its customers in every way to achieve optimum implementation and integration. In this way, users of the Full ID | Governance solution kit not only benefit from the diverse range of individual components available, they can also rely on our experience and expertise when it comes to analysing requirements, technology and project control, as well as matters related to service, maintenance and support. Any additional services which may be required in conjunction with certificate management can also be taken care of by D-TRUST, our trust service provider.

Greater data security for small and medium-sized companies

With this range of supplies and services, we specifically want to reach small and medium-sized companies who do not have the resources needed to increase their security level as required. Compliance management is in our opinion another important topic in this area. In addition to being aware of internal company rules of behaviour, employees should also be familiar with and observe current regulations. That's why we also offer special related eLearning programs and on-site training as part of our Full ID | Governance solution.

Integrated approach towards ideas and action

Our most recent EasyPASS project is further proof that integrated concepts of this kind can lead to greater security and process efficiency. With this project, we were able to meet the requirements for a pan-European tender for automated border control systems.

As one of the world's leading system suppliers of high-security technologies, not least with the German ePassport system, the new German ID card or the electronic residence permit, Bundesdruckerei has also made a name for itself in complex government application fields as well as in many areas of the private sector. With this experience, we will have installed a total of 90 state-of-the-art eGates at major German airports by the end of 2014 and together with our consortium partner Secunet Security Networks AG we are also responsible for design and commissioning, as well as maintenance and support.

Just like with the Full ID | Governance solution kit, in this case too the basic component is a document verification system at the entrance to the eGates. Other components of this Full ID | Border solution include an integrated camera system for comparing the face in the gate, a monitoring system which can be used to control the individual functions of the eGate, as well as a background system that is used to configure all the settings and control rules.

The benefits are obvious

With perfectly matched system modules like these which are geared to highly specialised applications, border control officers will be easily able to adapt the control rules of an eGate to national and local security situations and at the same time network information from various different sources. However, the authority to evaluate and decide basically remains with the user as is the case with Full ID | Governance solution kit. This means that in addition to boosting the process efficiency of border controls, comfort for travellers will also improve significantly. All of this is possible without having to make any concessions where a consistently high level of security is concerned.

Datability – A challenge and task of tomorrow

Surrounded by terms like cloud computing, smart living, smart grids, M2M communication or NFC, the term "datability" – the motto of this year's CeBIT and a signal for improved, sustainable and responsible handling of data and identities – already describes one of the major tasks of tomorrow. In order to master future challenges, we not only need highly innovative solutions and products, we especially need system know-how that has grown in many different technology applications.

With a track record that dates back 250 years, our company has repeatedly demonstrated that we have the determination and capability to master change. That's why for us today Full ID | Management and Datability mean actively helping the private sector, public authorities and institutions to make their processes and data more secure by employing all of our expertise and all the necessary technologies and services which we can now supply from a single source. ☒



The officer's
best friend.

Thanks to the KINEGRAM®, the authenticity of banknotes and government documents can be checked by the naked eye.

For banknotes: LEONHARD KURZ Stiftung & Co. KG
Schwabacher Straße 482 | D-90763 Fuerth | www.kurz.de | sales@kurz.de

For government documents: OVD Kinegram AG | Member of the KURZ Group
Zaehlerweg 12 | CH-6301 Zug | Switzerland | www.kinegram.com | mail@kinegram.com

KINEGRAM®

Multi-Access ID Card for every Russian citizen

By Andrey Golushko, JSC Mikron

In January 2013, the Russian government introduced the Universal Electronic Card (UEC), which is a combination of an ID document and payment card. The UEC is currently issued on a voluntary basis, but is expected to become obligatory for all 143 million Russian citizens in 2014.



□ All-inclusive ID and payment card

With the UEC, the Russian government plans to offer an all-inclusive ID and payment instrument, accepted everywhere across the country on federal, regional, and municipal level, used by all state institutions (revenue and customs or the driver's licence registration authority, for instance), and for a wide range of financial activities. The card is supposed to become a universal tool for banking and payment, including mobile wallet transactions, payments for commercial and state goods, and many more. The card is expected to be universally accepted across all payment terminals, including contactless payment methods. Yet, it could also be used as transportation card or provide access to health services as a medical electronic card and replacement for insurance certificates.

Universal ID document

The Universal Electronic Card (UEC) is a personalized smart card, which confirms that the holder is entitled to receive federal, municipal, and other services. The card's dual-interface chip contains the following personal details: name, place, date of birth, individual insurance account in the pension insurance system, mandatory health insurance policy number, and Bank Identifier Code (BIC).

Citizens can also use the card to find out who has requested their information, when, and why. The functional implementation of the UEC is provided by two electronic applications - identification and a bank application located on the integrated chip.

Versatile tool for federal and municipal services

The UEC is a convenient and versatile tool, providing quick and easy remote access to public informational resources, meant to legally bind citizens' electronic communications with public authorities and businesses. The UEC is meant to simplify bureaucratic procedures and improve the availability of service reception as well as the quality of public services. For instance, it offers the possibility of receiving wages and salaries, pension payments, social allowances, and benefits provided by regional and federal legislation. It enables its holder to carry out legal procedures remotely without personal presence (electronic signature).

Potential commercial services

The UEC is the key to a wide range of public and commercial services, including debit card functionality. The UEC could

provide storage and use of electronic tickets, coupon codes, and others, also via a contactless interface. In the field of sports, it could be used for various applications, such as gym memberships for instance. Another possible advantage is the access to cultural sites, including electronic ticket purchases. Furthermore, it could serve as a products and services selection platform to choose the most suitable car insurance, for in-stance, but also for further registration using digital signature. Benefits for car owners might include information about fines payments, parking fees, and more. The UEC could also provide a set of services for individual entrepreneurs, such as receiving payments from customers or filling in and submitting tax documents.

The chip operating system

Mikron, the main company of Sitronics Micro-electronics' business division, received approval from the federal authorized organization JSC UEC, allowing the use of Mikron's card platform (a microchip and the built-in operating system) with payment and identification applications for universal electronic card emission. The certificate issued by JSC UEC confirms that Mikron's chip module provided for the check with preset identification and payment applications corresponds to the requirements of the uniform payment and service system "Universal

Electronic Card" (EPSS UEC) and the UEC identification application specification.

UEC applications and characteristics

The UEC contains two mandatory federal applications (identification and banking).

- The Federal identification application includes the sector of personal customer data, the data area of the Federal Executive authorities of the Russian Federation (FFOMS, Pension fund, etc.), a specialized application for the formation of reinforced qualified electronic signature
- The unified payment service system provides the ability to use the card as a usual payment card, namely the instrument of cashless payment for all the goods and services consumed in the territory of the Russian Federation.
- A regional data sector is available for recording for each region with its powers.
- An additional regional application can be placed (transport application for instance).
- UEC has a contact / contactless interface with the ability to emulate Mifare.

UEC payment service EPSS

The unified payment service system "UEC" PRO100 is integrated into the EPSS

- Technically, this product is based on EMV M /Chip used by MasterCard
- PRO100 service does not require replacement of terminal equipment, and it does provide the ability to use the card as a usual payment card for all the goods and services consumed in the territory of the Russian Federation.

Russia's universal eCard goes live

The UEC project is recognized as a very significant e-government project to improve quality and efficiency of public services, increase accuracy of settlements with the state, or prevent fraud in services for the card owners. But it is also a challenge for a country the size of Russia. Of course, UEC still has some steps to go before the vision is a reality but the underlying technology, the UEC processing center — one of the key components of the e-government project — is already in place. In the pilot phase in 2012, 6,000 cards were issued across four test regions and tested by the employees of various state organizations and banks. The pilot proved successful and the processing centre went into full production at the start of 2013. The UEC project has now been launched throughout Russia. To date, more than 10,000 citizens have applied for the card and about 4,000 cards have been issued. ☑

The SwissPass – MORE THAN *just a card*

By Mario Voge, Trüb AG

From mid-2015, SBB, the main stakeholder of the VöV (Verband öffentlicher Verkehr = Swiss Union of the Public Transport Providers), will launch a multifunctional public transport card named 'SwissPass'. Bringing new values and services, the launch of the SwissPass marks the beginning of a new era for various markets, such as the travel, leisure or retail sectors.

□ The card itself is very classical, being made of PVC and equipped with standard optical and electronic features. The uniqueness is defined by a 'medium centric solution' – hosted by the card. This means that the medium ID is matched to the user identification. The optically and electronically personalized cardholder data does not say anything about the usability or the value of services linked to the owner of the SwissPass. Also, the individual legitimations are hosted by a system, which enables the owner of the SwissPass to link up the 'medium ID' and access different services and benefits at the backend.

The backend of the public transport sector is settled as the brain within the new era of Swiss transport and ticketing services. The SwissPass, as a legitimation for the current GA and Halbtax-Abo of the Swiss railway services, is just one out of many service options. Other railways ticketing schemes will follow step by step.

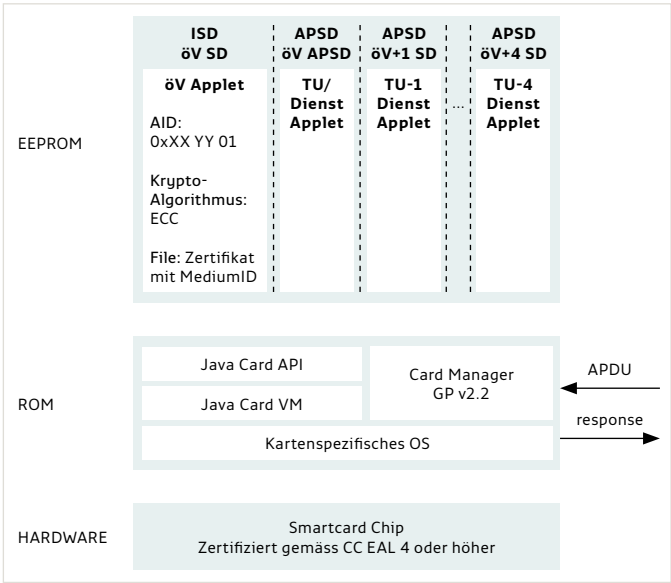
The backend will interoperate and extend with different service providers, such as Mobility (a car rental service), Velopass (a bike sharing service), Ticket Corner (a ticket service provider) as well as closed user systems.

Trüb AG was awarded as the supplier of the WTO compliant tender against significant European competitors thanks to its proven track record of RFID projects and international identity document solutions, with solid experience of complex and high volume projects. The company has profound know-how in project management and is known - and 3rd party proven or certified – for its high standards in quality and security. It will provide the complete value chain for the 20 Mio+ CHF SwissPass project, including the production of approx. 6 million cards within five years and the personalization of 160,000 cards per month within the first year of operation (peak volume 20,000 cards per day).



Technology

The card is equipped with two RFID based technologies and is a so-called ‘hybrid card’ with two separate antennas. The RFID microprocessor will host the above-mentioned ‘medium ID’ based on the ISO14443A standard. The chip has a standard CC EAL4+ certification to ensure the security of the chip platform. The RFID chip is embedded with security features of encryption: 3DES, AES and ECC (a premiere in Switzerland). The operation system is defined as Java Card v.3.0.1, a Java Global platform compliant solution (GP Version 2.2). A proprietary transport applet will ensure the secure storage of the ‘medium ID’, including certificates as trust anchors. The transponder chip is based on the ISO15693 technology allowing for the SwissPass to interlink to further services (i.e. Ski centers and leisure parks).



Source: SwissPass project

The card body is defined as a standard ID1 card according to the ISO7810 specifications. The printing will be in CMYK colors on both sides. Hidden, visual and tactile security features will ensure the level of trust. A lamination foil will ensure a service life of the cards of at least five years. A 3rd party test will prove the durability of the cards.

Realization

The joint project team of SBB and Trüb has just finished the conception phase and is now moving forward to the pilot start by Q3 in 2014.

The electronic personalization will be the premiere for Switzerland: Trüb will host a specific Certificate Authority (CA) service to generate the relevant keys and certificates to personalize a unique medium ID for every single owner of a SwissPass.

Until then, the technical realization is going ahead: The Swiss-Pass card is equipped with two ultra-violet prints at the front (Swiss map and changing numbers). Several logos and pictograms will be embedded as security features in the raw card. An overlay will enable holographic effects (transport pictograms) as a further security feature. A tactile element (RNIB notch), at the right front side, is the solution for handicapped or blind people. Several optical personalization elements will be applied out of Trüb’s comprehensive portfolio. At the front of the card, a few static (during raw card production) and dynamic elements (cardholder name, unique number (not the medium ID) and picture of the cardholder) will be printed. At the back of the card different QR codes will be printed for additional contact based services which cannot be covered by the two contactless chip modules.

As mentioned above, the electronic personalization will be the premiere for Switzerland: Trüb will host a specific Certificate Authority (CA) service to generate the relevant keys and certificates to personalize a unique medium ID for every single owner of a SwissPass.

The lettershop service as part of the fulfillment of the Swiss-Pass project is another competence field of Trüb. The main concern is to match every personalized card with the correct personalized documents (such as letters, incentives, customer level status, etc.) and with the adequate delivery options. This is a more complex task than it sounds. Due to the fact that Trüb is Switzerland’s leading supplier of banking cards the company has extensive experience in handling with such demanding services and will ensure a performance level of 99.8 %.



Business Continuity Management (BCM)

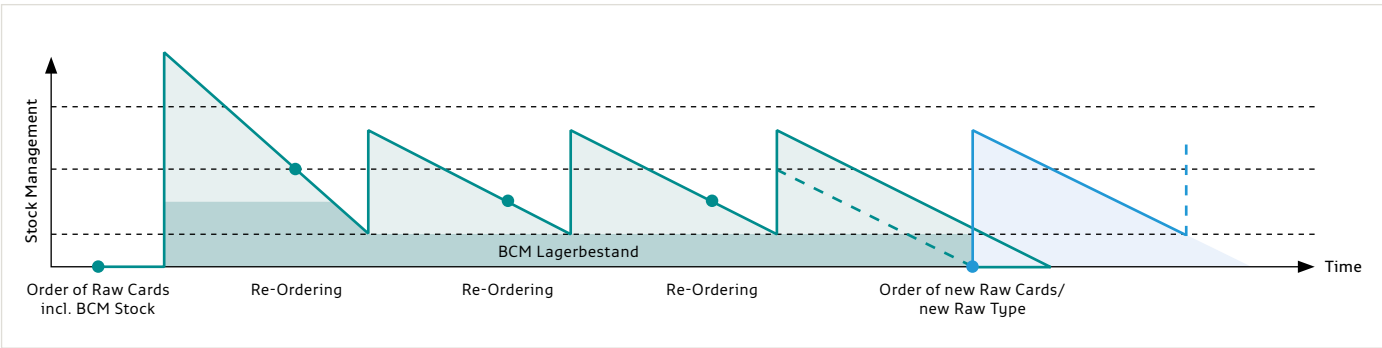
A specific requirement of the project has brought Trüb to a new level of services. The main requirements to BCM, Business Continuity Management, are to provide BCM services along the whole production cycle of raw card production and card personalization and to ensure load balancing, e.g. to act as ‘hot side’ for unexpected peak loads. The solution conceived by Trüb to meet with the challenges of a consistent BCM is based on complex and well-tuned logistical expertise. Trüb will ensure at least a stock of raw cards including chips, inlays and intermediate products at two sites. Finished raw cards will be additionally stocked at the two personalization sites. Defined quantities in stock will ensure to observe the contractual time frames for order, delivery and production workflow (see figure).

The established backup center will be defined as ‘hot site’ in order to ensure the uninterrupted services according to the service level agreements with the customers. A secure and second source data interface will enable a high level of trust and

operation services (data delivery, data preparation and production handling). All sites will be equipped with the complete range of end-to-end services for lettershop, packaging and delivery.

The future scope of the SwissPass is currently in discussion. The SBB, their partners in Switzerland and the neighboring countries are all interested in being connected to the attractive concept of these ‘medium ID’ centric services – with the objective to better serve their clients.

Trüb is today established as a partner for new services going much further than producing “just the card”. ID cards and related services will come more and more into the focus of vendors, service providers, issuers and finally also the consumers. Several countries in Europe have already established such services but with a decentralized approach, e.g. the cardholder data being stored on the card. The SwissPass is a different concept – and with it a new era has just started. ☒



Source: SwissPass project

SILICON TRUST PARTNER DIRECTORY 2014

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:

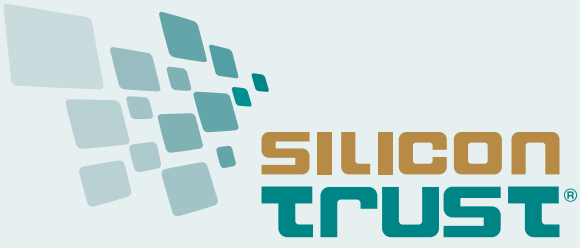
- Educating government decision makers about technical possibilities of ID systems and solutions
- Development and implementation of marketing material and educational events
- Bringing together leading players from the public and private sectors with industry and government decision makers
- Identifying 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 2011 fiscal year (ending September 30), the company reported sales of Euro 4.0 billion with close to 26,000 employees worldwide. Based on its core competencies in the fields of security, contactless communication and integrated microcontroller solutions (Embedded Control), Infineon offers a comprehensive portfolio of semiconductor-based security products for many chip card and security applications. Infineon uses this expertise to increase security in an



increasingly mobile and networked world, e.g. for mobile payments, system security and secure electronic sovereign documents. Infineon has developed innovative, hardware-based security solutions for over 25 years and has been the world market leader for 14 years.
www.infineon.com

GIESECKE & DEVRIENT



Giesecke & Devrient (G&D) is a leading international technology provider headquartered in Munich, Germany. Founded in 1852, the company primarily supplies central and commercial banks, cash-in-transit companies, and security printers with innovative technologies that render the cash cycle efficient and secure. As an end-to-end provider of smartcard and mobile security solutions, the Group develops and distributes hardware, software, and services to a client base that includes banks, mobile network operators, transportation companies, business enterprises, and original equipment manufacturers (OEMs). Governments and public authorities turn to G&D for passport, ID card, and border control systems, ensuring reliable identity verification.
www.gi-de.com

GEMALTO



Gemalto is world leader in digital security with over 10,000 employees operating out of 87 offices and 13 Research & Development centers in 45 countries. Gemalto is at the heart of our evolving digital society. Billions of people worldwide increasingly want the freedom to communicate, travel, shop, bank, entertain, and work – anytime, anywhere, in ways that are convenient, enjoyable and secure. In the public sector, Gemalto provides secure documents, robust identity solutions and services for governments, national printers and integrators in the service of citizens. Its products and solutions are deployed in more than 60 government programs worldwide, including 36 issuance and 16 enrollment projects. Gemalto is contributing to more than 25 ePassport initiatives; over 15 eID national programs and is active in all major eHealthcare schemes and numerous e-driving license, vehicle registration and tachograph projects.
www.gemalto.com



tru/window™ LOCK
A new dimension in photo-protection

INNOVATIONS IN SECURITY IDENTITY SOLUTIONS, SWISS MADE

- Secure documents in polycarbonate
- Passport datapage
- Identity card
- Residence permit
- Crew member certificate
- Driving licence
- Tachograph cards

www.trueb.ch

Absolute Identity



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.

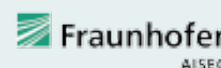
BSI



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 annual 2012 revenue of EUR 8.8 billion and 76,400 employees in 47 countries. Serving a global client base, it delivers hi-tech transactional services, consulting and technology services, systems integration and managed services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail, Services; Public, Health & Transports; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

www.atos.net

REGISTRATION
NOW OPEN

THE GLOBAL HUB FOR NEXT-GENERATION
CITIZEN & GOVERNMENT ID SOLUTIONS

SDW2014

QEII CONFERENCE CENTRE
WESTMINSTER, LONDON, UK

CONFERENCE: 16–18 JUNE 2014

EXHIBITION: 17–18 JUNE 2014

- Security documents, border control, ePassports, eID, registered traveller programmes, document design, breeder documents and anti-counterfeiting...
- Major focus on biometric technology and human identity-based solutions
- More than 100 companies exhibiting from around the world
- Register to attend the exhibition for free, or book now for preferential rates to attend the conference – the earlier you book – the lower the rate!
- Discounted rates for Government delegates – plus buy one place and get the second half price
- Lower rate conference places for delegates from African, Asian, South American and **(New for 2014)** Eastern European nations
- Conference sessions include a special focus on document examination
- Addition of conference interpretation services for French and Spanish **(New for 2014)**

IF GOVERNMENT AND CITIZEN ID MARKETS ARE YOUR BUSINESS,
SDW 2014 HAS THE ANSWERS...

www.sdw2014.com

Organised by:



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, prelamines, LaserCard® optical security media technology, and FARGO® card printers.

www.hidglobal.com

HJP CONSULTING



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

www.hjp-consulting.com

THE IDENTIV GROUP



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

www.identive-group.com

MICROPROSS



Micropross is a leading company in the supply of test and personalization tools for the smartcard industry. Active since 1979, the company features an in-house R&D center as well as production facilities. The cornerstone of Micropross activity is the design of solutions for engineers looking for tools to qualify, or certify their products and prototypes against a given specification. Micropross technology covers the whole spectrum of the smartcard industry: they supply protocol analyzers, terminal simulators, smartcard simulators, for both contact and contactless technologies. Depending on the customer requirements, the company supplies turnkey solutions, including hardware and automated test cases (for both analog and digital test plans).

www.micropross.com

MIKRON



MIKRON was founded in 1964. With main activities in semiconductor manufacturing (Power Management Products and RFID) MIKRON is an important player within the financial

strong industrial group of JSFC SISTEMA. MIKRON has about 1600 employees and is with a capacity of 50 Mio inlays and labels per month and a chip capacity of about 100 Mio per month the largest RFID manufacturer in Europe. Major activities are within the RFID and Industrial/Consumer market. Joint Venture and cooperation for technology will secure strong standing within the fast growing future market. 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

WORLD e-ID CONGRESS



Identity Services for Government, Mobility & Enterprise

Conference - Sept. 23-25, 2014 & Exhibition - Sept. 22-24, 2014 - Marseille, France

Now in its 10th edition, World e-ID Congress is set to gather 400 e-ID programs managers, government officials and technology experts around world's most inspiring large scale rollouts and next generation technologies.

2.5-day CONFERENCE (Sept. 23-25): 80 speakers, keynotes and panellists to review World's next gen e-ID services, trends and innovations along 10+ focus tracks.

Hot 2014 themes:

PROGRAMS EXPERIENCE, RESULTS & PERSPECTIVES

e-ID Gov Programs

Experience-sharing from most innovative large scale e-ID infrastructures worldwide

EU Funded Projects

Focus on Europe: e-Health, eDL, cross border interoperability, eIDAS, e-signature, e-Passport...

Emerging Countries

In partnership with the World Bank, emerging countries testimonials and use cases

Cybersecurity

Prestigious keynotes and insightful presentations from Gov. reps, cybersecurity centers, Industry...

KEY TRENDS & NEXT GEN SERVICES

Mobile ID

Signature, access, authentication... an in-depth coverage of latest roll-outs, applications, issues...

e-ID for Business

e-ID to enable new business, cut costs, improve usability & security: case studies and innovations

Biometrics

Is biometrics mature for the mass market? Stakes for the e-ID ecosystem and services delivery

Air Travel Service

How airlines, airports and service providers innovate on cross border, access control...

50-booth EXHIBITION (Sept. 22-24): the SMART SOLUTIONS SHOW will feature e-ID solutions leaders and add knowledge sharing, networking opportunities with the 1700 mobile/contactless, M2M and digital security professionals attending World Smart Week.

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 available 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

SMARTAC N.V.



SMARTAC 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. SMARTAC 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



T-Systems is Deutsche Telekom's corporate customer arm. Using a global infrastructure of data centers and networks, T-Systems operates information and communication technology (ICT) systems for multinational corporations and public sector institutions.

With offices in over 20 countries and global delivery capabilities, T-Systems serves companies in all industries. Approximately 47,600 employees worldwide use their industry expertise and ICT know-how to provide top-quality service. T-Systems generated revenue of around EUR 9.2 billion in the 2011 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

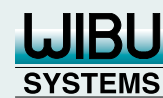
WATCHDATA TECHNOLOGIES



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' product portfolio offers digital asset, intellectual property and integrity protection against piracy, reverse-engineering and code tampering. The broad range of Wibu-Systems solutions covers application fields from computers to mobile, from embedded automation to cloud computing, from SaaS to virtualized models. Wibu-Systems has enabled new business models; software-powered businesses, whether in the consumer, corporate or embedded system realm, can monetize their investments through license orchestration schemes.

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, health-care, 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

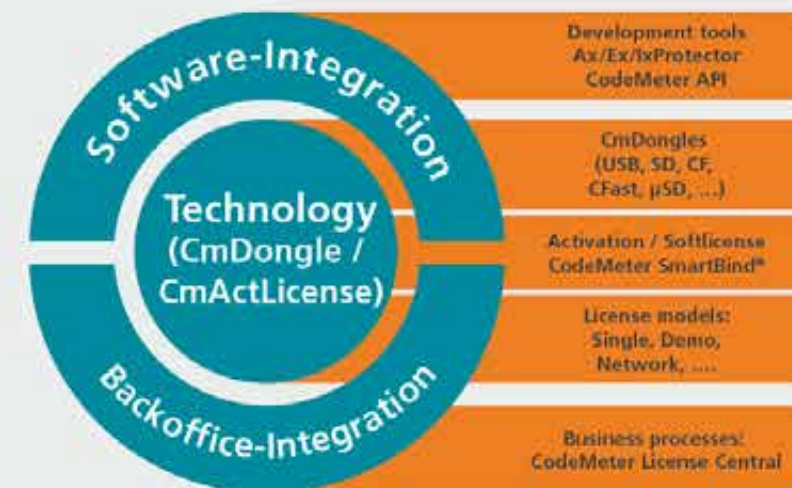
CodeMeter: Security against product piracy and manipulation



- Industry 4.0
- Cyber Physical Systems
- Software



Wibu-Systems is the global specialist in protection, licensing and security



CodeMeter® encrypts and signs software. It inhibits software piracy for desktop, server and cloud applications and prevents reverse engineering, counterfeiting and tampering of embedded software in machines and devices. The applications range from CAD and ERP, to ATMs, medical devices, industrial automation, PLCs, as well as energy, logistics, and facility management. In addition, CodeMeter enables new business models by facilitating software configuration of features in production and after sales.

CodeMeter includes protection tools, as well as cloud and intranet based systems for key, certificate and license creation and deployment. At the heart of the technology are secure elements, with built-in smart card chips. They are available for many interfaces, like USB, µSD, SD and CFast, support extended industrial requirements, including highly reliable flash mass storage, retrofit in existing systems in the brownfield and seamlessly upgrade them. They act like repositories for licenses, keys, certificates, and offer encryption and authentication using AES, ECC and RSA algorithms.



**SECURITY
LICENSING**
PERFECTION IN PROTECTION

www.wibu.com | sales@wibu.com | +49 721 931720

Trust, Performance and Convenience

Infineon serves the key success factors of Mobile Security

Learn more about Infineon's certified Secure Elements for reliable Mobile Security solutions at www.infineon.com/NFC