The VAULT

FEATURED ARTICLE

BORDER CONTROL ALONG INTERNATIONAL STANDARDS
Status, Trends and Outlook

ALSO IN THIS ISSUE

Infineon Technologies
The case for the eData page

cryptovision
Why eID cards and Digital Signatures need each other

Mühlbauer
Providing the citizens of El Salvador with eID cards

Melzer Maschinenbau
When innovation meets return on investment for Identity Solution Manufacturing

PAV Card
A family firm supplying worldwide solutions for Govt. ID, health & finance

Wibu-Systems
Three decades ahead of the curve

Meet us at
Riviera
J045

EAL5+ certified MTCOS® 2.5 on IFX, NXP, ST

MTCOS® – ID CHIP SOLUTIONS
FOR eGOVERNMENT APPLICATIONS

- High Security Operating System (MTCOS®), e.g. ePassports, eIDs, eHealth cards
- Independent worldwide supplier
- More than 65 eID-document references
- Up to EAL5+ Common Criteria certified on a unique variety of chip platforms

SecurITy

Common Criteria

MaskTech GmbH • Nordostpark 45 • 90411 Nuernberg • Germany • sales@masktech.de • www.masktech.de • +49(0) 911 95 51 49 0

Contents

Health & Donor Services

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

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

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

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

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

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

Contactless, RFID and NFC

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

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

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

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

---

cryptoVision

We create your eID solution

- Standardized, multi-app & bespoke eID documents
- Tools for easy personalisation
- eID application integration
- Document PKI

www.cryptovision.com

Subscribe to our NEWSLETTER now!

Meet us @

11th – 13th June 2019
SDW in London
booth S 120

18th – 20th June 2019
ID4Africa in Johannesburg
booth C 16

Why eID cards and DIGITAL *Signatures* *NEED* each other

By Markus Hoffmeister & Klaus Schmeh, cryptovision GmbH

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

ULTIMATE ID CARD
HIGH SECURITY DEMANDS HIGH TECHNOLOGY

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

☐ Digital signatures: mathematics used in practice

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

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

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

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

eID enables digital signatures

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

Electronic identity cards with a digital signature application are generally expected to make digital signatures more popular. Ben Drisch, eID consultant at cryptovision, explains: "The more people have an electronic identity document that supports digital signatures, the more attractive this technology will be

for both users and service providers." The legal foundation for a widespread digital signature use has long been laid, with countries all over the world having created digital signature acts. As one of the most important legal frameworks of this kind, the European Electronic Signature Regulation (also known as eIDAS) has been put into practice.

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

Digital signatures and future technologies

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

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

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

SILICON TRUST PARTNERS

Partners of the Silicon Trust are a vital element of the program. The partners represent all aspects of the value chain and are international representatives of the ID industry. They all share one common goal – to create awareness, to educate and to promote the need for silicon-based security technologies.

ABNote

ABnote™ is a leading global supplier of secure documents, services and solutions. If you have a credit card or an identity card, or have received a gift or loyalty card, or any other plastic card, chances are that you have used an ABnote product. If you have interacted with a financial institution, or have used your smart phone to make a payment, you have likely taken advantage of an ABnote service.
We are proud of our legacy – over 200 years of manufacturing high quality, tamper-resistant products to governments, financial institutions, retailers and other organizations throughout the world. Today, our products and technology encompass multiple markets, keeping pace with today's rapidly changing requirements for convenient and secure transactions.
www.abnote.com

AdvanIDe

Advanced ID Electronics – is one of the leading silicon distributors, focused on components for RFID transponders, chip cards and RFID readers and terminals. Thanks to its optimized semiconductor supply chain, AdvanIDe can guarantee manufacturers of smart cards, RFID transponders and readers the most efficient access to the latest semiconductors.
www.advanide.com

AGFA

Agfa is commercially active worldwide through wholly owned sales organizations in more than 40 countries. In 2014 the Group achieved a turnover of € 2,6 billion. Agfa develops, produces and sells special films for the card industry. PETix™ is a range of high-performance polyester films, for cards with a lifetime above 10 years and a high chemical, scratch and thermal resistance.
www.agfa.com

ATOS

Atos SE is an international information technology services company with 2014 annual revenue of € 9 billion and 86,000 employees in 66 countries. Serving a global client base, it delivers IT services through Consulting & Systems Integration, Managed Operations, and transactional services through Worldline, the European leader and a global player in the payments services industry. It works with clients across different business sectors: Manufacturing, Retail & Transportation; Public & Health; Financial Services; Telcos, Media & Utilities.
www.atos.net

AUSTRIACARD

AUSTRIACARD AG is a holding company of businesses providing end-to-end solutions and products in the field of Digital Security and Information Management. The Group brings together the century-long heritage in printing services and state-of-the-art digital data solutions (Information Management division) with the well-established production and personalization of smart cards and the offer of cutting-edge digital payment solutions (Digital Security division). The combination of well-established industrial roots with an expanding services portfolio that meets the needs of the increasingly digital and mobile economy is at the very core of the Group's confidence in its future.
www.austriacardag.com

AVATOR

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

BALTECH

BALTECH is specialized in ISO14443/15693/NFC Reader technology. The core competencies are RF-Interface technology and sophisticated high level functionalities supporting the latest card technologies and security mechanisms. All products are 100% developed and manufactured in-house. This is the basis for customization capabilities offered to deliver application tailored, cost optimized products from readers up to terminals with individual functionalities for various applications.
www.baltech.de

CARDPLUS

CardPlus is a consulting firm with a focus on customized, enterprise level, Identity and Security Management Solutions. We offer a full range of Professional services to build, transform, implement and manage our customized enterprise level security and identity solutions. Due to our vast hands-on experience in designing and implementing secure travel and identification systems for governments and large public sector customers, we are uniquely positioned to understand your highly complex security requirements and translate the same into practical, workable solutions.
www.cardplus.de

CHARISMATHICS

charismathics® has been pioneering the global identity management arena since 2005 and is offering security products and services for a variety of industries ranging from corporate to finance, from e-government to health services, from e-education to telecommunications. The company delivers PKI security solutions addressing traditional smart cards, convenient USB keys, handy soft tokens or even cutting edge mobile applications.
www.charismathics.com

COGNITEC

Cognitec develops market-leading face recognition technology and applications for industry customers and government agencies around the world. In various independent evaluation tests, our FaceVACS® software has proven to be the premier technology available on the market. Cognitec's portfolio includes products for facial database search, video screening, and biometric portrait capturing.
www.cognitec-systems.de

CRYPTOVISION

cryptovision is a leading supplier of innovative cryptography & public key infrastructure (PKI) products. The lean and intelligent design of the complete product range makes it possible to integrate the most modern cryptography and PKI application into any IT system. cryptovision PKI products secure the IT infrastructures of diverse sectors, from private enterprise to government agencies. The consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems to the design of complete cross-platform cryptographic architectures.
www.cryptovision.com

DE LA RUE

De La Rue is a leading provider of sophisticated products and services that keep nations, their economies and their populations secure. At the forefront of identity management and security, De La Rue is a trusted partner of governments, central banks and commercial organisations around the globe.
www.delarue.com

DIGITAL IDENTIFICATION SOLUTIONS

Digital Identification Solutions is a global provider of advanced identification solutions, specialized in secure government and corporate applications for ID cards and ePassports/Visa. By applying innovative technologies, they develop unique, scalable credential solutions, which perfectly meet the ever-changing demands of international customers.
www.digital-identification.com

HBPC

Pénzjegynyomda Zrt. (Hungarian Banknote Printing Shareholding Company) is the exclusive producer of 'Forint' banknotes, and is one of the leading security printers in Hungary, specializing in the production of documents and other products for protection against counterfeiting. Currently, HBPC produces passports, visa, ID documents, driving licenses, securities, duty and post stamps, tax stamps and banderols, paper- and plastic-based cards, with or without chip, and is aiming to provide complex system solutions.
www.penzjegynyomda.hu

HID GLOBAL

HID Global Government ID Solutions is dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide. HID Global Government ID Solutions offers government customers an end-to-end source for their most demanding state and national ID projects. With Genuine HID™, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Government ID Solutions offerings include expert consulting services, data capture, credential management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelaminates, LaserCard® optical security media technology, and FARGO® card printers.
www.hidglobal.com