NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2021 | #30

The VAULT

SECURED TRAVELS

FEATURED ARTICLE

Coil on Module Contactless for Polycarbonate Datapages

Infineon Technologies

ALSO IN THIS ISSUE

Wibu-Systems
Digital sovereignty needs security

Mühlbauer ID Services
Luminous safety on Visa Pages

cryptovision & Atos
Atos acquires German cryptography specialist cryptovision

cryptovision
Post-quantum cryptography isn't rocket science – or is it?

Infineon Technologies
World's first TPM 2.0 with open-source software stack

Our eID solutions* are flexible, secure, certified. So you can do things just the way you want. Our Government ID experts and our global network of qualified partners will lead the way. Find out more on **cryptovision.com/eID**

*Java Card™ Applet Suite | Personalization | Middleware | Certificate Management

Contents

Imprint

THE VAULT ISSUE 30
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Rainer Bergmann, Oliver Winzenried, Philip Seebauer, Klaus Schmeh, Katharina Schuldt, Markus Moesenbacher
PHOTOS: INFINEON TECHNOLOGIES, ISTOCKPHOTO, KROWNE COMMUNICATIONS, WIBU-SYSTEMS, MÜHLBAUER, OVD KINEGRAM, PARAGON ID, CRYPTOVISION
EDITION: June 2021.
The publisher and the Silicon Trust team would also like to express their gratitude to Rainer Bergmann for his invaluable help, support and contributions towards the Silicon Trust program in the last few years. We shall miss his enthusiasm and optimism and wish him well for the future. Thank you, Rainer!

SILICON TRUST *completes* FIRST global ONLINE seminar roadshow *featuring Infineon's* SECORA™ Technology SOLUTIONS

By Steve Atkins, Program Director, The Silicon Trust

☐ Following on from a successful online seminar for the EMEA region this April, Silicon Trust continued to present their SECORA™ seminars for APAC and the Latin America regions on the 6th and 12th May respectively.

SECORA™ is Infineon's family of one-stop security solutions with integrated operating system (OS) providing a cost-efficient way to fast and agile implementations. It is based on a solid chip platform, which is highly secured and reliable, as well as easy to install and delivering best price-performance ratio.

There are four SECORA™ security solutions subcategories, which were presented by Hans-Jörg Frey, Thomas Mickalski, Ajay Hanyalu and Markus Moesenbacher, respectively.

SECORA™ Pay – Flexible solution providing a complete portfolio for everything from contact cards to smart payment accessories, combined with the latest EMV-ready applications, to meet regional market requirements.

SECORA™ Connect – System solution for smart wearables to provide contactless secured payment, ticketing or access applications via Near Field Communication (NFC).

SECORA™ ID – Ready-to-go Java Card™ solution optimized for all electronic identification (eID) applications allowing maximized customization for local needs.

SECORA™ Blockchain – Fast, easy-to-use Java Card™ solution supporting best-in-class security for blockchain system implementation.

Also speaking were **Ulrich Dreefs** from **Fidesmo** presenting **"Onboarding Payment and other Services to Smart Devices"** and **Benjamin Drisch** (and **Fermín Teuctzintli Vázquez Pérez** for the Latin America Seminar) from **cryptovision** presenting **"Fast prototyping of multipurpose eID cards on Infineon's SECORA ID X platform"**.

By the end of the seminar roadshow on the 12th May, the seminar had had representatives attend from over 40 separate countries throughout the world, with registrations numbering over 260. A significant number for the first-ever Silicon Trust roadshow. Timings were kept to local time zones, as well as simultaneous translations in Spanish for the Latin America seminar.

Rainer Bergmann, Director Special Projects Smart Card Solutions and Infineon SCS representative for the Silicon Trust said, "Security solutions are complex and diverse. New application markets require their own form factors, which only adds to the complexity. Infineon Technologies appreciates the Silicon Trust's efforts to establish and execute a series of three SECORA™ webinars that addresses both these established and new markets such as Payment, ID, Access, Wearable & Convergence Applications. During these webinars Infineon, Cryptovision and Fidesmo presented their products, services and solutions for all these application markets. Based on the feedback we got, one of our take-aways is that such kinds of solution-oriented webinars really connect with our customers".

"Performing the three webinars at slots which are time-wise friendly to Asia, Latin America and EMEA respectively was another reason we found such a willing and engaged audience. The fact that each webinar was an event on its own (i.e. not an event held during another larger event) and that each webinar lasted just 2 hours (a duration which is perceived to be reasonable and easy to add to the attendees' calendar) were two further reasons to make them successful," he added.

"Last, but not least Krowne – for the first time ever – offered simultaneous translation (English – Spanish,) during the Latin America webinar. A great idea and appreciated by the Latin American audience. All in all, I am sure that these webinars demonstrated once again, that establishing HW-based security solutions is not an activity by an individual single company, but it is all about partnering and cooperation. I hope that Krowne will organize webinars for Silicon Trust members and friends in the near future," he concluded.

Feedback was also positive from the attendees from all regions, with many writing to express their satisfaction of the 2-hour seminar.

This positive feedback from both presenters and attendees has given the Silicon Trust a drive to present more seminars in the future. The next seminar session proposed for the autumn/ winter timeframe will aimed at the needs in African countries. More details will be available this summer. ☒

LUMINOUS SAFETY on VISA *pages*

By Katharina Schuldt, Mühlbauer ID Services GmbH

☐ Whether it's a physical or an electronic document, it's the trustworthiness of the document that counts. Creating a new identification system means thinking about which security attributes need to be integrated and how these attributes are going to be proved – either manually or electronically.

Secure and seamless end-to-end solutions that address both physical and electronic applications, must include secure processes, as well as secure functions. The implemented identification and verification solutions, systems and products should be future-proof, meaning scalable and adaptable to future requirements and challenges.

Providing highly secure documents is an essential part of counteracting worldwide threats of criminal and terrorist activities. The positive identification of persons by means of secure documents – and therefore the confirmation of the document validity – is crucial.

Accordingly, we need both a secure document and appropriate equipment to check it. A passport reflects a person's identity and transforms it into something tangible, official. Being officially registered means being officially authorized to participate in public life, to submit applications or to cross borders. The German travel document specialist and leading global player of the security sector Mühlbauer, developed an innovative ePassport, which provides additional safety by incorporating individual images into the passport. The idea is to integrate different security features into pictures on the visa pages to combine both design and security. The pictures show for example cultural-historical monuments of the respective country, such as Germany's famous Neuschwanstein Castle and feature elements, which are only visible under different UV wave lengths. A security officer, checking the passport for authenticity, would only need to use a UV flashlight to discover dozens of small, shining windows in the castle, hidden under natural light. As this and many other security features do not only appear on one or two pages of the passport, but on nearly every page, differing in nature and appearance, it is quite difficult to counterfeit the ID document.

However, this is not the only intention of the ePassport. The holder should also be able to identify himself with his passport and thus with his country. The embedded images on the visa pages convey pride in one's origins and transform the passport from a neutral object into an emotional part of one's identity.

The heart of each travel passport is the Holderpage. It contains the holder's personal data, such as name, date of birth, nationality, and also the passport number and the biometric image of the holder. This page is the first to be checked at the airport gate or border crossing - therefore the most important

> *The idea is to integrate different security features into pictures on the visa pages to combine both design and security.*

security features are incorporated here. Shifting images or texts, a relief structure on the document's surface, metallized holograms or a transparent window with elements, which can be seen from both sides, are only a few of Mühlbauer's wide range of features to make a document more secure. The key is not to randomly include as many functions as possible, but to select and combine features that meet the specific requirements and form a comprehensive security concept.

One of the most important techniques is the personalization of identity documents. The sophisticated MB ALFRESCO PICTURE technology smartly combines color picture personalization with laser engraving. To achieve the highly secure personalization result, the image of the holder is split into two parts using special image processing algorithms. The converting process transfers all picture information, which describe the details (forensic information), into a greyscale image. This greyscale information containing all contrast information of the picture is engraved into the inner layers of the document by using laser engraving technology. The remaining color parts are converted to a separate color image, which is then printed on the blank document's surface. Due to the special characteristics of the ink, the colors penetrate the card surface, thus thwarting counterfeiting attempts of scratching off the surface. The final result is a high resolution color picture, which shows utmost details. This picture technology has the same long lasting durability characteristics and resolution as a pure laser engraved picture. To further increase the security, the holder's image is secured by an additional protective layer. Attempts to remove the photo are protected, as the greyscale information remains inside the document. The greyscale picture can be additionally verified under Infrared light. Due to the special color properties of the MB ALFRESCO PICTURE, optical variable features (e.g. Holograms) shine through the color picture and thereby protect it against replication by photo copying. The highest level of security is reached by laser engraving the biographical data and a secondary holder's portrait into the document material.

There are several ways to check these security features, depending on the security level to which they are assigned. Features under 'Level 1' can be verified without further tools. 'Level 2' security features can be validated with (handheld) devices. The highest security 'Level 3' features are verified by using forensic testing methods.

It is becoming increasingly important to also be able to check the passport validity without personal contact. Modern ePassports are equipped with Radio-Frequency Identification (RFID) chips and Machine Readable Zones (MRZ). In this way, unforgeable certificates can be read out directly by machines. The biometric photo or the fingerprint - stored on the chip or in the MRZ - makes it possible to assign a document uniquely to the person. The information can also be checked against databases and thus verified. These so-called eGates simplify and accelerate the process and offer contactless, and thus a more secure passing, especially in times of Corona. ☒

Mühlbauer
High Tech International

Security is not a product, but one of the most valuable goods of a nation. The core of a holistic ID program is the constant capability to increase and optimize the integrity of the national identification scheme. Mühlbauer is strongly committed to providing reliable and secure government solutions for your citizens, thus creating trust and absolute confidence whilst meeting all your individual requirements.

Mühlbauer – Your Reliable Partner for Your National ID Program

www.muehlbauer.de

Coil on MODULE CL for POLYCARBONATE *DATAPAGES*

By Philip Seebauer, Infineon Technologies AG

As globalization becomes more prevalent, so too are the number of passport holders and annual border crossings. In combination with a rising number of geopolitical conflicts, which result in an increase of migration, the annual number of border crossings will most likely continue to grow in the future. Under the current circumstances, the motivation of travel document forgery increases as political conflicts grow. At the same time, while the current pandemic has curtailed cross border travel to a certain extent, there are signs that once we are post-pandemic, travel will slowly and steadily return to acceptable numbers and so too will the requirement for high security travel documents in volume.

Passport forgery is a real consequence of increasing globalization

The top target for fraudsters is the datapage, which contains the holder's personal data. Due to their security-critical character, official identification documents for travel must be developed according to the highest security standards, in order to enable a reliable protection against aging, manipulation and fraud. Appropriate security is expected over the entire lifetime of the travel document, which is typically up to ten years.

With such a scenario, it is increasingly important to improve protection against passport forgery. A developing trend in this field are polycarbonate datapages with an embedded security controller. The combination of security IC and polycarbonate datapage has resulted in new possibilities to make passports even more forgery-resistant.

The polycarbonate eDatapage

Over the last two decades, the exceptional performance of polycarbonate (PC) as a substrate for identification documents has made it the material of choice for datapages, outperforming laminated paper datapages in areas such as security and durability. Recent improvements in the sophistication of the polymer material itself, and in the laser systems that engrave it, have caused passport issuers to take notice. Over 40 countries have chosen it for their national identity or residence permit programs and close to 30 national passport programs are currently using it* (Thales Group – More than two decades of innovation in polycarbonate: https://www.thalesgroup.com/sites/default/files/gemalto/gov-infographic-poycarbonate.pdf)

For example;

- 1989 – The first polycarbonate document issued with the Finnish driving license
- 1995 – Switzerland released the first polycarbonate ID card widely used as a travel document
- 1997 – Finland issued the first polycarbonate datapage in their passports
- 2005 – Sweden issued the first polycarbonate eDatapage in their passport
- 2016 – Cameroon introduces a colour photo with laser personalization in a polycarbonate document
- 2017 – Germany introduces a polycarbonate compound for their passport eDatapage, as well as a window integrated into the polycarbonate card and picture of the passport holder on the title page.

> *It is important that the datapage is designed and constructed to defend against a large variety of threats, as an attacker usually only needs to identify and exploit one weakness in order to access and manipulate the data contained therein.*

Since the first introduction into the passport world, a growing number of countries have adopted a polycarbonate datapage. Polycarbonate, due to its unique properties, has won the trust of governments as the material of choice for durability and tamper resistance.

The material attributes of polycarbonate with its multilayer structure, which is indivisibly fused after lamination, is forming the so-called 'polycarbonate Monoblock', enabling significantly more security features at multiple levels.

A so-called 'polycarbonate Monoblock' consists of 'top to toe' polycarbonate, which connects to one block during the lamination without any chance of delamination. With printing, security features and personalization on different layers inside the body and a tactical surface are possible. After the lamination process, the individual layers are closely combined, providing improved robustness and an increased tamper resistance.

In comparison to conventional solutions, where the chip is located in the cover, polycarbonate datapages with embedded security controllers – the so-called eDatapages – increase protection against forgery significantly.

During the production process, it is crucial to adhere to the element of a 100% 'polycarbonate Monoblock' even when introducing additional items, such as security features or antennas: Having a wired antenna on polycarbonate continues to support the 100% Monoblock concept. It keeps the existing construction, as only the wire is inserted onto one of the existing polycarbonate layers and prevents a change of the lamination process, as no new material is brought into the card itself.

Infineon Technologies has developed a special package solution for highly robust, flexible and long-term reliable government ID and passport documents that will also allow for a thinner eDatapage – Coil on Module. Coil-on-Module also allows the option for the adding of additional security layers that can help guard against datapage manipulation.

eDatapage guards against datapage manipulation

It is important that the datapage is designed and constructed to defend against a large variety of threats, as an attacker usually only needs to identify and exploit one weakness in order to access and manipulate the data contained therein.

The security features of the datapage efficiently protect the document against manipulation. Usual attempts to mechanically destroy the chip itself are easily recognized as mechanical damages, e.g., scratches, will remain on the polycarbonate material as evidence of physical manipulation.

Therefore, the implementation of personal data on only one page makes the manipulation of the documents much harder.

The mechanical abrasion of the page – typically from the back – has been used by fraudsters for many years to reveal and alter personalization data. In this case, an effective defense depends upon the layers of security features and their design within the datapage, in conjunction with the antenna, which is necessary for every electronic passport. eDatapages result in an effective, easy, safe and convenient solution against counterfeiting.

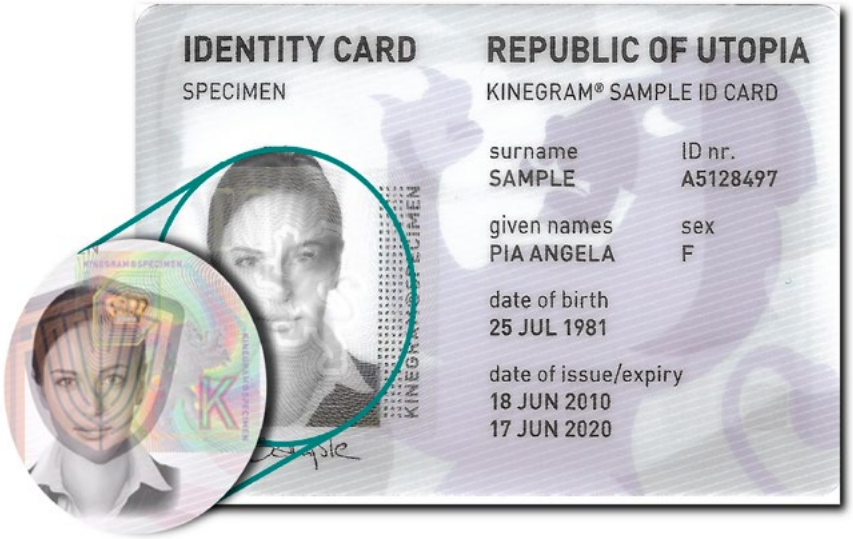


Figure 1 - Kinegrams®, holographic features placed over the photograph reduced the possibility of manipulation through 'Back Side Milling'

The antenna, for example, can be used as a prevention against such mechanical counterfeiting and manipulation techniques, which is known as 'Back Side Milling'.

Polycarbonate can be susceptible to softening by certain organic chemicals, and a combination of mechanical and chemical methods can be utilized by criminals to access and alter data, more or less invisibly. However, even if it were possible to split the datapage, the result would be two separate pieces, each encapsulating and protecting the personalization within the fused PC blocks beneath a network of security features.

Advanced, multi-technology defenses include traditional print and personalization features, as well as embossing, applied diffractive devices and transparent windows. Special antenna technologies with embossing or a Kinegram® or holographic feature, also make it even more difficult to cover up such manipulations. Furthermore, the antenna can be used as an additional watermark, which only appears when viewed by transmitted light, similar to banknotes.

Current eDatapages can be thick – but not for much longer

Looking at current module technologies: Because of its module design, standard contactless (CL) packages with over molded leadframe, which are currently applied for ePassports, require a multiple layer construction of compensation and crack prevention layers. This layer structure impairs the mechanical robustness of the passport, as only relatively thick datapages are currently possible.

Furthermore, thickness for an inlay with standard module technology, with over molded leadframe and copper wire, is currently 330 µm, which results in datapages within an average thickness between 750 µm and 850 µm.

"Infineon Technologies has developed a package solution for highly robust, flexible and long-term reliable government ID and passport documents that will also allow for a thinner eDatapage – Coil on Module. Coil-on-Module also allows the option for the adding of additional security layers that can help guard against datapage manipulation."

This leads to rigid and inflexible datapages, which do not meet the flexibility and haptics of traditional passports without polycarbonate datapages. Additionally, due to the high costs for polycarbonates, a thicker datapage is additionally more expensive than conventional solutions.

While currently the standard thickness for an inlay with conventional module (such as MCS8) is typically 330µm, Infineon now has a package solution with inductive coupling technology for contactless inlays below 200µm, giving the end document manufacturer much greater flexibility. This may indeed bring a cost variable into the overall production cost

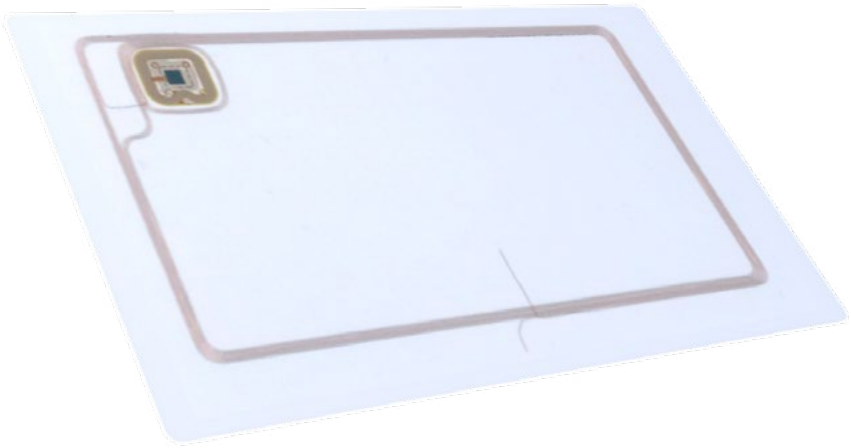


Figure 2 –Inlay Laminated Contactless Module from Infineon

equation as the reduction in polycarbonate material may offset the cost of additional security layers.

This is an attractive argument for passport manufacturers as they look to reduce the thickness of the datapage that carries the chip. The current goal is the reduction of the eDatapage using Coil-on-Module to 600µm and less.

Some manufacturers rely on the bare die flip chip solution, where the security controllers are placed directly without package on a printed or etched antenna. This technology is currently used in transport ticketing solutions. Direct flip chip enables thinner CL inlays which results in a thinner eDatapage but also brings some downsides.

One example are aluminum antennas which are etched onto a PET (polyethylene terephthalate) layer and then placed between the polycarbonate layers with special adhesives. The adhesive residues that are required for gluing can lead to delamination. Both technologies also require huge antenna areas. These antenna areas can cause ghosting artifacts (the shape of the antenna is visible due to roughness and height differences) on the finished product.

Coil on Module CL overcomes all these problems. The inlays have a thickness of below 200µm, giving the end document manufacturer much greater flexibility in terms of thickness and the potential of adding additional layers with all the benefits of standard copper wire solutions – although one should not underestimate the benefits associated with a thin, flexible eDatapage in terms of document usage and convenience.

Coil on Module CL is an innovative package technology that is only 125µm thin, i.e., 50 % thinner than standard packages, and does not require conventional crack prevention. This enables innovative antenna techniques, thinner inlays with less visibility of the module, a polycarbonate monoblock, and delivers outstanding mechanical performance.

"While currently the standard thickness for an inlay with conventional module (such as MCS8) is typically 330µm, Infineon now has a package solution with inductive coupling technology for contactless inlays below 190µm, giving the end document manufacturer much greater flexibility."

Coil-on-Module CL (contactless)

Coil on Module CL (contactless) is designed for highly robust, flexible and very thin polycarbonate eDatapages. The Coil on Module CL technology is based on inductive coupling, which improves the possibilities due to the superior antenna connection technology.

Unlike conventional package technologies, Coil on Module CL uses electromagnetic waves for the connection between module and antenna. A small antenna on the chip module connects to a coupling area on a standard-sized antenna in the passport, using

Figure 3 – Highlighting the Visible Coil on Module CL

an electromagnetic field within the passport. Electromagnetic coupling substitutes mechanical coupling. This lack of mechanical galvanic connection with no soldered or welded connection, massively minimizes the chance of breakage between module and antenna – a huge advantage for a passport with a ten-year lifecycle.

Due to the lack of direct connection, the Coil on Module CL module can also be used as an additional optical security feature (highlighted in Figure 3) and may, in fact, reduce field returns as there is no physical connection between module and antenna.

Inductive coupling technology brings advanced ruggedness and flexibility

The benefits demonstrated by inductive coupling technology, will go a long way to delivering an advanced ruggedness of the datapage with enhanced tamper resistance, as well as a more flexible datapage. With these functionalities in place, the ten-year lifetime requirement of the passport becomes even more reliable.

The Coil-on-Module is a proven technology that enables CL communication in combination with extremely robust packaging for hundreds of millions of payment and government applications in the market. Coil on Module CL is the further development of this technology and is used in polycarbonate datapages, as well as ID1 applications.

Conclusion

The move from traditional passport datapages to passports with eDatapages has meant the integration of one or more smartcard technologies into the production process.

With more applications being added to the functionality of a passport (electronic travel visas – or even time stamps – for example) there is a greater urgency for industry innovation in addressing the physical durability issues that are required to future-proof the credential of tomorrow. Requirements for tamper resistance, durability and flexibility in eDatapage design will increase, as greater customization of the passport takes place alongside increased usage of the passport document.

The benefits demonstrated by inductive coupling technology, as well as Infineon's drive towards much leaner and thinner chip modules, will go a long way to delivering an advanced ruggedness of the eDatapage with enhanced tamper resistance, as well as a more flexible eDatapage.

Many ePassports today deliver a ten-year life time guarantee with a rugged and durable eDatapage. However, using Coil-on-Module CL, the datapage becomes thinner and more flexible and it is this very flexibility that allows a variety of enhancements to be made in terms of document security; be it the addition of security layers or using its very flexibility as a tamper-resistance asset in itself. ☒

ATOS acquires GERMAN *CRYPTOGRAPHY* specialist *cryptovision*

The Silicon Trust

☐ Atos has announced that it has signed an agreement to acquire cryptovision GmbH, a leader in state-of-the-art cryptographic products and solutions for securing digital identities. This acquisition will strengthen Atos' cybersecurity product lines and boost the company's business in the public sector and defense market in Europe.

Founded in 1999 and headquartered in Gelsenkirchen, Germany, cryptovision designs, develops and implements cryptography software, security solutions and hardware products. Its unique solutions are made in Germany, certified by the Federal Office for Information Security (BSI) and accredited by the NATO. The company has a proven track-record of successfully addressing organizations' digital security challenges, in particular those in the public and defense sectors, as well as other sectors with highly demanding regulations and security standards.

The transaction is expected to close by end of Q3 2021 and is subject to the approval of the local governance and regulatory bodies of both parties. ☒

"We are delighted to welcome cryptovision to the Atos family and to work together to develop even more effective security solutions that meet growing cybersecurity and privacy needs. cryptovision products complete the existing Atos cybersecurity products portfolio, so we will be able to address new projects and customers, both in the German market and internationally. This strategic move further expands Atos' strategy to strengthen its cybersecurity presence, capabilities and portfolio worldwide."

Pierre Barnabé, Senior Executive Vice President, Global Head of Big Data & Security at Atos.

"The combination of the two companies will enable numerous synergies in their go-to-market approach. Atos will benefit from cryptovision's strong network of resellers and global technology partnerships in the e-ID markets. cryptovision will benefit from Atos' trusted relationship with European government customers and the Group's ability to deliver end-to-end integrated solutions on a national and international scale. With the now agreed affiliation with Atos, cryptovision benefits in many ways – in particular through the global presence and comprehensive cyber security expertise of an international group. At the same time, cryptovision will be able to expand its technological depth of value creation for its customers."

Markus Hoffmeister, Founder and CEO of cryptovision.

Revolutionary Inline Production Equipment for MRTD Products

Punch + Test

- Highest automation level for maximum accuracy, security and yield rates
- Shortest lamination times
- Minimum demand of operators, floor space and energy
- Inline efficiency and flexibility

Lamination

Multiple Unwind

Collation

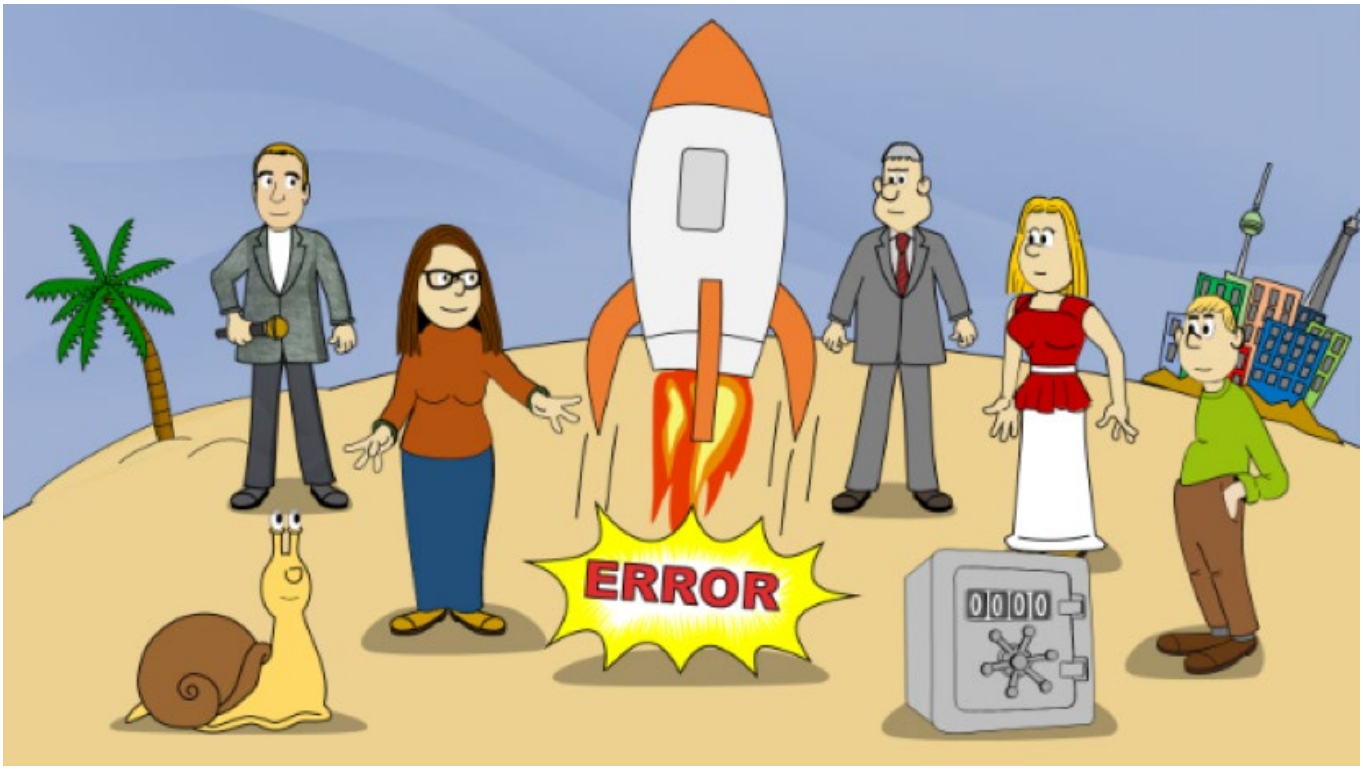
INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

more ▷ **www.melzergmbh.com**

Post-*Quantum* CRYPTOGRAPHY isn't *Rocket* Science – *or* IS it?

By Klaus Schmeh, cryptovision GmbH



Post-Quantum Cryptography needs to play a major role in the eID technology in the years to come – otherwise Quantum Computers might render eID documents useless one day. However, Post-Quantum Cryptography is hard to understand for somebody who doesn't have a mathematics degree. This article explains the three main families of Post-Quantum Crypto Systems – lattice-based crypto, code-based encryption, and hash-based signatures – with cartoons in an easy-to-understand way. Mathematical exactness is, of course, out of scope.

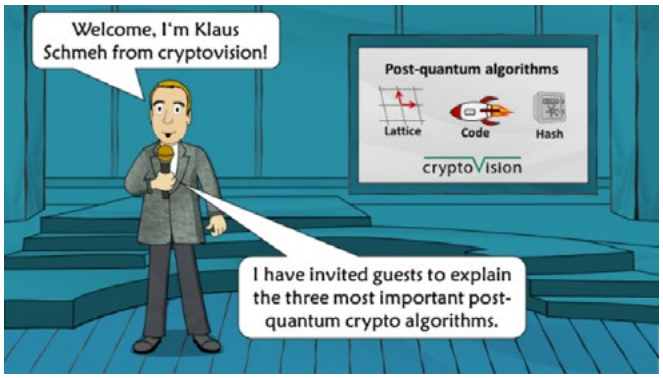
☐ Post-Quantum Cryptography

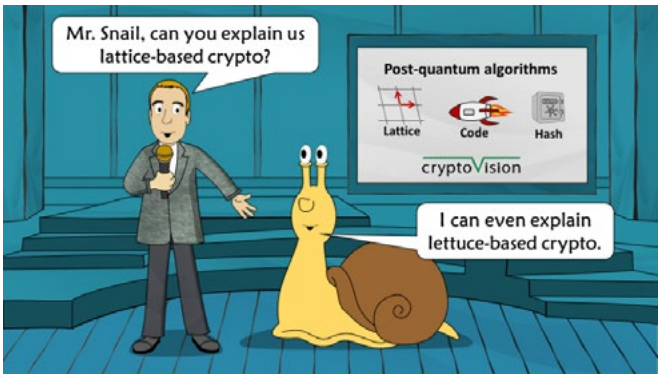
Quantum Computers are a major threat for today's encryption technology, as they can easily break asymmetric algorithms such as RSA and Diffie-Hellman. Among other things, virtually all eID systems in the world will become almost useless as soon as powerful Quantum Computers become available.

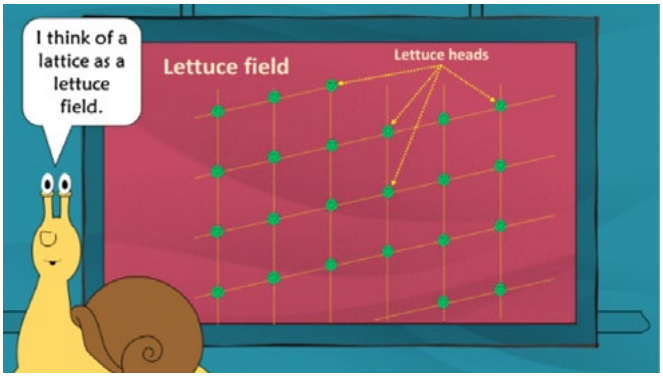
So far, useful Quantum Computers are more a matter of science fiction. The systems that exist today are capable of determining that 21 is the product of 7 and 3, but they are still miles away from breaking a 1,024 bit RSA key. However, this may change as the technology advances. For this reason, quantum-proof crypto systems need to be researched now and implemented in the near future. Systems of this kind, commonly referred to as Post-Quantum Cryptography, already exist but are rarely used to date. Standardisation is still pending. As post-quantum methods are based on sophisticated mathematics, they are not easy to understand. In the following, three of the most important Post-Quantum algorithms are presented in a cartoon story: lattice-based, code-based, and hash-based methods.

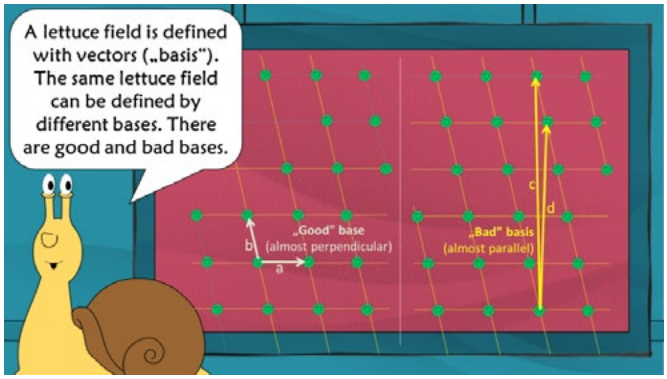
Lattice-based methods

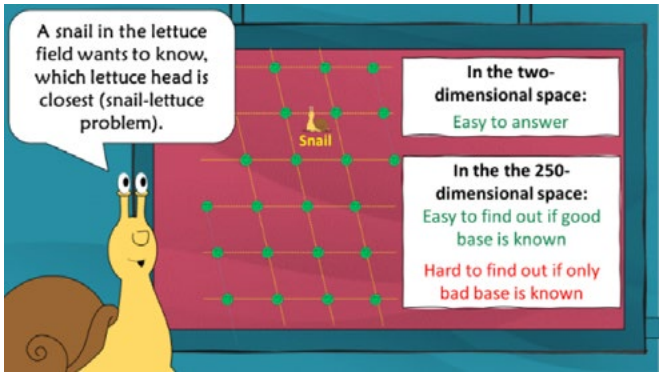
A lattice can be thought of as a lettuce field on which lettuce heads are arranged at equal distances. A lattice can be defined with a good basis (vectors almost perpendicular to each other) or with a bad basis (vectors almost parallel to each other). For encryption, a snail is placed in the lettuce field. The vector between the snail and the closest lettuce head encodes the message. In two dimensions, it is easy to determine the closest lettuce head and thereby decode the message. In 250-dimensional space, however, this is only possible with a good basis. But only the receiver has such a base (as private key), while the sender has to work with a bad base (public key).

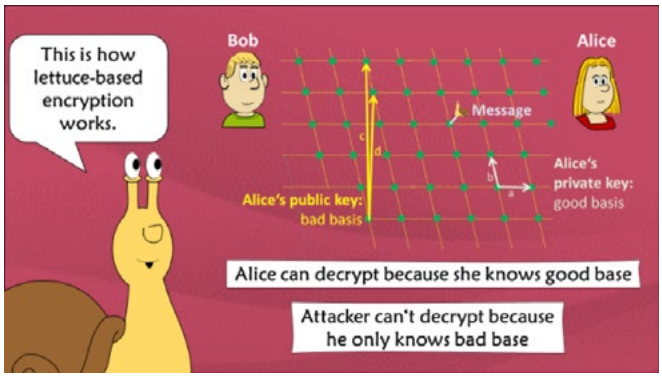






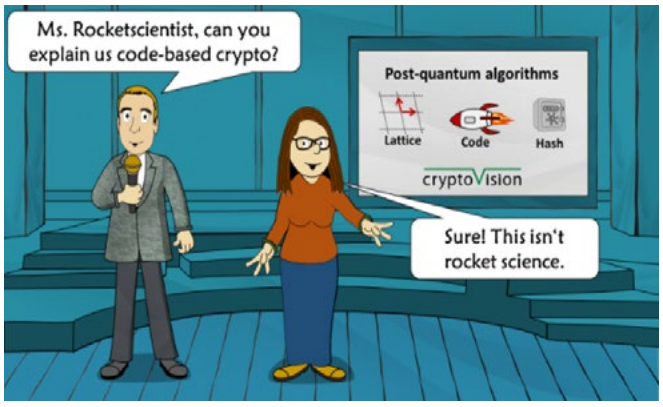


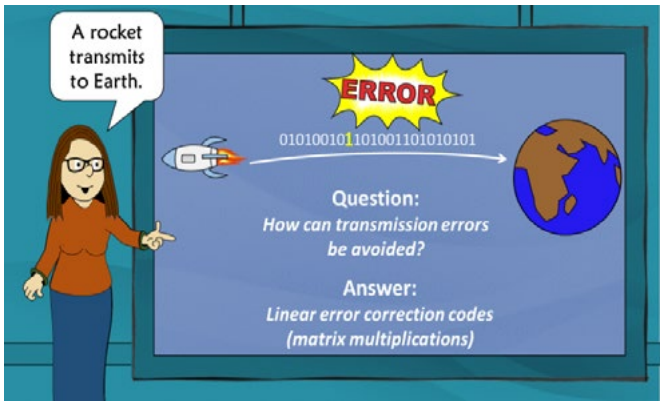




Code-based methods

When a rocket transmits to Earth, transmission errors can occur. Fortunately, there are powerful checksum procedures (referred to as "error-correcting codes") that correct incorrect bits. If such codes are applied to several thousand bits at once, 100 errors or more can be corrected – but the correction process becomes extremely costly. This principle can be used for encryption: The sender of a message puts it into a form where an error-correcting code can be applied. Then he inserts errors. Recovering the original message from the erroneous one is now very costly – unless one has secret additional information (this refers to a matrix that is used in this context). However, only the recipient has this secret additional information (private key).





Integrity Guard – the smartest digital security technology in the industry

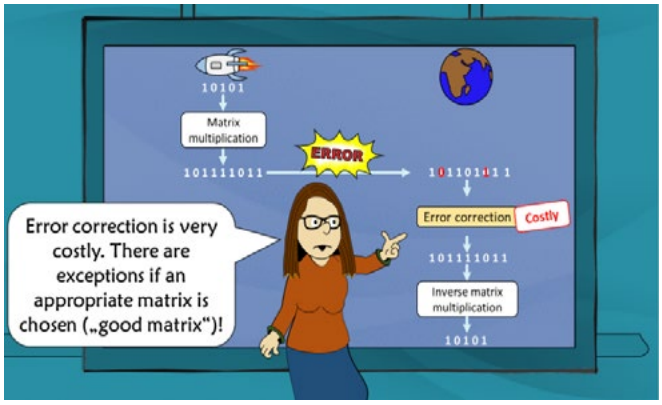
You need security? Relax with Integrity Guard!

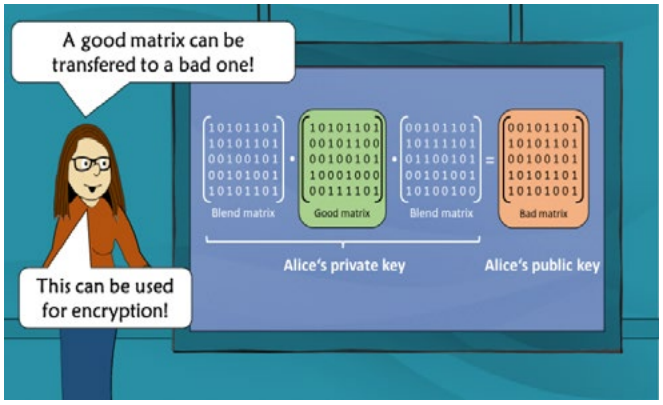
With more than 1.5 billion chips sold, Integrity Guard is setting the technological standard for chip-based security. It bundles several highly sophisticated digital security mechanisms that combine to cover a broad spectrum of potential attacks. Integrity Guard has been developed for applications with high data security requirements for a particularly long life cycle, such government-issued electronic ID documents (passports, national ID and health care cards).

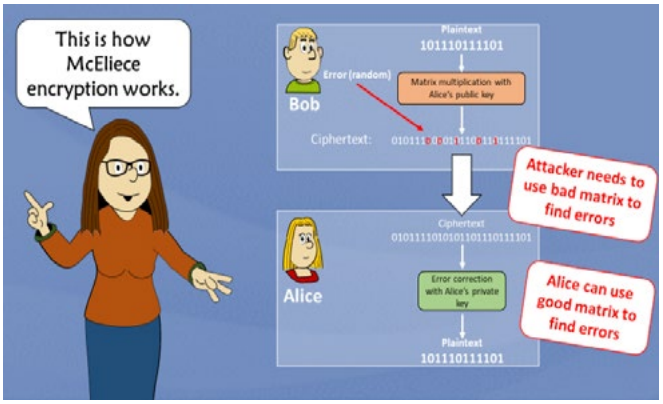
Security chips with Integrity Guard feature:

- Robust security for demanding needs
- Even in the CPU core, data is always encrypted
- Harmless events don't cause false alarms
- Chip architecture reduces need for costly updates
- Automated security features for faster time to market

www.infineon.com/integrityguard

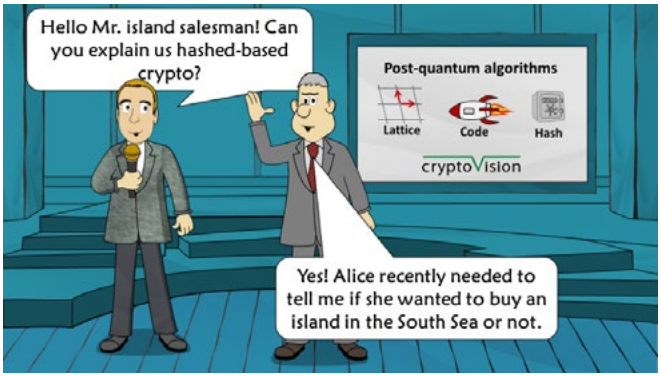


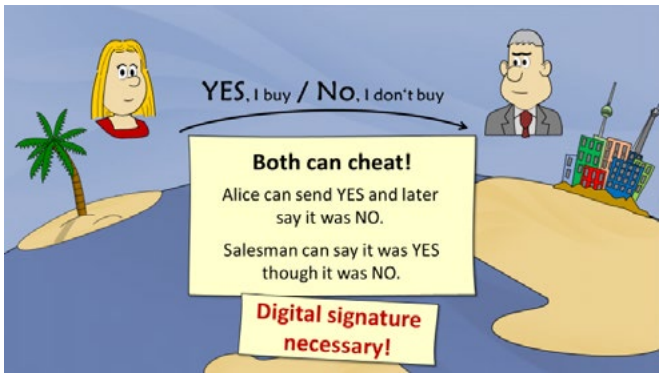


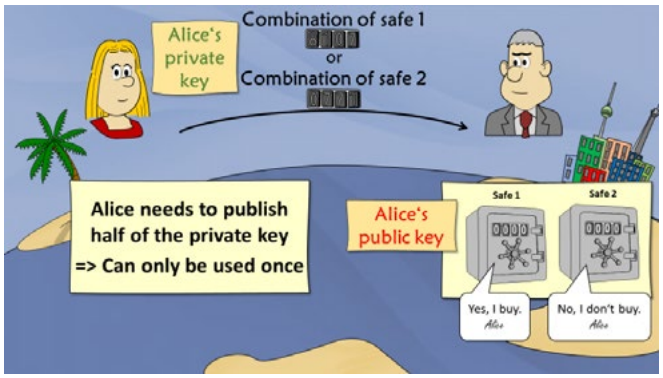


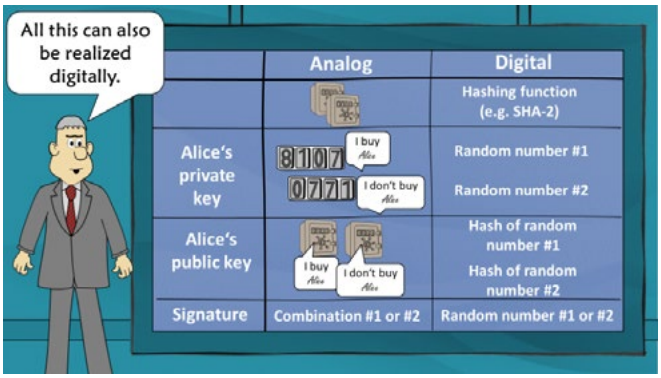
Hash-based methods

There is only one piece of information that Alice wants to convey from a South Sea island to the island seller back home: "yes, I'll buy the island" or "no, I won't". To prevent either from cheating, Alice provides the salesman with two combination-lock safes before she leaves. One contains the yes message, the other the no message – each with her signature. When Alice has made up her mind, she sends back either the yes combination or the no combination – but not both. The salesman now has access to Alice's yes or no message in black and white, including her signature. Such a process can also be implemented digitally. A hash function and hashed messages then take the place of safes and combinations.









Cryptovision's post-quantum activities

Cryptovision, a Germany-based company with two decades of experience in the eID business, has always attached great importance to providing their customers the best available crypto algorithms. To achieve crypto agility, cryptovision solutions allow for switching from one crypto system to another by mouse click. Currently, the cryptovision team is preparing to equip their products with post-quantum crypto algorithms. The goal is to implement post-quantum standards as soon as they are established.

Cryptovision is aware that Post-Quantum Cryptography will only succeed if developers, consultants, and other IT people understand this mathematically sophisticated technology. For this reason, cryptovision engages in activities that aim to explain post-quantum methods to a non-mathematical audience. Among other things, a German whitepaper titled "Post-Quanten-Kryptografie" (available on the company's website) has been created.

"Post-Quantum Cryptography is hard to understand for somebody who doesn't have a mathematics degree. However, there are ways to explain it in a vivid and non-mathematical fashion."

Klaus Schmeh, cryptovision

In addition, cryptovision employees publish articles (such as this one) and give presentations that explain Post-Quantum Cryptography in an easy-to-understand way, often involving cartoons and real-world analogies. Post-Quantum Cryptography is a crucial future technology. Cryptovision is dedicated to put it into practice. ☒

DIGITAL sovereignty needs SECURITY

By Oliver Winzenried, CEO and co-founder, Wibu-Systems AG

Tough, reliable, and maybe a little bigger and louder than it needs to be: The Ford F-150 is not just America's favorite truck, but seemingly emblematic for what the United States stands for. But in February 2021, production of Ford's flagship truck was hit by a problem that no car enthusiasts and only very few industry executives would have ever dreamed of only a decade ago: The global shortage of microprocessors forced a drastic reduction in production numbers. Production lines stopped, shifts were cancelled, and the car maker had to realize the same hard truth that many of its competitors also had to accept this past winter: The digital age knows no borders and no country, let alone a single company can be an island, an entity unto itself, set apart from the ups and downs of today's connected world economy.

With every incident of this nature, the calls grow for digital sovereignty. In 2019, the European parliament had already defined digital sovereignty as "Europe's ability to act independently in the digital world", a question of strategic autonomy. As the global microprocessor shortage shows, this may be a worthwhile aspiration, but it still remains a far-off ambition. At the same time, increasingly high-profile ransomware attacks, now affecting even critical infrastructure of national importance, such as the May 2021 Colonial Pipeline attack, show that digital sovereignty cannot ever be realized under any isolationist terms, as not just markets and supply lines, but threats and attack vectors are also distinctly global. The challenge is clear: There can be no digital sovereignty without security, but that security cannot be understood only in terms of walls built and vulnerabilities patched. Instead, it has to be an evolving, open, and multi-disciplinary effort. It requires the will and the ability to not rely on other people, other countries, or other industries to do the work for you, but to keep pace with developments globally, in order to be sovereign and secure locally.

Wibu-Systems, the pioneering proponent of all things IT protection, licensing and security, has long understood this ambidextrous quality of digital sovereignty and security: The need to build up local, regional, national or supra-national resources, expertise and capable to be able to hold one's own ground and enforce one's own standards, and the simultaneous need to reach out to other actors, thinkers, researchers, and even competitors around the world to spark a mutually

beneficial conversation for greater IT security. It can be a hard sell, as security in and unto itself is not a product that you can collaborate on and then take to market. Instead, it is a process: An evolving technological answer to evolving technological threats. It is never finished, but requires constant care and close attention (and considerable investments). Poorly executed, it can be a nuisance for users and vendors alike. Done right, it can be a quiet, almost unnoticed asset for the product itself, be it a user-friendly licensing solution for an application or a dongle with market-leading encryption and security technology on board that can execute amazing IT protection feats in the background. Done even better, IT security can play a big part in enabling new business models, with licensing becoming a vital building block for subscription, pay-per-use, or add-on service models, as exemplified by Wibu-Systems' CodeMeter technology. But whatever the case may be: For IT security to be a genuine part of digital sovereignty, it has to counterintuitively remain open and collaborative, a community effort.

Karlsruhe, the historic baroque city in Germany's upper Rhine valley, has mastered this art of local excellence combined with cosmopolitanism since its foundation. Built as a model community around the residence of the Margrave of Baden, it merged innovative ideas of urban planning with an early commitment to academic and technical excellence. The original Polytechnicum of 1825 has since evolved into the Karlsruhe Institute of Technology, and a unique research and enterprise ecosystem has developed around it, including Wibu-Systems, which was founded in the city three decades ago. To mark this milestone, the company recently brought an architectural vision to life that is a fitting expression of its commitment to local roots, combined with openness and shared progress: On a new campus near the former freight yards of the Rhine valley's arterial rail route, Wibu-Systems not only gave itself new head offices and production facilities, but also created the House of IT Security; a dedicated home, incubator and shared space for researchers, established enterprises, and aspiring young startups operating in the field of IT security. With almost 60,000 square feet of space for fixed-lease tenants or project teams, the House of IT Security is set to become a new focal point for Karlsruhe's vibrant IT

House of IT Security

community. More than 4,000 IT companies are already based in the vicinity, far surpassing even Silicon Valley in terms of the number of enterprises per square mile. The greater region is also home to other global leaders of industry, like SAP, itself a partner of Wibu-Systems. It is regional super-clusters like these that will become essential for digital sovereignty to become a reality.

The new head offices of Wibu-Systems themselves are also true to the idea of digital sovereignty, with local excellence plus cosmopolitan openness. Over its three decades in the industry, the company's technology has evolved from its origins in licensing hardware, to cover a vast range of hardware, software and cloud solutions for software protection, licensing and security. Its progress has been powered by constant research and development, often in partnerships with academic institutions like the KIT, including fundamental research for example its Blurry Box encryption technology. With representatives and subsidiaries around the world, Wibu-Systems has been serving its global clients with solutions that match their changing needs and the evolving nature of the digital realm and the threats within it. Its newest addition to the CodeMeter technology, CmCloud and CmCloudContainers, brings the popular protection and licensing capabilities of its hardware CmDongles and software license containers to the cloud, with all of its unique abilities and security concerns.

Despite the airy and intangible vocabulary of data living in the clouds, the new digital age has a very solid and tangible side to it, one that is of particular salience for digital sovereignty: Connected industry and smart factories. As the digital revolution has disrupted old supply chains and is beginning to replace the monolithical manufacturing behemoths of old with new forms of manufacturing-as-a-service and new, agile producers vying for orders in the industrial IoT, industrial machines are no longer disconnected hulks of metal, but instead smart, connected, and ready to adjust their processes and output to each changing order, often sent to them from a product designer on the other side of the planet. Now that this vision of Industry 4.0 is becoming reality, connectivity again also means susceptibility to new threats and new attack vectors. Wibu-Systems has long played a leading role in powering the rise of the industrial IoT and connected industry, and has been supplying the world with both industry-grade versions of its protection hardware CmDongles, with formats ranging from classic USB dongles to

integrated ASICs, as well as a dedicated version of its CodeMeter solution for the embedded systems that make up the backbone of the industrial and non-industrial IoT. Wibu-Systems is also contributing substantially to new standards and concepts for a secure connected world, including pioneering work on new ideas of trustworthiness and chains of trust in digital enterprises. Many of these projects enjoy financial support from EU or German federal sponsors and are pursued with high-profile research institutions like the Fraunhofer Societ: A clear sign that politics, academia and industry have grasped the importance of home-grown digital and security expertise for digital sovereignty on a national, EU-wide and even global level.

Despite the global reach of its business and its outspoken commitment to interdisciplinary and international cooperation, Wibu-Systems also follows the ideas of digital sovereignty in its own business operations, as exemplified by the production and lab facilities on its new campus. Designed to be not only exceptionally environmentally friendly, but also highly secure and technologically forward-looking, the new production unit was designed with the aid of an innovative process and architecture development approach that used such novel techniques as digital twins and virtual modelling to achieve the best laid out and most efficient manufacturing facilities possible. A model application of the DigiFab4KMU project, the facilities are a perfect example of the process design and automation potential afforded by new technology and a model for other small to medium-sized tech enterprises in the German-language region and the EU at large to follow. At the same time, the decision to retain its production operations at home – and supercharged with innovative technologies – gives Wibu-Systems full control over the security and quality of its wares, a factor near and dear to the company's heart and readily visible in the look and feel of its physical and software products.

What is happening in Karlsruhe is not only a story of regional excellence, but a case study of global significance in the search for true digital sovereignty. Far from being a return to isolationism, it represents a move towards sharing resources, assets and expertise in the truest sense of the term: Not monopolized or hoarded, but shared among many centers in a connected and multi-polar world. ☒

World's *first* TPM 2.0 with OPEN-*SOURCE software* STACK

By Infineon Technologies AG

☐ Trusted Platform Modules (TPM) enable secured remote software updates, disc encryption and user authentication. Hence, they are crucial for connected industrial, automotive and other embedded devices. To further facilitate seamless integration in Linux-based systems, Infineon Technologies AG now provides its leading OPTIGA™ TPM 2.0 solution with a comprehensive TSS[1] host software implementing the latest FAPI standard. Infineon has developed the open-source software jointly with Intel Corporation and Fraunhofer Institute for Secure Information Technology SIT.

By using Infineon's plug-and-play OPTIGA TPM 2.0, IoT system integrators can significantly improve the security of connected products. Software integration with TSS-FAPI does not require specific skills in low-level security specifications and reduces source code development by a factor of up to 16. Therefore, expenses and time to market can be reduced. Additionally, manufacturers can accelerate the process for certifying their industrial devices according to the IEC 62443 standard for industrial applications, which requires hardware-based safety from level 4 upwards.

The FAPI[2] specification has been released recently as an international standard by the Trusted Computing Group (TCG). The specification is implemented in the TSS stack[3] together with the associated tools and plug-ins. The TSS stack is open-source software, which allows seamless integration of the TPM 2.0 in Linux-based systems. This includes the support of typical Linux software for device authentication, data encryption, software updates and remote device management.

In addition, the FAPI enables the native support of the PKCS#11 standard as a generic interface for user authentication, single sign-on and e-mail encryption/signing. The FAPI provides a default configuration for cryptographic functionalities, system integration and automated processing of security mechanisms according to the latest state-of-the-art and industrial best-practices.

The OPTIGA TPM acts as a vault for sensitive data in connected devices and lowers the risk of data and production losses due to cyberattacks. Infineon's TPMs are certified by independent certification bodies according to Common Criteria, an international set of guidelines and specifications developed for evaluating information security products. The TSS stack, including the recent FAPI, has been verified with the Infineon TPM portfolio to achieve compliance and interoperability.

Availability

Application developers can use the OPTIGA TPM SLB 9670, OPTIGA TPM SLI 9670 and OPTIGA TPM SLM 9670 Iridium boards and TSS Quickstarter offered by Infineon to get started right away. Board and source code packages for the Infineon AURIX™, as well as for Arduino microcontrollers are available now. More information about Infineon's OPTIGA TPM is available at www.infineon.com/TPM. More information about the Github Project (including the downloadable code) is available here: https://github.com/tpm2-software/tpm2-tss ☒

1 TSS – TPM Software Stack - https://trustedcomputinggroup.org/resource/tss-fapi/

2 FAPI – Feature API as specified by the Trusted Computing Group - https://trustedcomputinggroup.org/resource/tss-overview-common-structures-specification

3 https://github.com/tpm2-software/

SILICON TRUST DIRECTORY 2021

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 COUNCIL

The Executive Council has been the steering committee of the Silicon Trust since 2008. It drives the Silicon Trust by defining the topics and directions of the program's publications, workshops and meetings.

INFINEON TECHNOLOGIES

Infineon Technologies AG is a world leader in semiconductors. Infineon offers products and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2016 fiscal year (ending September 30), the company reported sales of Euro 6,5 billion with about 36,000 employees worldwide. Infineon is the world's leading vendor of secure chip card ICs used for passports, ID cards, payment cards, mobile subscriber authentication (SIM cards), access cards and trusted-computing solutions as well as being a technology driver in the hardware-based security field.
www.infineon.com

ADVISORY BOARD

The Silicon Trust Advisory Board supports the Executive Council in defining the direction of the program in terms of public policy and scientific relevance.

BSI

Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security. It has been established in 1991 as a high level federal public agency within the area of responsibility of the Ministry of the Interior. The BSI's ultimate ambition is the protection of information and communication.
Especially in the area of smart card technology, BSI is responsible for the design and definition of secure solution requirements for governmental identification documents. The German ePassport has been introduced in 2005, the second ePassport generation followed 2007, and starting in 2010 the all-new German eID card has opened a new trustworthy approach to Internet authentication for all German citizens. Security of all these documents is based on BSI specifications, developed in close collaboration with European/international standardization bodies and leading industry partners.
www.bsi.bund.de

FRAUNHOFER AISEC

Fraunhofer AISEC supports firms from all industries and service sectors in securing their systems, infrastructures, products and offerings. The institution develops qualitatively high-value security technologies, which increase the reliability, trustworthiness and tamper-resistance of IT-based systems and products. The approximately 80 members of the Fraunhofer AISEC scientific and technical staff balance economic needs, user-friendliness, and security requirements to develop optimally tailored concepts and solutions.
The security test labs are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyze the security of products and hardware components as well as software products and applications. In our laboratories, functionality, interoperability and compliance are tested to give clients targeted, effective advice. Strategic partnerships with global corporations as well as with internationally recognized universities guarantee scientific excellence as well as its market-driven implementation.
www.aisec.fraunhofer.de

SILICON TRUST PARTNERS

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

AdvanIDe

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

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 cybersecurity 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

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

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

GEMALTO

Gemalto, a Thales company, is a global leader in digital security, bringing trust to an increasingly connected world. We design and deliver a wide range of products, software and services based on two core technologies: digital identification and data protection.Our solutions are used by more than 30,000 businesses and governments in 180 countries enabling them to deliver secure digital services for billions of individuals and things. Our technology is at the heart of modern life, from payment to enterprise security and the Internet of Things.We have built a unique portfolio of technology and expertise including physical and digital identity credentials, multiple methods of authentication – including biometrics – and IoT connectivity as well as data encryption and cloud service protection. Together, these technologies help organizations protect the entire digital service lifecycle from sign-up to sign-in and account deletion with data privacy managed throughout.Gemalto is part of the Thales group, a €19bn international organization with more than 80,000 employees in 68 countries worldwide.

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

MASKTECH

MaskTech is the leading independent provider of high secure system on chip designs, embedded ROM masked products, security middleware, certification and integration services focused on human credential applications. MTCOS – MaskTech Chip Operating System – is a high performance and high security operating system, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

MELZER

For decades, MELZER has been internationally known as the leading production equipment supplier for cutting-edge ID Documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customised solutions in combination with the unique modular inline production processes ensure the highest productivity, flexibility and security, leading to maximum yield and the lowest per unit costs. Numerous governmental institutions, as well as private companies, rely on industrial solutions supplied by MELZER. The Melzer product portfolio also includes advanced RFID converting equipment for the production of Smart Labels/Tickets and Luggage Tags.

www.melzergmbh.com

MICROPROSS

Established in 1979, Microprоss is the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Microprоss has proven expertise in the design of laboratory and manufacturing test tools which are all considered as references in their domains. These tools allow users to fully characterize and test the electrical and protocol performance of products such as smartcards and smartphones in design, conformance, and production. In 2015, National Instruments acquired Microprоss.

www.microprоss.com

MK SMART

Established in 1999 in Vietnam, MK Group is the leading company in Southeast Asia with years of experience in providing Digital security solutions and Smart card products for the following industries: Government, Banking and Fintech, Transport, Telecom, IoT, Enterprises, and the Consumer market.

With production capacity of over 300 mio. card per annum and more than 700 employees, MK Smart (a member of MK Group) is ranked under the Top 10 largest card manufacturers globally. The companies production facilities and products are security certified by GSMA, Visa, Mastercard, Unionpay, ISO 9001 and FIDO. Our system and solutions business unit offers advanced issuance solutions and software for integrators and operators in all targeted industries.

MÜHLBAUER ID SERVICES GMBH

Founded in 1981, the Mühlbauer Group has grown to a proven one-stop-shop technology partner for the smart card, ePassport, RFID and solar back-end industry. Further business fields are the areas of micro-chip die sorting, carrier tape equipment, as well as automation, marking and traceability systems. Mühlbauer's Parts&Systems segment produces high precision components.

The Mühlbauer Group is the only one-stop-shop technology partner for the production and personalization of cards, passports and RFID applications worldwide. With around 2,800 employees, technology centers in Germany, Malaysia, China, Slovakia, the U.S. and Serbia, and a global sales and service network, we are the world's market leader in innovative equipment- and software solutions, supporting our customers in project planning, technology transfer and production ramp up.

http://www.muehlbauer.de

OVD KINEGRAM

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

www.kinegram.com

PARAGON ID

Paragon ID is a leader in identification solutions, in the e-ID, transport, smart cities, traceability, brand protection and payment sectors. The company, which employs more than 600 staff, designs and provides innovative identification solutions based on the latest technologies such as RFID and NFC to serve a wide range of clients worldwide in diverse markets.Paragon ID launched its eID activity in 2005. Since then, we have delivered 100 million RFID inlays and covers for ePassports. 24 countries have already chosen to rely on the silver ink technology developed and patented by Paragon ID for the deployment of their biometric electronic passport programs.Today, Paragon ID delivers nearly 1 million inlays each month to the world's leading digital security companies and national printing houses, including some of the most prestigious references in the industry. Through 3 secure and certified manufacturing sites located in France (Argent sur Sauldre), USA (Burlington, Vermont) and Romania (Bucharest), Paragon ID ensures a continuous supply to its local and global clients. Visit our website for more information and our latest news.

www.paragon-id.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

POLYGRAPH COMBINE UKRAINA

State Enterprise "Polygraph Combine "Ukraina" for securities' production" is a state company that has more than 40 years of experience in providing printing solutions. Polygraph Combine "Ukraina" has built up its reputation in developing unique and customized solutions that exceed the expectations of customers and partners. Moreover, the enterprise offers the full cycle of production: from prepress (design) processes to shipment of the finished products to customers.It offers the wide range of products: passports, ID documents, bank cards, all types of stamps (including excise duty and postage stamps), diplomas, certificates and other security documents. Find more information at:

www.pk-ukraina.gov.ua

PRECISE BIOMETRICS

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

www.precisebiometrics.com

PRIMEKEY

One of the world's leading companies for PKI solutions, PrimeKey Solutions AB has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

www.primekey.com

Accelerate your eID project with SECORA™ ID

When time is tight and you need a customized solution …

SECORA™ ID is our new ready-to-go Java Card™ solution optimized for electronic identification (eID) applications. It accelerates your time-to-market through ready-to-use applets supporting rapid project migration. Combined with our free development tool, the SECORA™ ID platform gives you maximum freedom to develop your individual eID or multi-application solutions.

Highlights:

- Ready-to-go solution for fast time-to-market
- Easy and rapid migration of individual projects
- Open platform for highest flexibility
- Best-in-class security controllers and wide choice of packages
- Targeting the highest international security standards for eID applications

Find out more:
www.infineon.com/secora-id

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

SECOIA EXECUTIVE CONSULTANTS

SECOIA Executive Consultants is an independent consultancy practice, supported by an extensive global network of experts with highly specialized knowledge and skill set. We work internationally with senior leaders from government, intergovernmental organizations and industry to inspire new thinking, drive change and transform operations in border, aviation, transportation and homeland security. SECOIA provides review and analysis services for governments in the field of Civil Registry, Evidence of Identity, Security Document issuance and border management. Also, SECOIA specialises in forming and grouping companies for sustainable, ethical sales success. Adding to the consulting and coaching activities, SECOIA offers Bidmanagement-Coaching and RFP preparation / Procurement assistance for Government offices and NGOs. Try us, and join the growing family of customers.

www.secoia.ltd

SIPUA CONSULTING

SIPUA CONSULTING® is a leading and well-established consultancy company, focusing on customized e-ID solutions for government agencies and institutions around the world. Based on detailed market intelligence and long-lasting relationships within the e-ID ecosystem, SIPUA CONSULTING is in the strategic position to conceptionalize, promote and implement various projects along the value chain.

www.sipua-consulting.com

UNITED ACCESS

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

www.unitedaccess.com

WATCHDATA TECHNOLOGIES

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

www.watchdata.com

WCC

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

www.wcc-group.com

WIBU-SYSTEMS

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

www.wibu.com

X INFOTECH

X INFOTECH, a leading systems integrator and a developer of software suite Smarteo, delivers premium solutions for issuing, managing and verification of electronic ID documents and smart cards. The company's turnkey solutions are fully independent and flexible, and in combination with unrivalled team expertise, allow smart card and eID programs to be implemented easily, adapting to any environment by supporting any equipment and chip type. With successfully implemented projects in 45 countries already, X INFOTECH is now a trusted business partner and preferred solutions and services provider for hundreds of customers.

www.x-infotech.com

MASKTECH

We make chips intelligent

MTCOS®

Independent – High Secure Card Operating System

- ELECTRONIC PASSPORT
- ELECTRONIC NATIONAL ID
- ELECTRONIC TICKETING
- ELECTRONIC HEALTH
- ELECTRONIC RESIDENCE PERMIT
- ELECTRONIC DRIVING LICENSE

MTCOS 2.5 EAL5+

certified on IFX, NXP and ST

We hope to see you at one of the upcoming events!

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

Common Criteria

WIBU SYSTEMS

Game over for hackers, crackers, and pirates

When software makes great products and services possible, CodeMeter provides:

- IP protection against reverse-engineering attacks
- Innovative business models for vendors and users
- Security-by-design for software and intelligent devices

Start now and request your CodeMeter SDK
s.wibu.com/sdk-cm

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

SECURITY
LICENSING
PERFECTION IN PROTECTION