NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

AUGUST 2020 | #26

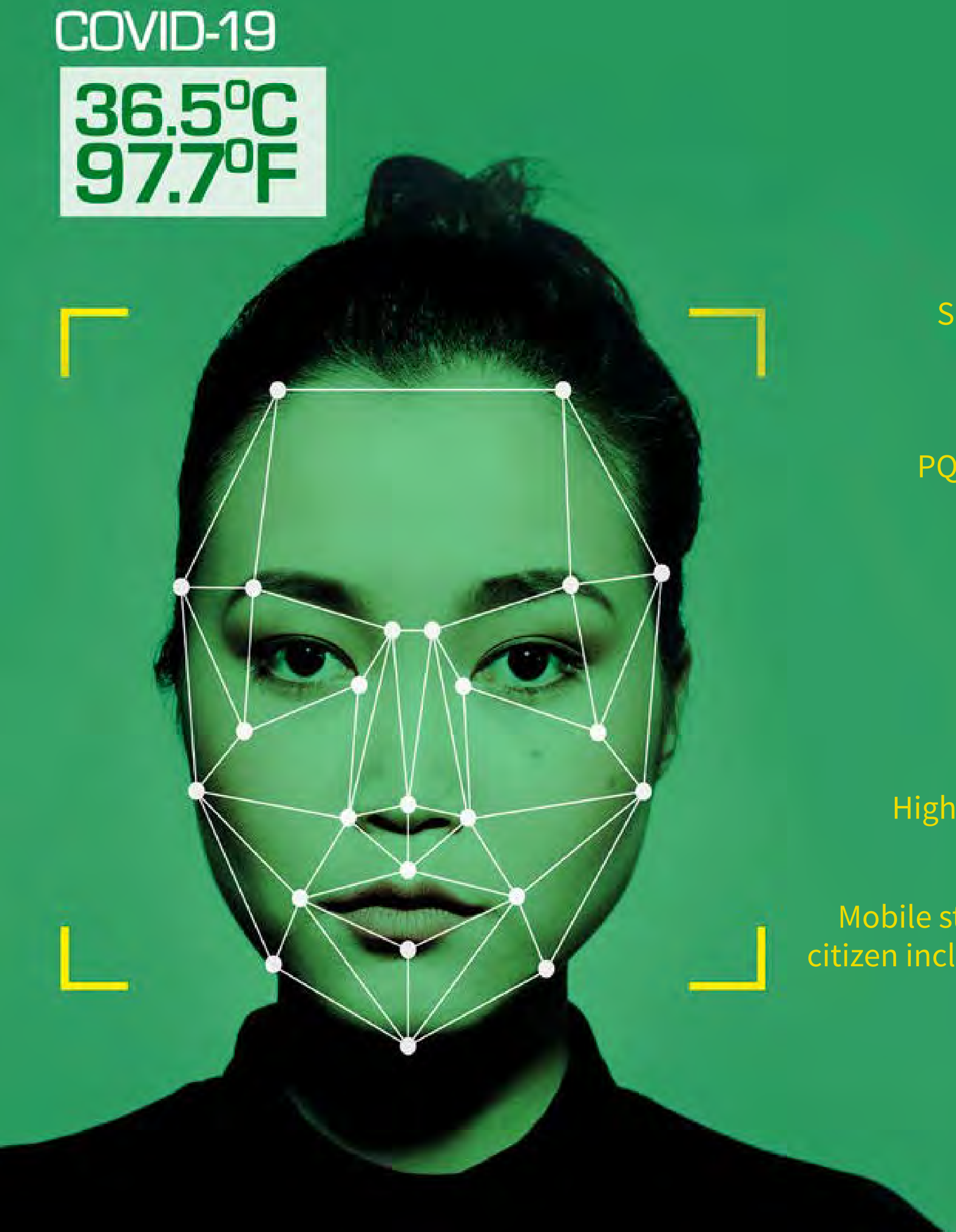
The VAULT

BRAVE NEW WORLD

FEATURED ARTICLE

The reason why secure biometric systems still require hardware based security

Infineon Technologies



ALSO IN THIS ISSUE

Infineon Technologies
Secure Blockchain Access Using Infineon's SECORA™ Solution

Wibu-Systems
PQC4MED Crypto-Agility for Post-Quantum Security In Medical Devices

Cryptovision
Full speed ahead with eID solutions

Mühlbauer
Highly-Secure Document Life Cycle

X-Infotech
Mobile strong authentication for better citizen inclusion into the digital economy

SIPUA Consulting
Introducing SIPUA Consulting A Focus on Africa

Contents

Imprint

THE VAULT
Published bi-annually by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10629 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Rainer Bergmann, Daniela Previtali, Bernd Zwattendorfer, Maurizio Skerlj, Markus Mosenbacher, Alexander Sipua Ngnobamdjum, Markus Hoffmeister, Uljana Belokrinicka, Dr. Mike Bergmann, Carmen Kempka
PHOTOS: WIBU SYSTEMS, INFINEON TECHNOLOGIES, ISTOCKPHOTO, MÜHLBAUER ID SERVICES, CRYPTOVISION, X INFOTECH, KROWNE COMMUNICATIONS, SIPUA CONSULTING
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE
EDITION: September 2020.

Are you *REALLY* JANE *Doe*?

The reasons why secure biometric systems still require hardware-based security

By Bernd Zwattendorfer, Infineon Technologies

□ Are you really Jane Doe?

The proof of a claim of a person's identity – both identification and authentication – are fundamental processes for granting or denying access to services. These being either physical (yes, you really booked the hotel room) or digital online (yes, you are authorized to use the cloud service). Identification and authentication have entered our daily lives, meaning that today different mechanisms for supporting identification and authentication exist.

One easy and user-friendly way is through the use of biometrics. Biometrics, or a biometric characteristic, is defined as "a biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition"[1]. Therefore, by recognizing and verifying certain biometric characteristics (e.g. against a stored template), a person can be distinguished from others and thus uniquely identified and authenticated. Typical biometric characteristics captured for identification and authentication are a person's face, fingerprint, or voice. Of course, other biometric characteristics exist and can be captured for verification. Table 1 briefly lists physiological and behavioral biometric characteristics.

Biometrics is attractive for identification and authentication purposes for several reasons. One of the biggest advantages is that biometric characteristics are universal to humans, i.e. they can be measured from each individual. Furthermore, biometrics provide uniqueness, which allows the distinguishing of individuals from each other without the need of restricting the context. Finally, biometric characteristics very rarely change over time.

Physiological

- Face
- Fingerprint
- Vein pattern
- Palm
- Eye (iris and retina)
- DNA

Behavioral

- Voice
- Signature dynamics
- Typing
- Physical movements
- Gestures

Table 1 - Biometric characteristics

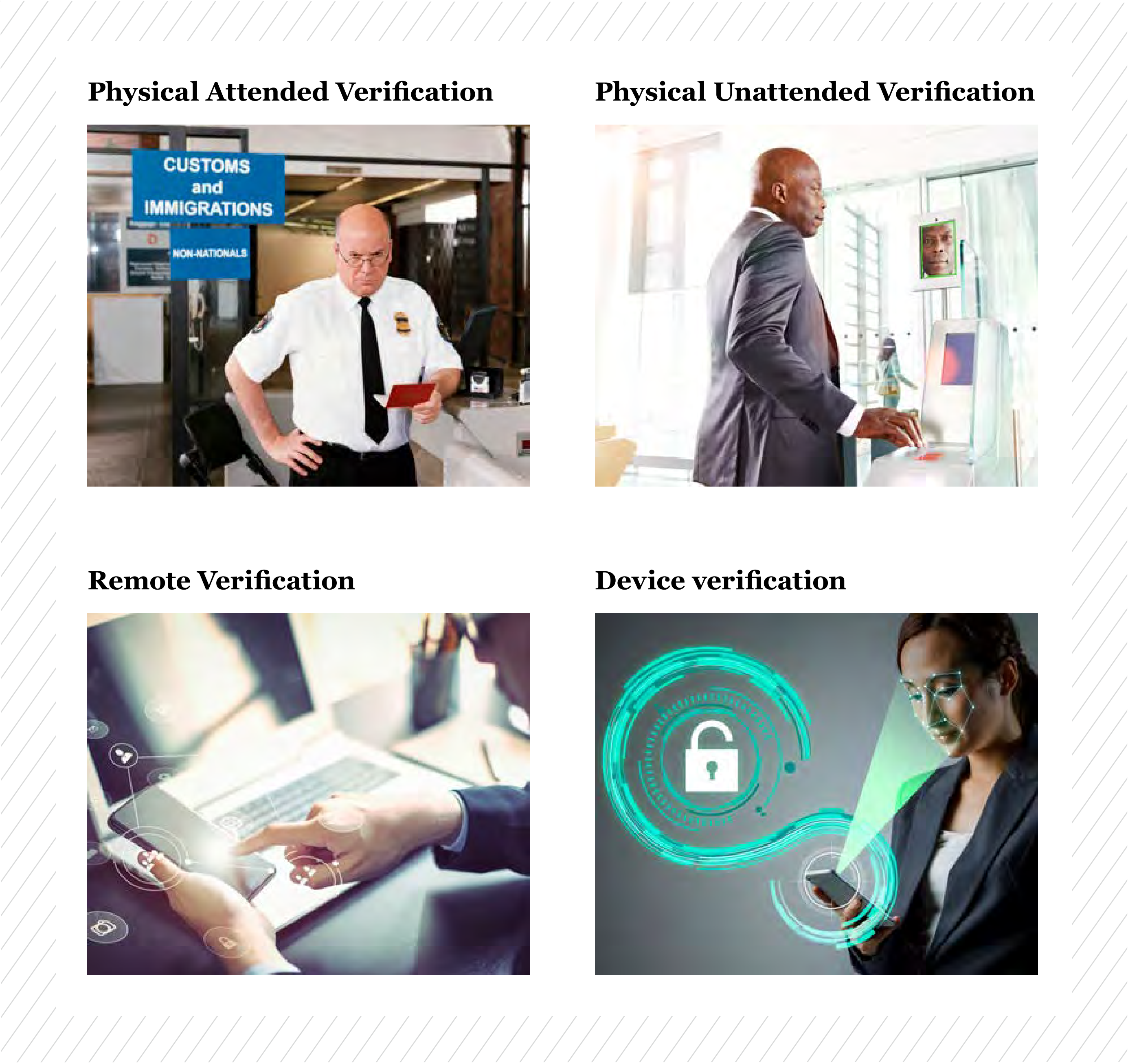
[1] *ISO/IEC 2382-37:2017(en) Information technology — Vocabulary — Part 37: Biometrics*

Biometric use cases

Biometrics can be used in various ways and systems. Biometrics entered our lives many years ago. Typical application areas are travel and border control, logical or physical access and even consumer applications.

For travel and border control, besides facial data, many electronic passports have also been equipped with fingerprints, which are stored on a security chip. Enterprises requiring a high level of security for their physical and logical assets are now protecting themselves with biometrics; For instance, door systems are equipped with biometric access control mechanisms. Finally, nearly every smartphone today contains some kind of biometric sensor, protecting access to the individual device itself.

Biometrics support different use cases, Figure 1 illustrates the more prominent ones in a generic manner. During a physical and attended verification process – even supported by electronic means – a human entity will still perform an additional check on the biometric characteristics. During a physical unattended verification process, biometric verification is fully automated, and access to a building, room, or gate automatically granted or denied. Biometric technologies can also support remote use cases,


Physical Attended Verification

Physical Unattended Verification

Remote Verification

Device verification

Figure 1 - Biometric use cases

e.g. protecting access to a remote online service. Finally, many devices already have built-in biometric sensors that can be used as convenient alternative to PINs as unlocking mechanisms for the devices.

Architectural systems

There is no single, unique approach on how biometric characteristics are captured, where they are stored, and where and how they are processed, e.g. comparing reference data for verification. Different architectural approaches and systems have emerged over the last few years, all displaying both advantages and disadvantages. Table 2 briefly categorizes biometric systems based on biometric capture, storage, and processing and provide implementation examples.

Smart cards, FIDO tokens (Fact Box 1) or electronic passports are typical examples where the biometric data is stored locally in a security chip. This provides users a high level of security and privacy, as the user can keep the card in their domain for control of the data. The sensor for capturing and matching the data can be on the card itself or on an external reading device. If biometric data matching is carried out in the secure element itself, it is usually referred to as Match-on-Card (MoC). If data matching is carried

Where and how are biometrics captured?	• Sensor on device	• On-card finger-print sensor • Smartphone built-in sensor
	• Sensor external to device	• On-card finger-print sensor • Smartphone built-in sensor
Where biometrics are stored?	• Local	• On-card finger-print sensor • Smartphone built-in sensor
	• Remote	• Server • AFIS (Automated Fingerprint Identification System)
Where and how are biometrics processed/ matched?	• Local matching	• Match on Smart Card / Secure Element
	• Reader matching	• Match on the reading device
	• Remote matching	• Match on the system/server

Table 2 - Biometric systems categorized

out on the reading terminal, such as for electronic passports, it is referred to as Match-on-Terminal. In these examples, matching can be executed offline, thus no connection to any remote server is required. However, only 1:1 and no 1:n matching is supported in this case. A 1:1 matching refers to the comparison of a single captured data item against a single stored data item (1 person's biometric information exactly matches 1 stored template), whereas 1:n matching refers to the comparison of a single captured data item against many (n) stored data items. The process of 1:n matching (where 1 person's biometric information is searched in an entire database of templates) is typically supported by a server-based approach because they have larger storage capabilities as well as the required higher computing power.

One example for server-based systems is AFIS (Automated Fingerprint Identification Systems). In such systems, biometric data for verification are captured locally by an external reading terminal and are subsequently transmitted to a remote server for matching against stored reference data sets. The level of privacy is lower compared to chip-based solutions, as users have no direct control over their remotely stored data. However, AFIS supports 1:n matching. Nevertheless, for verification this always requires an online communication channel between the reading device and the server, where all the biometric data is stored for comparison.

The need for hardware-based security

According to the EU data protection regulation (GDPR)[2], biometric data has been classified as one special category of personal data per se and is prohibited from being processed for the purpose of uniquely identifying a natural person. While there are certainly some exceptions for its processing within GDPR guidelines, biometric data is sensitive data in and of itself and therefore is in need of special protection.

Fast Identity Online (FIDO)

FIDO is an emerging industry standard for improving the security of online authentication. Insecure username/password mechanisms should be additionally protected by a strong second factor or substituted by other authentication factors such as biometrics. The main idea is to authenticate locally against a FIDO authenticator (USB token, smart card) and to transmit the authentication result to the online service to decide about granting access to the service or not. By that, no personal-related information such as biometric data is transmitted to the online service. FIDO supports biometric capturing and verification/matching directly in secured hardware on the FIDO authenticator, thus providing a very high level of protection for biometric authentication data.

[2] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

Hardware-based security such as security chips should be the means of choice for protecting security-critical data, such as biometrics. Hardware-based security offers strong tamper-resistant protection across the entire product lifetime, regardless of the application. Hardware-based security can be incorporated into biometric systems and applications, where biometric data can be stored locally or even remotely.

When dealing with biometrics, template storage and its matching procedure are the most security critical functionalities; it is paramount that these features be packed with hardware security. The highest level of security can be achieved, when biometric data is stored in a tamper-resistant security chip, where the matching takes place within the security chip itself. Furthermore, decentralized storage of single biometric templates in a security chip provides higher protection compared to a centralized storage of many different templates in a remote database. If the database becomes compromised, biometric data of many individuals could be revealed. In the case of single hardware-based local storage, only a single template can be disclosed after a successful attack.

Summary

Using biometrics for identification and authentication provides a fast and user-friendly way compared to traditional knowledge and password-based authentication mechanisms. However, whereas lost passwords can easily be recovered by creating a new one, lost biometrics – if they get into the wrong hands – could cause severe personal and financial damage. Biometrics simply cannot be changed; the link to its individual and its identity is in the static nature of biometric data itself. Once compromised, the identity threat will last forever. This is the biggest argument for protecting biometrics properly, preferably with tamper- resistant hardware-based security. ☒

The impact of COVID-19 on biometric verification

The COVID-19 pandemic affects everyone by reducing physical contact, not only with persons, but also with common surfaces. This affects biometric technologies too, especially biometric data capturing mechanisms with commonly used sensors. It is expected that we will see a trend towards contactless biometric capturing mechanisms (face recognition, contactless fingerprint sensors) as well as contact-based sensors for single individuals only (fingerprint sensor on card) in the future.

SECURED *Blockchain* access using Infineon's SECORA™ *TECHNOLOGY*

A Silicon Trust exclusive interview with Infineon's Maurizio Skerlj and Markus Moesenbacher

A blockchain is, in the simplest of terms, a time-stamped series of chained records of data that is managed by a cluster of computers not owned by a single entity. Each of these blocks of data (i.e. blocks) is secured and bound to each other using cryptographic principles (i.e. chain). The blockchain network has no central authority - it is the very definition of a democratized system. Since it is a shared ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.

□ The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. This verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history.

Most of us have heard of blockchain when talking about cryptocurrencies, such as Bitcoin. However, if we look beyond fintech services, it can also be used in other applications such as logistics, energy supplies, social networks, messaging, gaming, online marketplaces, storage platforms, voting systems, predictive markets, online shops and brand protection. The list goes on and on.

Infineon Technologies is also entering the Blockchain arena with their SECORA™ Blockchain solution. Silicon Trust's Program Director, Steve Atkins, spoke to Maurizio Skerlj, Senior Director and Head of Product Line Identity Solutions and Markus Moesenbacher, Head of Product Marketing to understand what Infineon's plans are in this marketplace.

Steve Atkins: *Blockchain technology is more and more present in the marketplace, but how does Infineon contribute to this?*

Maurizio Skerlj: We started with blockchain technology a few years ago and what we noticed is that new applications besides fintech currency and bitcoin started to appear, smart contracts etc. and being a system that provides mutual trust without a central authority is ideal for other applications, especially identity management. When we looked at it we found that it is when people tend to access the blockchain at one point, it is not as profoundly protected as the rest. Once the information is forwarded in the blockchain system it is efficiently protected using the mechanism as a strength. Access can be open when you open up your own access to the system. We have seen the use of people protecting their signature and passwords and with the loss of potentially millions of dollars or pounds or euros worth of bitcoin. The reason is, we need to secure the traffic, and this is exactly where Infineon is using know-how, developed over years, using smart cards and documents like passports to secure the access using the very same encryption and know-how in a different way.

SA: *What markets are Infineon targeting with this solution?*

MS: We don't target a specific market. What we try to provide is a basic technology for security access for blockchain and the cloud and we've been working with a number of companies; ranging from small startups to companies and established system operators. And the applications are very diverse - from smart contracts (something that is definitely needed) to government applications (such as eVoting). Other applications include brand management, supply chain management and actually any use-cases that are based on blockchains can integrate the Infineon solution.

SA: *How is the product supplied?*

MS: Infineon developed first a small starter kit which is ready to use out of the box (”Blockchain Security 2Go”). It's five sample cards - pre-initialized with a ready-to-use blockchain OS that people working with blockchain can recognize, allowing them to perform various functions and it allows those functions to be implemented without a large knowledge about security.

What we did then was to take everything that was made available in this kit and we developed a product that is useful for high volume manufacturing – specifically for integrators and card production – called SECORA™ Blockchain. In the future we would deliver form factors that would enable embedded solutions in such elements as dongles, tokens, contactless cards or other important devices. SECORA™ Blockchain will be supplied by Infineon and distributors from July 2020 onwards.

Steve Atkins: *Markus, we talk a lot about hardware-based security, but what are the actual advantages behind this?*

Markus Moesenbacher: Actually, the distributed nature of the blockchain technology may come with inherent security, but it poses real challenges when it comes to securely interacting with the system.

> “ *What we did then was to take everything that was made available in this kit and we developed a product that is useful for high volume manufacturing – specifically for integrators and card production – called SECORA™ Blockchain*

For example, generating transactions is an extremely sensitive process, because it uses the private key to add new valid data into the blockchain. As these data represent assets, e.g. cryptocurrencies or identities, the highest available protection is needed and we can basically differentiate between three security levels.

The simplest form, Level 1, is just to store the blockchain user credentials on a personal device, like a laptop or a phone: it is convenient, but it exposes the secured information to widely used software attacks.

There is a better level, Level 2, by using a Trusted Execution Environment (TEE) on the device which provides better protection against attacks compared to level one, but it is still not the highest level of protection.

It’s here that Infineon enters the game with a lot of experience in security components – Level 3. The highest security against physical attacks can be achieved using a security microcontroller. The security controller, which has several mechanisms, can protect against attacks such as probing, side channel attacks, or fault injection.

So back to the question ‘Why hardware-based security?’ Let me explain that in a little more detail.

To interact with a blockchain, the user’s private key is both the identity and the security credential. If this key is stolen, the potential damage is immense. Infineon’s extensive security expertise provides the layer of security that is required to protect private blockchain keys. The integration of hardware-based security into blockchain applications such as tokens, hardware modules and smartcards make private keys much more robust against attack. The same technology that we are using for this product is already used for payment cards, for ePassports and many other security applications.

***SA:** How have customers reacted? What have been the use cases that have been realized so far in the area?*

MM: The reaction of customers so far has been very good since we first launched the starter kits. I’ll cover the product later in more detail.

We launched it at TRUSTECH 2018, where we showed a demo and held a speech and we had a lot of very positive customer feedback and high resonance and interest. We also organized hackathons to motivate startup companies to use our Blockchain Security 2Go starter kit.

One such project; for example, the Kryptoshilling of a startup company in Austria and we continue to have more customers who also have good and innovative ideas. One company, BLOCK42, has already developed brand protection based on SECORA™ Blockchain.

***SA:** Can you give a few more details about the actual Infineon offering?*

MM: Infineon provides on one hand as I mentioned already, the Blockchain Security 2Go starter kit, that is available at retailers such as Farnell, Newark, Digi-Key and Mouser. The starter kit is a tool for the customer to enable them to implement their own software on a smartphone and a PC. Support is given by the Github repository and further information can be found at www.infineon.com/blockchain. This is for the development of blockchain security and includes product information as well as information about tools like Github.

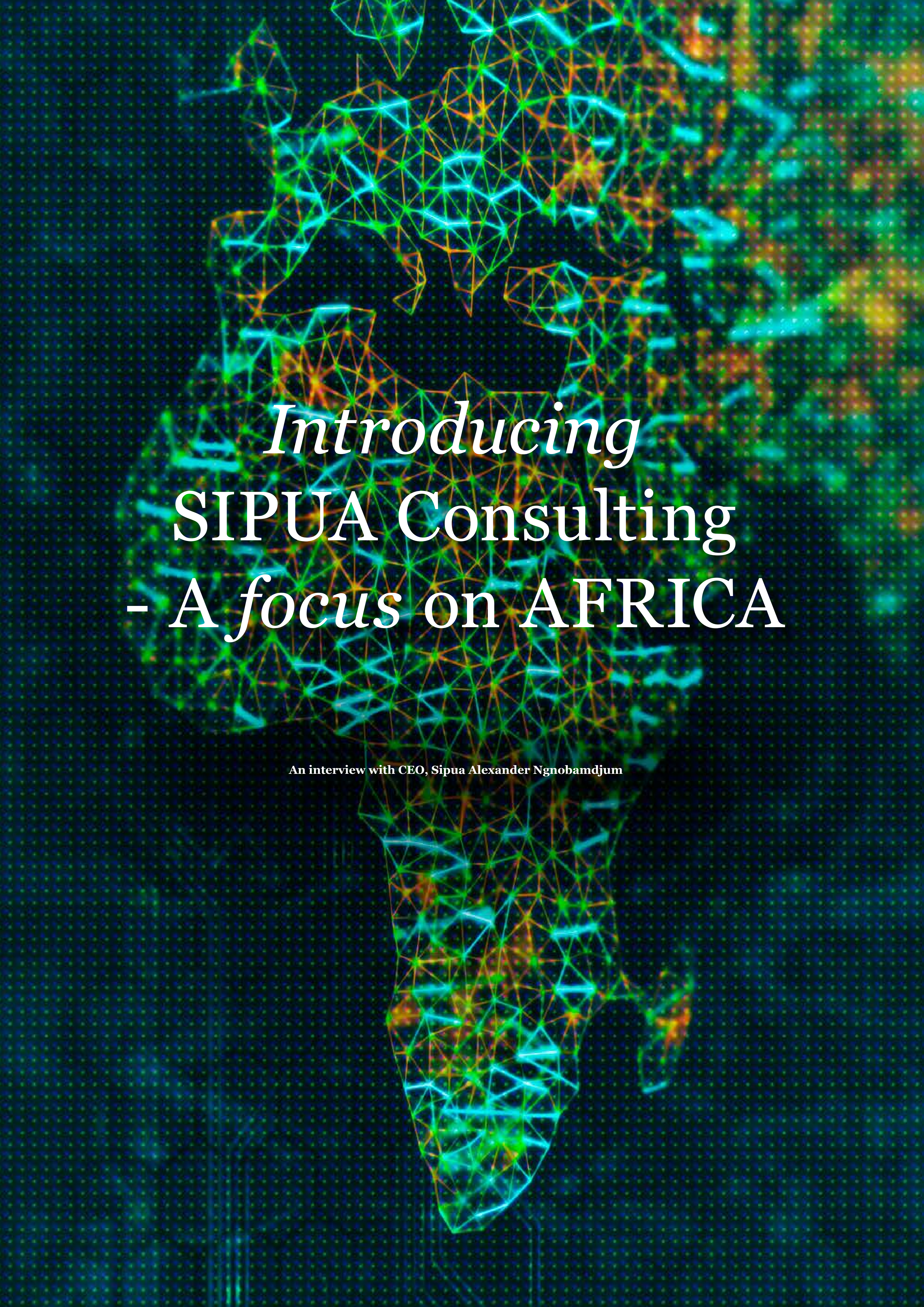
The Blockchain Security 2Go starter kit comprised of five sample cards and documentation with the link to the Github where you can find all the services and support information.

On the other hand, we have a volume product which we launched in April 2020. The volume product is called SECORA™ Blockchain and is an offering which is available in different to form factors such as modules, contactless cards, with NFC-enabled phones and also token form factors.

The product allows a powerful interface for key management and signature creation, while providing the highest possible hardware security, secured by an Infineon secure microcontroller.

***SA:** Gentlemen, many thanks for your time and willingness to speak to us. Best of luck with SECORA™ Blockchain.* ☒

infineon
Java POWERED
Sample card



Introducing SIPUA Consulting - A *focus* on AFRICA

An interview with CEO, Sipua Alexander Ngnobamdjum

□Who is SIPUA CONSULTING?

SIPUA CONSULTING is a consultancy company that has been established since 2012 in Hamburg (Germany). Our core competence is in the field of Government Consultancy, with a focus on African countries.

We have a network of representative offices in various African countries and a team of highly qualified business experts who are monitoring relevant activities in the field of infrastructure, ID-management and energy.

Based on our experiences in the market and on our analysis at the intersection between industry and administration, we are in the unique position to strategize and implement our projects along the value chain from both perspectives; the industry and the administration in charge.

What services do you offer?

We have been part of the electronic ID ecosystem since the establishment of our company in 2012. Our close relationships with stakeholders and decision makers were critical for some of the most successful implementations in regard to e-ID-projects on the African Continent.

Our services are in line with the principals of sustainability and social responsibility as established in the document *"Principles on Identification for Sustainable Development"*, published by the Worldbank and endorsed by numerous institutions around the world in 2017.

Under these guidelines, our partners and clients are benefiting from a broad range of market research activities and matchmaking events tailored to their needs and aspirations. This goes along with an expertise in state-of-the-art ID technologies and some visionary concepts, that we promote amongst institutions and stakeholders in potential markets.

What is your approach to a project? Can you talk us through your process?

Our approach in regard to a new project is quite simple and always straight forward. We ask ourselves:

- What are the needs and challenges of the institutions that are requesting our support?
- What are the proposals and solutions from our partners within the industry?
- How can we bring both parties together?

Normally, the result of such an analysis is a concrete proposal for the road ahead. This includes the definition of milestones and market entry and/or exit strategies.

All parties need to be involved. And through such an approach, even obstacles (that are part of any business activity in new markets) will be handled in the interest of our common goal: a successful project implementation in the field of an institutional ID initiative.

How important are partnerships within your process?

Partnerships are the key to success. That sounds quite obvious, but it is critical in the business field in which we are operating. Concerning the process of implementation for an ID project, we need to streamline the workflow of companies along the value chain, in order to deliver a successful and satisfying product for our clients.

SIPUA CONSULTING had the opportunity to collaborate right from the beginning with INFINEON TECHNOLOGIES as one of their Business Development Partners for the African Continent. And based on such a partnership, it was easy to include many other outstanding companies with their solutions, products and services. We remain grateful to all these partners, because our legacy and our success have been built on a solid ground with long-lasting partnerships.

How do you see the future for the ID market within Africa moving forward?

One thing is obvious – Africa is moving forward. And the importance of a highly professionalized ID management system is evident. If we succeed in providing the right solutions and in assuring the integration of all (c.f. "Principals on Identification"), the full potential of Africa and its wonderful people could be enhanced. And this process should be driven by the institutions in charge on the African Continent and for the benefit of their people. We just have to highlight the need for interoperability and some visionary concepts in order to provide an inclusive development.

This approach will not be the solution to all challenges, but it will help to address some of the most critical ones. SIPUA CONSULTING is prepared to participate in this ongoing discussion. ☒

Full SPEED ahead with eID *SOLUTIONS*

An interview with cryptovision's CEO Markus Hoffmeister

For over ten years, German security software specialist cryptovision has been excelling in the electronic identity document market. For CEO Markus Hoffmeister, the main reason for cryptovision's success is a customer-oriented market approach that relies on open standards and avoids vendor lock-ins. In order to meet the customers' needs even better, cryptovision has now launched "club cv" – a partner program best explained by Markus Hoffmeister himself.

> “ *While our products continue to play a major role in our thinking, our new approach is to act in a more market-driven way – along our market segments IT Security, IoT & Industry, and eID.*

□ ***VAULT:*** *Thank you for taking the time for this interview, Markus. We would have loved to have this chat at the Mindshare, cryptovision’s annual eID and IT security event. Sadly, the corona crisis got in the middle.*

Hoffmeister: Of course, we are disappointed that we had to cancel this year’s Mindshare as an onsite conference. But we had a great Digital Mindshare instead – a two-hour webinar with interesting presentations and interviews. To our regret, there was no way to celebrate our highly popular Cryptonite party online.

Cryptovision’s new strategy

VAULT: *What were the highlights of the Digital Mindshare?*

Hoffmeister: Among other topics, my colleagues presented case studies of some of our most interesting projects, supported by guest speakers from all over the world. Our Latin American representative Fermín Vázquez connected from Mexico and spoke about cryptovision’s Ecuador project – an activity that includes both electronic citizen cards and electronic passports, as well as the required PKI. We also had interview partners reporting live from the Netherlands and spoke to Kim Nguyen, D-Trust’s CEO in Berlin.

VAULT: *Many of the virtual attendants were impressed by the innovative concept of the webinar …*

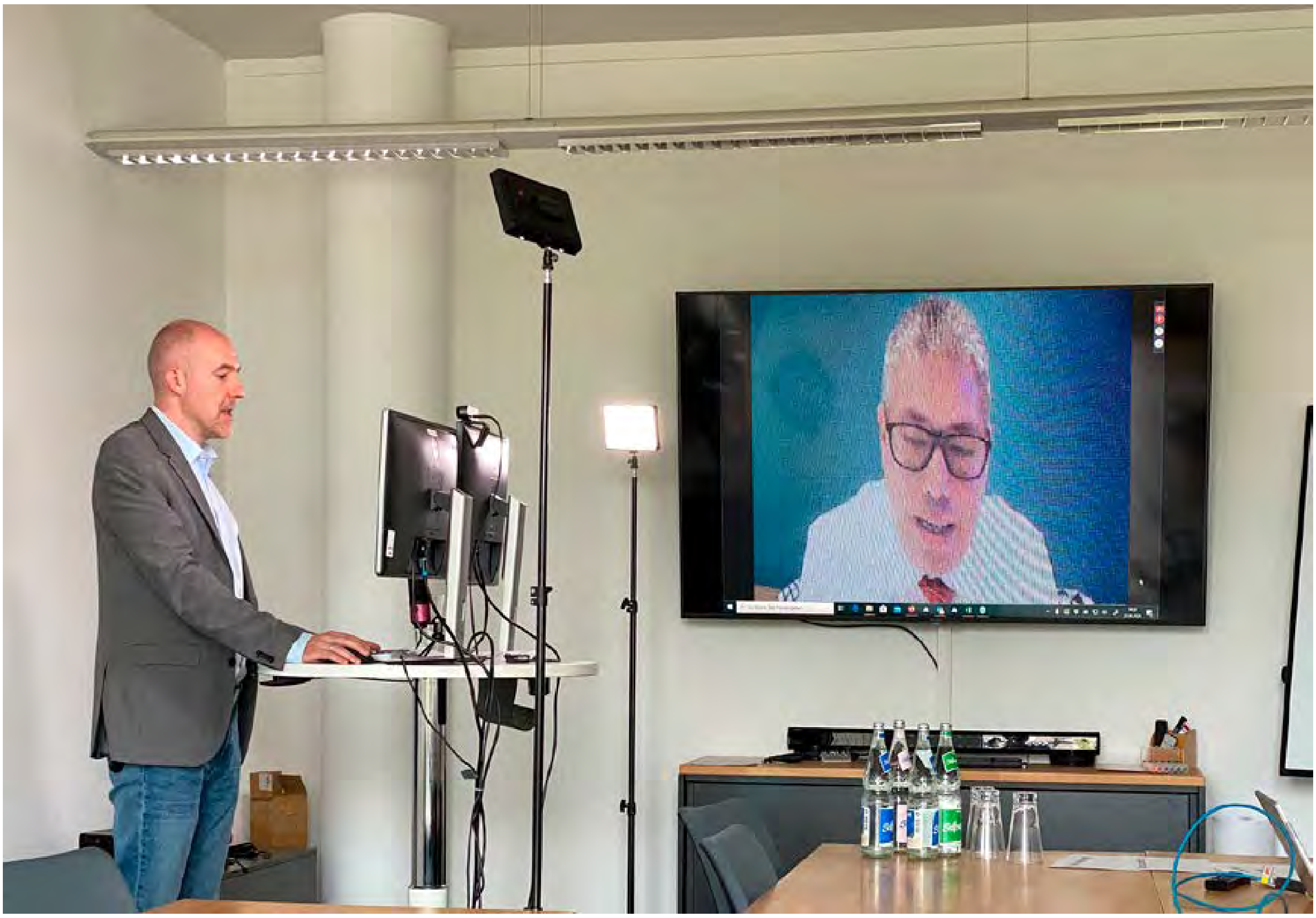
Hoffmeister: Indeed. We presented the Digital Mindshare as a fictive sports event we called “CryptOlympics”. We awarded gold medals and interviewed the CryptOlympic champions. The audience loved it.

VAULT: *Apart from your ability to organize great events, what makes cryptovision so successful in the eID market?*

Hoffmeister: Together with our partners, we create turn-key solutions for our customers; our portfolio covers the whole eID solution stack. As we are neither a card producer nor a system integrator, we focus on the customer’s needs and not on a certain technology we want to sell. This means, among other things, that we rely on open standards and thus avoid vendor lock-ins. And then, we have gathered a great deal of know-how in numerous eID projects in countries such as Malta, Uzbekistan, Ghana and Ecuador – just to name a few, especially with multi-application documents and highly customized eID cards.

VAULT: *You mention partners. Didn’t Infineon recently make an announcement with cryptovision?*

Hoffmeister: Yes, and this was a real milestone for us. Our Java Card based eID application framework ePasslet Suite is now available on Infineon’s Secora ID X – a new plug-and-play chip and operating system platform for realizing highly secured eID documents. ePasslet Suite has long been available on Infineon chip platforms via our partner and customer Veridos, but now, as an additional service, ePasslet can also be directly sourced from Infineon. This new option significantly increases flexibility when implementing card-based eID projects.



Snr. Product Manager Ben Drisch during the Digital Mindshare Interview with D-Trust CEO Kim Nguyen

***VAULT:** Did you make other announcements at the Digital Mindshare?*

Hoffmeister: Yes. My managing director partner Marco Smeja and I introduced cryptovision's new business strategy. So far, our focus has been mainly on products. While our products continue to play a major role in our thinking, our new approach is to act in a more market-driven way – along our market segments IT Security, IoT & Industry, and eID.

***VAULT:** What are the benefits of a market-driven approach in the eID documents segment?*

Hoffmeister: cryptovision is well positioned in the eID market. Our product portfolio contains an eID application suite, a personalization SDK, eID document middleware, and various infrastructure products such as PKI software. However, customers ask for solutions, not for products. As mentioned, cryptovision covers the whole eID solution stack in a customer-oriented way, and we believe that this strategy will be even more successful if we follow a more market-driven approach.

Introducing club cv

***VAULT:** What else happened at the Digital Mindshare?*

Hoffmeister: At the Digital Mindshare, we launched our new partner program, "club cv". Having a strong network of partners and currently facing a huge number of partnership inquiries, we founded club cv to structure our partner-related activities and to optimize cooperation. We know that only if our partners benefit from us the way we benefit from them, a long-term collaboration, including the sharing of leads, is possible.

***VAULT:** What are the benefits of joining club cv?*

Hoffmeister: Club cv is ideal for small and medium eID technology providers, including, but not limited to, card producers, system integrators and state printing agencies. Our partner network enables us to jointly create solutions on the highest level, without an all-dominating, large-scale enterprise being involved. Our contributions are attractive sales benefits, early product releases, and the service of our excellent consultants.

cryptovision club cv

> “Club cv enables us and our partners to jointly create solutions on the highest level.
>
> Markus Hoffmeister,
> CEO of cryptovision

***VAULT:** Do all club cv partners have to commit to revenues?*

Hoffmeister: No. Club cv is meant to be more than a revenue generator; it is a platform to exchange ideas with like-minded people. We allow for putting the focus on mutual technical integration. Keeping our end customers in mind, we want to be able to support more tailor-made solutions and broaden our and our partners' portfolios.

***VAULT:** When will club cv open for applications?*

Hoffmeister: The official start of club cv is scheduled for January 2021. However, we have already opened the Member Level. This means that all our partners have the opportunity to register online as club cv members.

***VAULT:** Where can I learn more about club cv?*

Hoffmeister: You will find all necessary information at the club cv website: www.cryptovision.com/club-cv.

***VAULT:** Finally, will there be an onsite Mindshare again in 2021?*

Hoffmeister: Nobody knows for sure what the situation will be next year. Obviously, many industries, companies and individuals will be longing to get back to normal. A big party may not be the most important thing, but we sincerely hope to make a Gelsenkirchen Mindshare and Cryptonite happen next year – the legendary firework finale may then even be twice as long! ☒

Mobile STRONG *authentication* for *BETTER citizen* INCLUSION into the *DIGITAL* economy

By Uljana Belokrinicka, X Infotech

□ The demand for affordable digital solutions, accompanied by trusted security and protection of data, is growing globally. At the same time, the economic impact of digital identity is hard to overestimate. The McKinsey Global Institute performed research in this area and concluded that, "In the emerging economies, basic digital ID alone could unlock 50% to 70% of the full economic potential, assuming adoption rates of about 70%". The Institute also stated that "By 2030, digital ID has the potential to create economic value equivalent to 6% of GDP in emerging economies on a per-country basis and 3% in mature economies, assuming high levels of adoption".[1] Simultaneously, modern technology promises an optimistic drop in costs for the supporting infrastructure and a reduction of implementation expenses. As a result, digital identity has become a market boosting tool, both for public and private sectors.

Ensuring the reduction of administrative load, growth of citizen streamlined activity and an increase in online generated turnover - digital identity is a priority focus for forward-thinking nations that wish to include citizens into a digital economy. Other essential noneconomic values created by digital identity go beyond quantitative measures; privacy, inclusion protection of rights, international harmonization and transparency.

[1] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

2020 was a challenging year

This present year has demonstrated the importance of having the ability to create streamlined, remote authentication for the normal functioning of the economy. Spring 2020 was the worst, revealing the inferiority of traditional identification and authentication tools. The ability of governments and the financial sector to physically provide public services levels has brought into question. In some countries, renewal of Internet banking credentials became nearly impossible due to closure of all bank branches. Residents of other countries were unable to prolong their permits due to the closure of migration service branches. Elsewhere, citizens were unable to receive ID documents: passports, identity cards, driving licenses, social cards. Citizens of many countries were limited to exercise their voting right due to the postponement of elections. In other countries, patients experienced problems in accessing public health infrastructure for consultation and medical prescriptions. The current situation stresses the importance of digital remote access to services and the ability to get identified and authenticated.

The right to be recognized

Digital services are based on digital identity and authentication. The World Bank's latest research, however, indicates that nearly 1 billion humans or one in seven people globally, do not have a legally recognized ID. Nearly 3.4 billion humans have limited ability to identify themselves in the digital world. The remaining 3.2 billion humans have limited access to efficient digital-identity-based online benefits[2] This is a frustrating statistic in times of globally increasing digital interactions. And an even more terrifying one in times of pandemic situations, when the access to physically provided services is significantly limited. One of the most serious obstacles for citizens is an inability to prove one's identity and to get authenticated properly.

Digital times require digital measures

The important challenges for the digital economy, also pandemic-caused, include convenience and secure digital authentication. Future-oriented governments should seriously consider equipping their citizens with a universal, yet affordable, tool for single remote authentication that works for a range of public services. They may take after a banking sector where the implementation of digital-identity-based online solutions is accelerating.

Mobile scenario

Today, we are witnessing a continuous increase of mobile technology presence in our daily life – even in developing countries. More and more citizens worldwide go online using only their smartphone. The number of mobile users is expected to reach 3.8 billion by 2021 and will continue to grow.[3] This shows that the main channel to approach the needs and challenges of digital identity should be mobile in nature; that it is a universal portal to digital reality and must be used as a trusted tool for authentication of digital identity. The winning scenario to respond to these growing market demands is a combination of easy user experience with the highest possible security.

At X Infotech we are proud to contribute to the economic growth in emerging markets with our Secure Mobile-ID strong user authentication solution, aimed at increasing citizen inclusion into the digital economy, as well as combating pandemic-created access limitations.

Secure Mobile-ID is a 'must-have' component for successful digital transformation. A strong mobile authentication solution is empowering banks and governments to provide digital-identity-based secure online services remotely. Simultaneously equipping end users with easy-to-use mobile applications to be used for authentication to:

- streamlined registration
- e-government services
- financial and banking services
- secure payments
- digital taxes
- online voting
- negotiation closing and electronic document signing
- public health and social services
- visa access and border crossing

This secure PKI-cryptography-based universal solution is accompanied by Digital Onboarding for trusted biometric enrolment. Multifactor strong authentication is possible by combining what the user:

- IS (biometric data)
- HAS (mobile device)
- KNOWS (only-user-known PINs)

Secure Mobile-ID promises a fast and secure journey towards a new reality of mobile-empowered digital identity – welcoming in an era where everyone is able to be digitally identified and has access to basic social and economic services, independently from limitations caused by the absence of ID, a global pandemic or regional distance. ☒

[2] https://id4d.worldbank.org/global-dataset/visualization

[3] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Highly-Secure DOCUMENT Life *CYCLE*

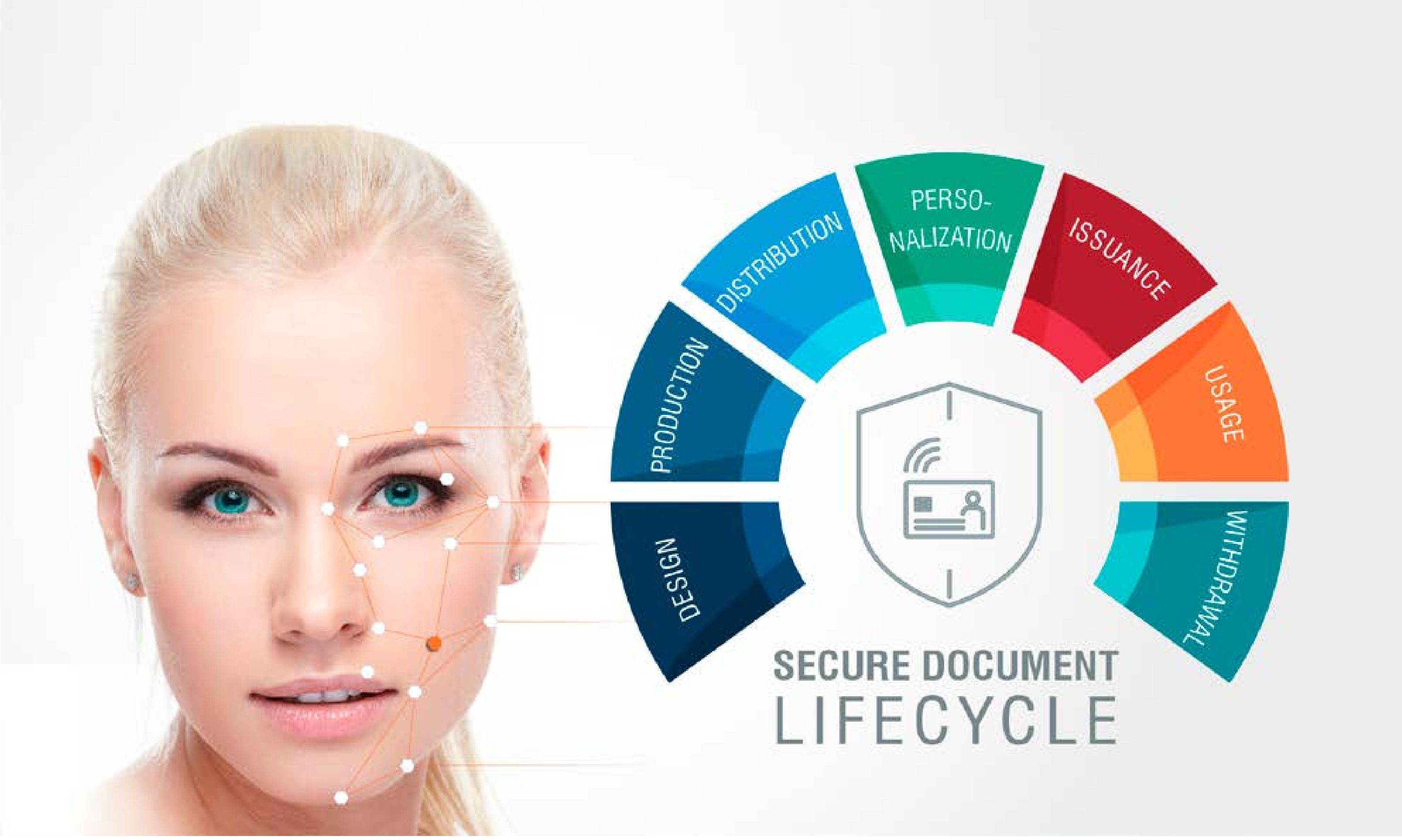
By Dr. Mike Bergmann, Mühlbauer ID Services GmbH

Infrastructure of Trust by Constant Security Advancements

□ Identification documents are not just a piece of plastic, but highly-secure auxiliaries for every citizen of age to actively participate both in an analogue and a digitalized world. The proper identification of citizens is a vital component of a well-functioning society – no matter if it is about political, social, cultural and economic participation or international travel. However, this delicate balance can be upset by criminals and fraudsters, who spare no effort to steal and fake identities. Thereby not only harming the individual as such, but also the whole of society. That is why slashing ID fraud and identity theft, improving document security and creating an infrastructure of trust are high on the agenda of governments and authorities around the world.

But how can ID documents be designed, produced, distributed, personalized, issued, used – and possibly withdrawn – in the most secure and reliable way?

The DESIGN of a secure identity document is science and art in union. The process not only requires skilled and well-experienced designers, graphic artists and security experts, but also a clear vision and understanding of the identity document's intended purpose: Shall it be a national or an international ID document? Which security features shall be included in the document? We can resort to a variety of security features, most of which are endowed with microscopic printing figures or specific color-shifting characteristics, which would make any attempts by forgers to tamper with the document immediately visible. To provide even more reliable protection against copying, the document design may include holograms or security inks which reveal their unique effects in specific angles or when illuminated with infrared or ultra-violet light.



Another vital part of ID document life cycle management, the PRODUCTION process, takes place in a high-security production facility. Regarding the security of the production site, international standards, e.g. the IT security guideline ISO 27001, define common security guidelines for the IT systems used. Furthermore, a company's certification as Security Printer (according to ISO 14298) and as Security Supplier (according to CWA 15374) guarantees total compliance with all required security standards.

To provide reliable information about the life cycle of every single secure document, tracking and documenting the material usage of raw materials, intermediate materials and the final products is crucial. This requires track and trace of every single action of operators, service engineers and all software programs and tools involved in the production process.

A safe storage of blank documents is essential, especially during the DISTRUBUTION process. To avoid security gaps in the document life cycle, it is recommended to store the ready-for-delivery blank documents in a vault, securely transport them in dedicated transportation vehicles and, once they have reached their destination, store them in a secure and manipulation-safe warehouse. To make this process even more secure, one can resort to a technique which combines production and personalization in one process step: Every single document is already pre-personalized with dedicated personal information (e.g. the color facial image or textual elements). Therefore, there are no more blank documents in circulation which could potentially be used by fraudsters. The ID document production of the Republic of Bosnia and Herzegovina serves as a vivid example in this case.

During the PERSONALIZATION process, the citizen's personal data are applied to the blank document. But first of all, the personal data have to be acquired in a secure and reliable way – another possibly weak point in document life cycle management: During the document application process, the applying citizen's identity must reliably be determined, usually by presenting a valid birth certificate. However, in this case, the document authentication might pose a challenge, as the birth certificate may either be very old, from a foreign issuer or printed on plain paper.

This process can be simplified and streamlined by means of self-service kiosks which limit the effort of additional operators. Kiosks automatically capture face images, fingerprints and signature, as well as read already existing ID documents. The verified data is then stored in a civil register and may be enriched with further data (e.g. updated pictures or addresses) over time.

Furthermore, another important link in the chain, the civil register, must be protected and securely connected to the personalization management system. By means of the user management, to which all systems are connected, the life cycle

> *“From the very first design drafts of a document up to the document’s final destruction – every process step has to be carefully planned, managed and put into practice.*

of the secure ID document can seamlessly be documented. The personalization management may be connected to further external systems to provide data preparation or cryptographic functions. In its Doc. 9303, ICAO, an organization of the United Nations, defines valid data preparation guidelines for electronic Machine Readable Travel Documents (eMRTD), including name truncation, splitting or chip data generation. These guidelines guarantee international interoperability and document acceptance and thus ensure document security.

During the ISSUANCE process, the secure ID document is handed over to the corresponding document holder. Before the ID document is officially issued, a verification needs to be conducted to prevent the highly-secure document from being delivered to the wrong applicant: For this very purpose, the biometric verification of fingerprints or face can be employed. To ensure a seamless life cycle documentation of the ID document, operator and document tracking is mandatory.

The ID document’s actual USAGE takes the longest period of its life cycle. On a daily basis, it is used for the proof of identity, e.g. during elections, in casinos or shops, or when opening a bank account. However, the need for document security does not end here, as security also means permanent availability to users: The ID document’s lifetime is usually ten years. To ensure this high durability, the mechanical and electric parameters are important features which can already be influenced during the document’s design and production.

The WITHDRAWAL of an ID document finally marks the end of its life cycle. The process usually combines the document’s physical destruction and logical revocation. Reasons for withdrawing a document can be manifold: For example, the document might have expired or have got lost, so it is revoked with no physical access. Therefore, revocation lists have to regularly be updated to be able to promptly inform authorities not to accept the document if it is presented during a verification process. In addition, a compromized certificate, used for chip personalization, may ease an ID document’s withdrawal.

To summarize, to reliably avoid identity theft and document fraud, the life cycle management of every single ID document in circulation requires the highest security level possible. From the very first design drafts of a document up to the document’s final destruction – every process step has to be carefully planned, managed and put into practice. To avoid friction and glitches between different stakeholders and create a document infrastructure of trust and security, one-stop shop providers can be entrusted highly-secure national ID projects: Offering comprehensive government solutions from one single source, they implement individualized ID projects in a holistic and integral manner.☒

⟨PQC|4|MED⟩

Crypto-agility for post-quantum SECURITY in *medical DEVICES*

Dr. Carmen Kempka, Senior Cryptography Expert, Wibu-Systems

□ Each hardware generation brings new potential, and with it, new ways to attack the integrity and confidentiality of sensitive data. Progress in the field of quantum computers is particularly critical: A sufficiently powerful quantum computer could completely break a large part of the cryptographic methods currently in use and carry out known attacks much more efficiently than conventional computers. In order to be able to guarantee long-term security, it is important to always be one step ahead of the curve and to prepare now for the potential threats brought by the hardware of the future.

PQC4MED is a research project funded by the German Ministry of Education and Research (BMBF), started at the end of 2019, and dedicated to equipping medical devices with post quantum cryptography (PQC) capabilities. As a project coordinator, Wibu-Systems is cooperating with partners from science and industry, to prepare medical devices for the coming post-quantum era through security-by-design. The primary goal of this project is for the medical technology sector to integrate crypto-agility in embedded systems early on in the manufacturing process. Secure elements play an important role in this process, as they can support the flexible substitution of cryptographic algorithms. Algorithms can be replaced in secure elements either "in field" by means of firmware updates or "in factory" by adopting modular hardware. This approach keeps a window open for introducing future algorithms that are resistant against quantum computers, but whose security and robustness are still being investigated. The update process itself must also be protected, especially for "in field" updates, to be able to react robustly to new threats.

Wibu-Systems intends to lay down a new foundation for the production of PQC-capable systems, with a sustainable secure infrastructure and a platform for highly secure updates.

Our Partners

In PQC4MED, we are bundling the competencies of our partners from science and industry. Infineon Technologies AG has already contributed significantly to SPHINCS+ and NewHope, candidates for NIST standardization for post-quantum algorithms. In this project, Infineon is working on long-term security for firmware updates and generic hardware modules for the secure elements planned to run the post-quantum secure algorithms. Schölly Fiberoptic GmbH is implementing and testing lastingly secure update mechanisms for the firmware of secure elements, as well as for software and data protection on endoscopy devices. macio GmbH is supporting PQC4MED with modular software libraries and interfaces for communication between applications and post-quantum secure protectors. The Institute for IT Security (ITS) of the University of Luebeck, Germany is analyzing post-quantum algorithms with a focus on side-channel analysis in software and hardware. The German Research Center for Artificial Intelligence (DFKI) in Bremen, Germany is implementing, integrating, and evaluating post-quantum algorithms for use in medical devices, concentrating on their hardware implementation and evaluation in practice. The research group KASTEL, as part of the Institute for Theoretical Computer Science (ITI) of the Karlsruhe Institute of Technology (KIT), will model and analyze the security of update mechanisms in the search for a verifiably secure update mechanism. Finally, Wibu-Systems AG is contributing its unique expertise and experience with using hardware secure elements as part of a holistic and comprehensive protection and licensing infrastructure.

Crypto-agility: Flexibility is key

Cryptography that is secure against attacks from quantum computers, as well as the mathematical problems it is based on, have received much less investigative attention from researchers than conventional cryptography. By contrast, the problem of factorizing large numbers, on which the RSA cryptosystem is based, was originally introduced by Euclid around 2300 years ago.

This project calls for intensive attention to current progress in the field of post-quantum security and its standardization. At the same time, our update platform and secure elements must be equipped with the necessary crypto-agility to be able to react to new results in the field of post-quantum cryptography if they want to guarantee lasting security.

PQC in the medical field: A special challenge

Medical technology is a market known for its heavy reliance on embedded systems. At the same time, this raises the legal bar considerably in terms of the German Data Protection Ordinance's and EU-GDPR's standards for the trustworthiness, long-term security, and integrity of personal data during processing, transmission, and storage.

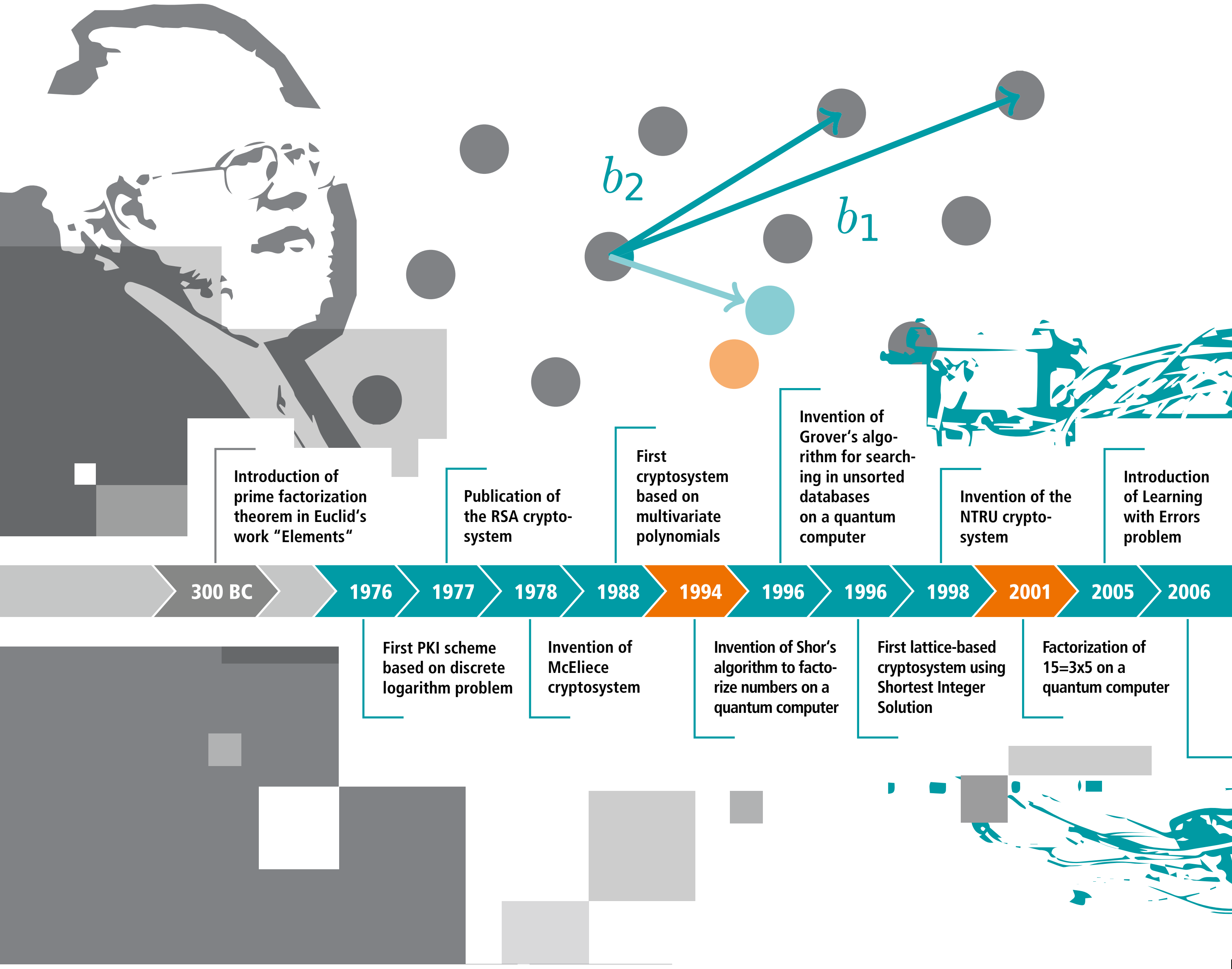
Despite the often lower memory capacity and computing power of embedded systems, the high security requirements for medical devices must be met, and both highly sensitive patient data and the intellectual property of the often extremely complex software on medical devices must be protected in the best possible way.

Is conventional cryptography really threatened by quantum computers?

Many of the common encryption, signature, and key exchange methods are based on hard mathematical problems that cannot be solved with currently available algorithms with the ease or speed needed in actual practice to crack the encryption. For example, RSA encryption is based on the problem of factorizing large numbers, while cryptographic algorithms such as DSA, ECIES, ECDSA and ECDH are based on discrete logarithms. These are just some of the cryptographic algorithms genuinely threatened by quantum computing.

In 1994, Peter Shor first developed an algorithm that can efficiently factorize large numbers using a quantum computer. This algorithm can be extended to calculate discrete logarithms, even on elliptic curves. In 1996, Lov Grover developed a quantum algorithm that efficiently finds elements in an unsorted database, also endangering symmetric cryptography.

The mentioned asymmetric cryptographic algorithms based on factorization or discrete logarithms would be broken by a sufficiently strong quantum computer. For most of the commonly used symmetric schemes and hash algorithms, the key length or output length would have to be at least doubled in order to achieve a similar level of security as they had without the availability of quantum computers.



300 BC: Introduction of prime factorization theorem in Euclid's work "Elements"

1976: First PKI scheme based on discrete logarithm problem

1977: Publication of the RSA cryptosystem

1978: Invention of McEliece cryptosystem

1988: First cryptosystem based on multivariate polynomials

1994: Invention of Shor's algorithm to factorize numbers on a quantum computer

1996: Invention of Grover's algorithm for searching in unsorted databases on a quantum computer

1996: First lattice-based cryptosystem using Shortest Integer Solution

1998: Invention of the NTRU cryptosystem

2001: Factorization of 15=3x5 on a quantum computer

2005: Introduction of Learning with Errors problem

2006

How acute is the danger of quantum computers?

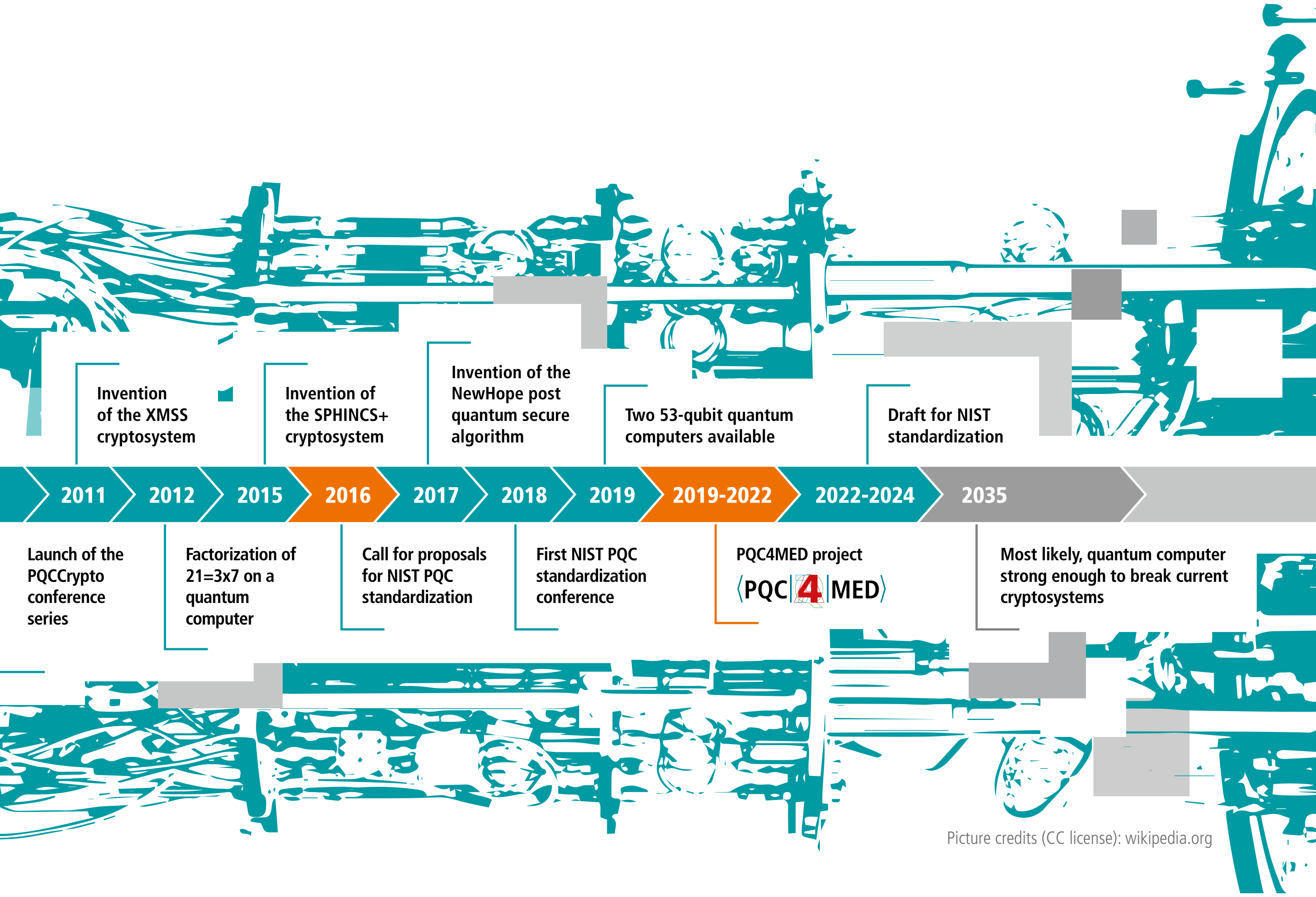
When Shor and Grover published their algorithms, quantum computers were still a theoretical construct, with their actual reality seemingly far away. Then, in 2001, the first number was factorized on a working quantum computer: 15 = 3 x 5.

Today, quantum computers with more than 50 qubits exist. Both IBM and Google have already built a 53-qubit quantum computer, and several other companies are actively researching the construction of quantum computers of different architectures. Programming languages for quantum computers have already been developed.

However, this does not yet represent an acute danger for the cryptographic procedures currently in use. In order to break RSA 2048 by factorization, a few thousand qubits would be necessary even on an ideal, error-free quantum computer. However, due to the error-proneness and short lifespan of quantum states, one would actually need a few million qubits. Breaking discrete logarithm-based methods such as ECDSA would be a challenge of a similar order of magnitude.

At what point do we have to start worrying?

A very simple estimate is provided by Mosca's Theorem: "If X + Y > Z, then worry"



Invention of the XMSS cryptosystem

Invention of the SPHINCS+ cryptosystem

Invention of the NewHope post quantum secure algorithm

Two 53-qubit quantum computers available

Draft for NIST standardization

2011 | 2012 | 2015 | 2016 | 2017 | 2018 | 2019 | 2019-2022 | 2022-2024 | 2035

Launch of the PQCrypto conference series

Factorization of 21=3x7 on a quantum computer

Call for proposals for NIST PQC standardization

First NIST PQC standardization conference

PQC4MED project

⟨PQC|4|MED⟩

Most likely, quantum computer strong enough to break current cryptosystems

Picture credits (CC license): wikipedia.org

Here, X is the time for which our currently used cryptography has to remain safe. Y is the time needed to prepare our infrastructure for switching its cryptographic paradigm, substituting the corresponding procedures, and re-protecting all data currently protected with previous procedures. Z is the time it takes until a quantum computer is available that is powerful enough to break current cryptographic procedures. According to the NIST PQC project, this could be as soon as Z=15 years.

Expert groups and standardization committees are currently working intensively on post-quantum security. The selection of candidates for NIST standardization is already in its second round, and a draft for the standardization of post-quantum-secure methods is planned for 2022-2024.

It is difficult to predict when exactly a quantum computer will exist that can break current cryptography. It is important, however, that the move to post-quantum-secure procedures takes place before this happens. Our infrastructure must already be adapted to PQC by then, and sensitive data must already be protected with procedures that are robust against quantum computers.

How does post-quantum cryptography work?

Like most cryptography used so far, post-quantum secure methods are based on hard mathematical problems, for which neither a conventional nor an efficient quantum algorithm has yet been found.

> *“Like most cryptography used so far, post-quantum secure methods are based on hard mathematical problems, for which neither a conventional nor an efficient quantum algorithm has yet been found.*

Candidates for post-quantum secure methods are lattice-based methods, code-based methods, isogenies (mappings between elliptic curves), multivariate polynomials, and hash-based methods. All of these methods differ strongly with respect to their key size, security, and efficiency. Furthermore, there are strong differences in their suitability for encryption and signatures. PQC algorithms are often less well studied cryptanalytically than conventional cryptography. Especially for the security of embedded devices, which is dependent on efficient algorithms, this introduces a risk that already implemented methods might have to be replaced. In order to achieve long-term security and to be able to react with sufficient speed to new cryptanalytic results, a high degree of crypto-agility – even across different PQC classes – must be guaranteed.

The PQC4MED project

PQC4MED is dedicated to crypto-agility for embedded devices with applications in critical infrastructures, such as medical devices. In order to guarantee long-term information security, "long-term security-by-design" must be achieved as early on as possible in the development of new device generations. This means equipping embedded systems with hardware resources that are made with the later integration of new cryptographic procedures in mind.

An updatable secure element forms the basis for any long-term guarantee of QC-resistant procedures and serves as an anchor of trust that enables "crypto-agility". This means that potential threats are fended off long before they take effect.

Crypto-agility needs to be achieved by:

- Developing and integrating powerful and flexible secure elements with upgradeable firmware.
- Developing a backend infrastructure with protection, licensing, and key management tools secure enough against quantum computers and resources for automating and controlling the system.
- Providing a process and user interface for on-site updates.☒

SPONSORED BY THE
Federal Ministry
of Education
and Research

Timeline illustration credits;
https://en.wikipedia.org/wiki/File:Quantum_Computer_Zurich.jpg under CC 2.0 https://creativecommons.org/licenses/by/2.0/
https://de.wikipedia.org/wiki/Peter_Shor#/media/Datei:Peter_Shor_2017_Dirac_Medal_Award_Ceremony.png under CC 3.0 https://creativecommons.org/licenses/by/3.0/
https://en.wikipedia.org/wiki/Lattice_problem#/media/File:CVP.svg under https://creativecommons.org/licenses/by-sa/4.0/

SILICON TRUST DIRECTORY 2020

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.

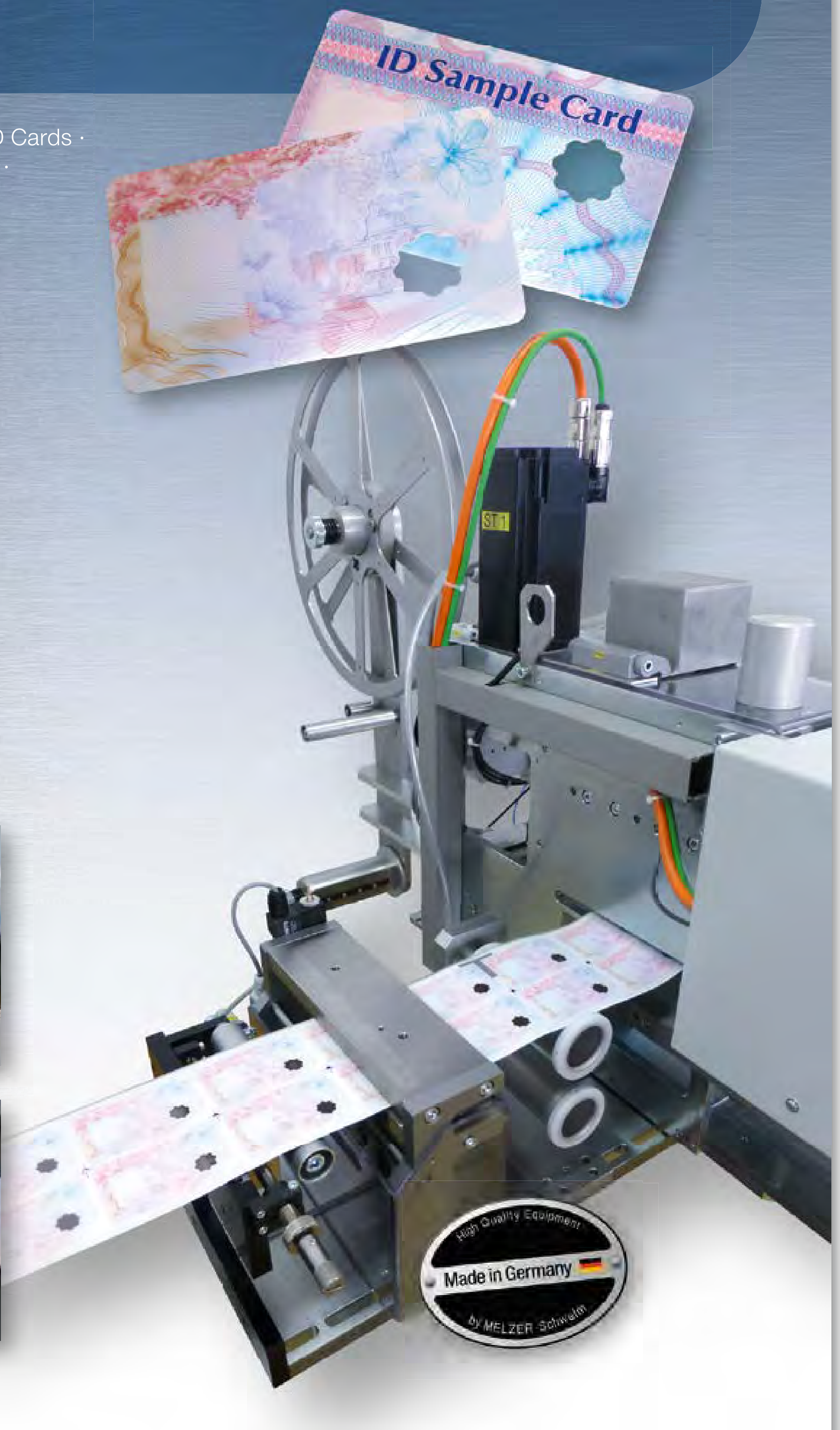
www.aisec.fraunhofer.de

Inline Window Application

IPS

Inline Production System for ID Cards · Data Pages · Driving Licenses · Resident Permit Cards

- ▷ Fully automatic punching and inserting
- ▷ For cards and data pages
- ▷ Zero gap technology
- ▷ Full lamination for utmost durability



INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

www.melzergmbh.com

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

With 60 years of experience MELZER has been internationally recognised and established as the leading equipment supplier for the production of the most advanced ID documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customized solutions, the modular machine system and the lean production approach ensure and maintain unsurpassed yield rates, flexibility and profitability. The MELZER product portfolio also includes a broad range of versatile RFID converting equipment.

www.melzergmbh.com

MICROPROSS

Established in 1979, Micropross is the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Micropross 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 Micropross in order to accelerate their development and strengthen them as the leader on their market, constituting a major milestone in the life of both companies.

www.micropross.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 protection against counterfeiting and maintains close contacts with police forces, customs authorities and internationally reputed security specialists. OVD Kinegram offers a full range of services: consulting, design, engineering, in-house production, application machines and support as well as after-sales service.

www.kinegram.com

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

X INFOTECH
secure identity and payments
Surname / Nom
JOHNSON
Given name(s) / Prenom(s)
CATHERINE
Personal No. / Num. personnel
241193-12421
Date of birth / Date de naissance
24.11.1993
Date of expiry / Date d'expiration
12.05.2021.
Holder's signature / Signature du titulaire
PA1055321
PASSPO
X INFOTEC
4407 8300 4938 3400
VALID FROM 05/16
EXPIRES END 05/21
JOHN JOHNSON
VER'S LICENSE
Surname / Nom
JOHNSON
Given name(s) / Prenom(s)
ROSE
Date of birth / Date de naissance
24.11.1990
Sex
FEMALE
Driving license No
PA2451631
Date of expiry / Date d'expiration
12.05.2021.

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

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.

TELETRUST

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the quality seal "IT Security made in Germany" and runs the IT expert certification programs "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Engineer for System Security" (T.E.S.S.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

www.teletrust.de

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

Cognitec

The trusted face recognition company since 2002

Most experienced and highly trusted

Cognitec has been providing face recognition systems to government and commercial clients worldwide for almost 20 years. Proud to maintain a stable, leading position in the industry, we are committed to delivering the best solutions available on the market.

Focused research and development

We use state-of-the-art machine learning techniques and deep learning principles to achieve continuous advancement of the various algorithms contained in our core technology.

Reliable customer service

Cognitec's clients rely on collaborative customer service, fast response times and competent work.

Superior technology

Our algorithms perform the most important face recognition tasks with market-leading speed and accuracy. Independent evaluation tests and real-life installations continue to prove the exceptional performance of Cognitec's technology.

Successful projects worldwide

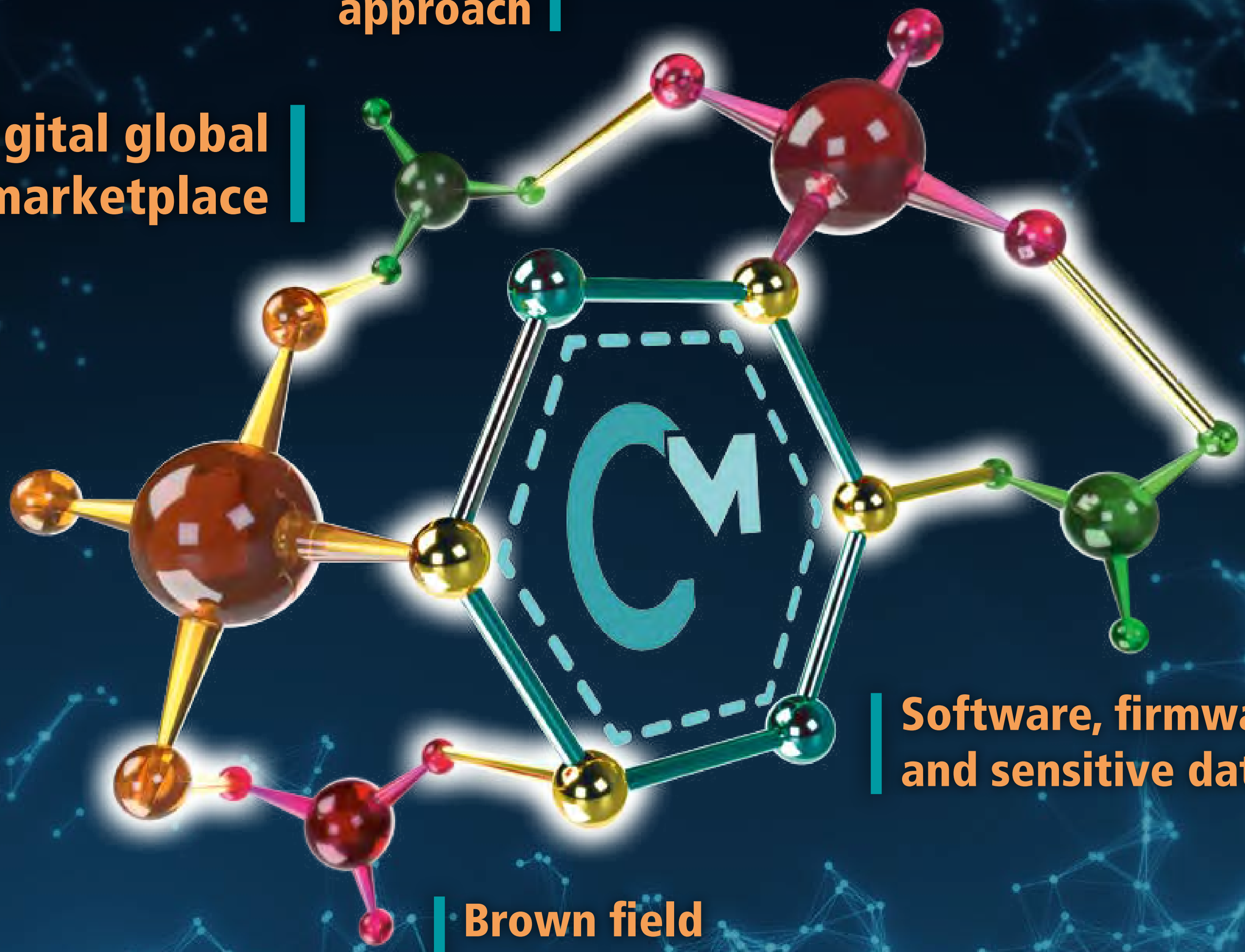
Alongside image database searches that prevent ID fraud and support criminal investigations, Cognitec's technology drives cutting-edge video security, eGate, people analytics, and photo indexing solutions.

www.cognitec.com | info@cognitec.com

CodeMeter – the Catalyst of the IoT driven Economy

Let CodeMeter inspire you with new license-driven business models

- Protect your digital assets from piracy and reverse engineering
- Secure the integrity of your endpoints from tampering
- Implement license-based readily adaptable business models



Customer centric approach

From the cloud down to FPGAs

Digital global marketplace

Software, firmware, and sensitive data

Brown field and green field

Don’t wait any longer
Start protecting your IP now!
s.wibu.com/sdk-cm

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

SECURITY
LICENSING
PERFECTION IN PROTECTION