NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

AUGUST 2023

The VAULT

QUANTUMania!

FEATURED ARTICLE

Beware the Quantum Revolution!

Quantum Computers Pose Grave Risk to Digital ID Security

Infineon Technologies

ALSO IN THIS ISSUE

Eviden
Post-Quantum Cryptography on eID Documents

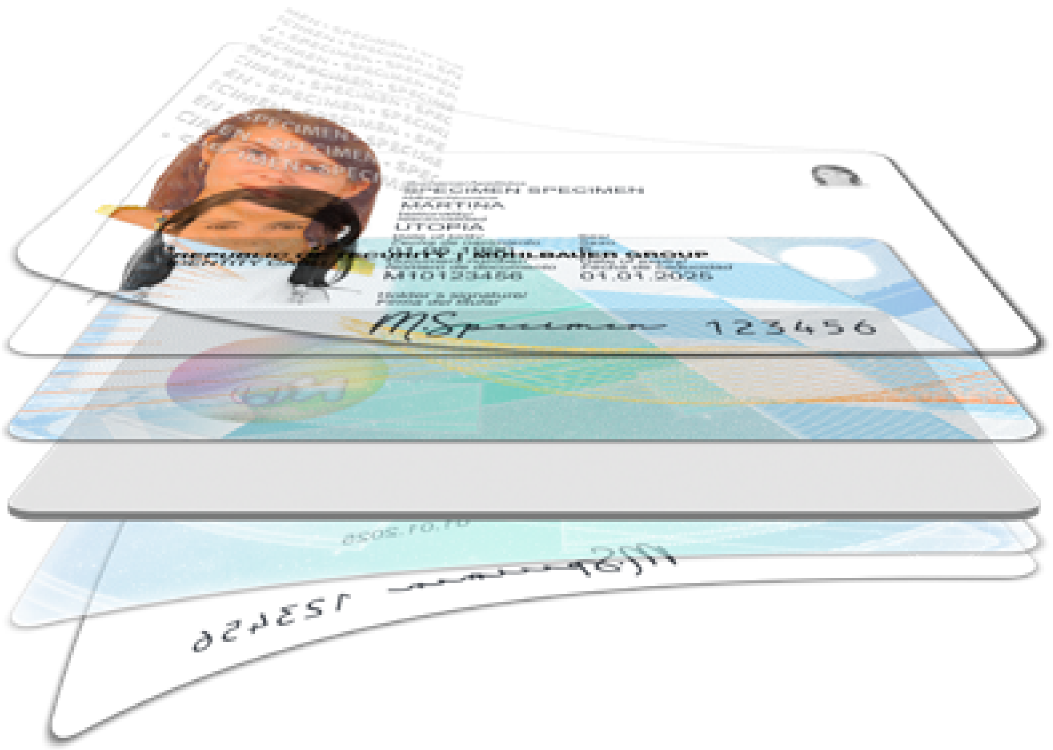
Wibu-Systems
Obfuscation vs Encryption: Friend or Foe?

Mühlbauer Group
ID Cards under the Magnifier

Contents

Imprint

THE VAULT ISSUE 37
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Nina Eggermann
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Steve Atkins, Katharina Schuldt, Robert Bach, Vasco Gomes, Klaus Schmeh, Dr. Carmen Kempka, Maurice Heumann.
PHOTOS: ISTOCKPHOTO, WIBU-SYSTEMS, MÜHLBAUER, INFINEON TECHNOLOGIES, KROWNE COMMUNICATIONS, EVIDEN
EDITION: AUGUST 2023. No portion of this publication may be reproduced in part or in whole without the express permission, in writing, of the publisher. All product copyrights and trade- marks are the property of their respective owners. all product names, specifications, prices and other information are correct at the time of going to press but are subject to change without notice. The publisher takes no responsibility for false or misleading information or omissions.



ID CARDS under the *magnifier* – HOW does the *HOLDER'S PORTRAIT* get on the PASSPORT?

By Katharina Schuldt, Mühlbauer Group

Whether in color or in black and white, today nearly every official national Identification Card features a picture of the cardholder. However, since the cards are usually valid for several years and the cardholder often changes his or her appearance during this time, the question arises as to the significance of the image. Does this image contribute to the security of the document at all? Is it even checked when passing a security control, and if so, how?

To answer these questions, we first need to look at how the image gets onto the ID card and what details are shown. A German specialist for Identification and Authentication solutions, the Mühlbauer Group, provides us with important insights into the creation and production of an ID card.

“A national ID card always consists of several layers,” explains Martin Ederer, team leader of the Document Solution department at Mühlbauer. “Each layer has its own function and specificity. We, at Mühlbauer, have developed machines and suiting software that do not simply print the cardholder's image, previously taken at an enrollment station, onto the card.” That simple print would not be tamper-proof and would therefore be more of a security vulnerability, than an important ID card component.

Instead, Mühlbauer has developed the MB ALFRESCO® technology, which smartly combines color picture personalization with laser engraving. Thereby the personalization process for a standard polycarbonate ID Card starts with the image processing: The image of the holder is divided into color and greyscale. During the pre-personalization, the greyscale elements, which contain all of the picture’s contrast information, are laser-engraved into the inner layer of the card body. The picture’s remaining color parts are converted to a separate color image and inkjet-printed on the blank document’s surface.

With this method, high resolutions can be achieved, which enables the retention of all the photo details such as moles and other special characteristics. As protection against external influences, an additional coating is applied to the image area. The finely structured coating offers a further increase in image quality.

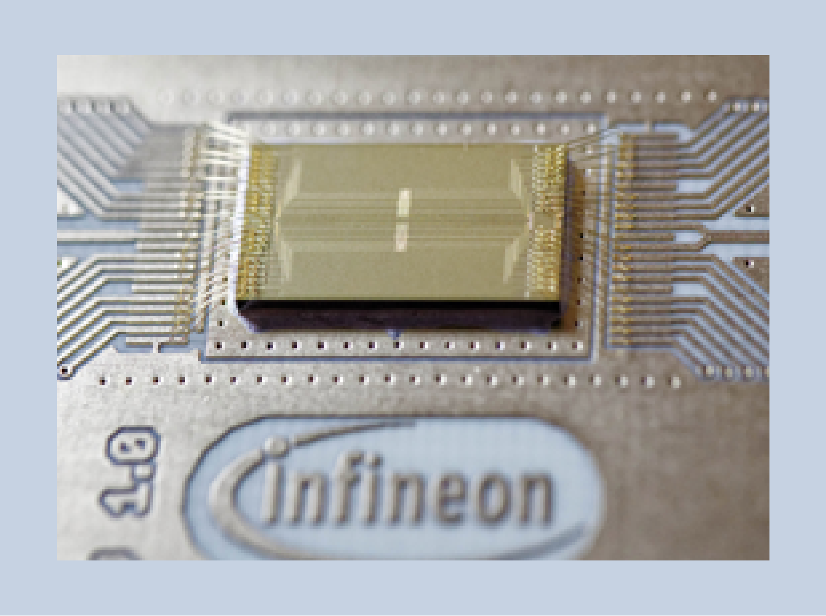
KATHARINA SCHULDT *is International Marketing Manager at the German technology company Mühlbauer in Roding. Before moving to the Upper Bavarian Forest, she was responsible for the promotional videos and product catalogs of the well-known toy manufacturer PLAYMOBIL near Nuremberg. She graduated in Journalism and Business Communication at the University of Europe for Applied Sciences in Iserlohn, Germany and can now look back on 10 years of experience in internal and external communication, guerilla marketing, video production and copy writing. Today she applies her creative ideas and the collected expertise to professional articles for the Mühlbauer Group.*

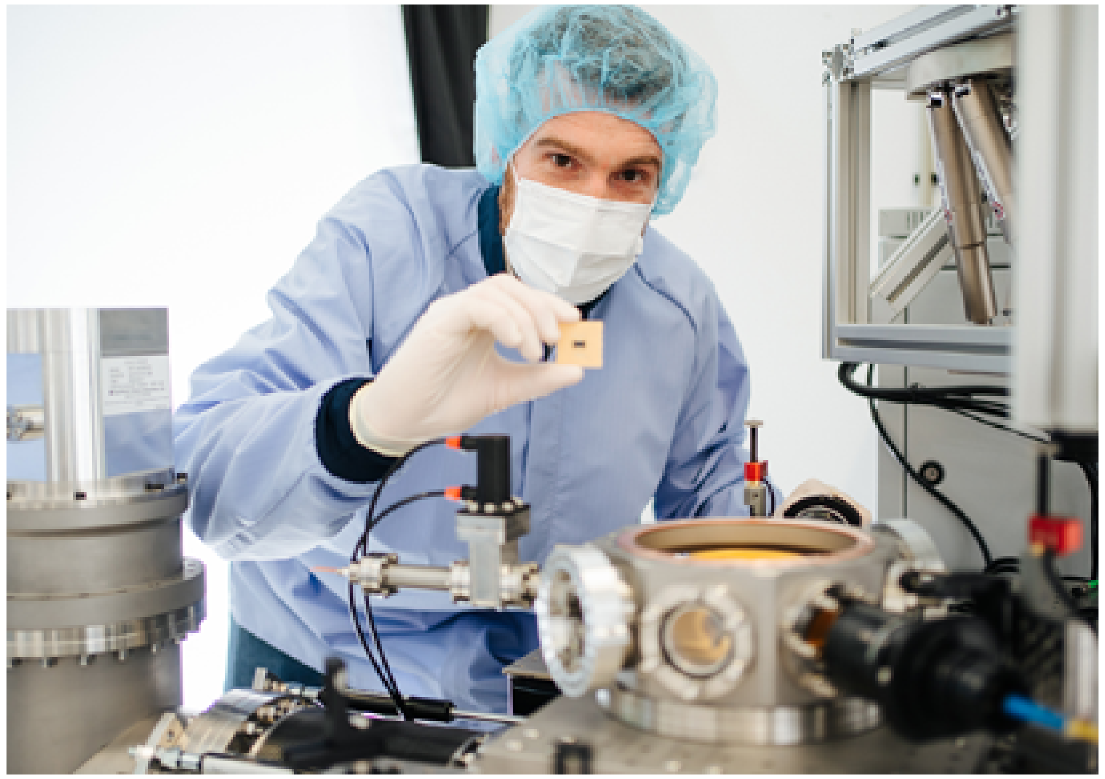
With such a detailed image of the cardholder, the security personnel at border crossings and airports naturally have completely different possibilities than with a simple, low resolution print. But are the images actually reviewed at all? Yes, they are! During manual border control, the border official checks whether the picture and the person match. Nowadays, so-called eGates are taking over this task at more and more checkpoints. Here, a camera matches the image stored on the chip of the ID document with the person. Thanks to artificial intelligence, even two people who look similar can be distinguished on the basis of small attributes. This often prevents people with false documents from passing through border controls undetected.

However, in order to protect the documents themselves from tampering, further state-of-the-art and forgery-proof technologies are needed. Here, too, the German security expert has taken several precautions to make counterfeiting virtually impossible, as early as in document production. As the greyscale information remains inside the document body, attempts to remove the photo can be easily detected. The greyscale picture can be additionally verified under infrared light. Due to the special color properties of the Mühlbauer 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. The complete document features a durability of at least 10 years.

Thus, we see that both the way an image is applied to a security document and the means of checking that image for counterfeiting, are of particular importance to security. The better the quality of the image, the more details can be checked for consistency. ☒

INFINEON TEAMS up with eLEQTRON to deliver *three generations* of trapped-ion QUANTUM PROCESSOR UNITS





Infineon Technologies AG and eleQtron GmbH, a pioneer in Quantum Computing (QC) from Siegen, North Rhine Westfalia, Germany, have announced their partnership to jointly develop trapped-ion Quantum Processor Units (QPUs) for scalable quantum computers. This second Infineon partnership with a key player in the ion-trap field is the first commercial activity in the German QC ecosystem. It underscores Infineon's prominent position in offering industry-leading ion trap QPUs that are manufactured predictably, repeatably, and reliably.

"As a leading company in developing quantum computing hardware, Infineon's goal is to provide the core components and, together with our partners, enable the first meaningful quantum computing systems based on trapped-ion technology. We contribute unique technology and world-class fabrication capabilities towards achieving quantum usefulness," said Richard Kuncic, Senior Vice President and General Manager Power Systems at Infineon Technologies. "Being chosen by eleQtron as a QPU supplier will enable us to accelerate our quantum computing hardware roadmap and expand our business in this emerging segment."

"Our partnership with Infineon represents a significant milestone in our strong mission to develop and competitively offer largely scalable quantum computing systems with high computing power, available for the huge business applications market," said Jan Leisse, CEO eleQtron. "We are confident that our pioneering technology based on ion traps and radio frequency waves, combined with Infineon's capacity and expertise in innovative QPU production, will provide the foundation for building quantum computing systems ready for first applications until mid-2027."

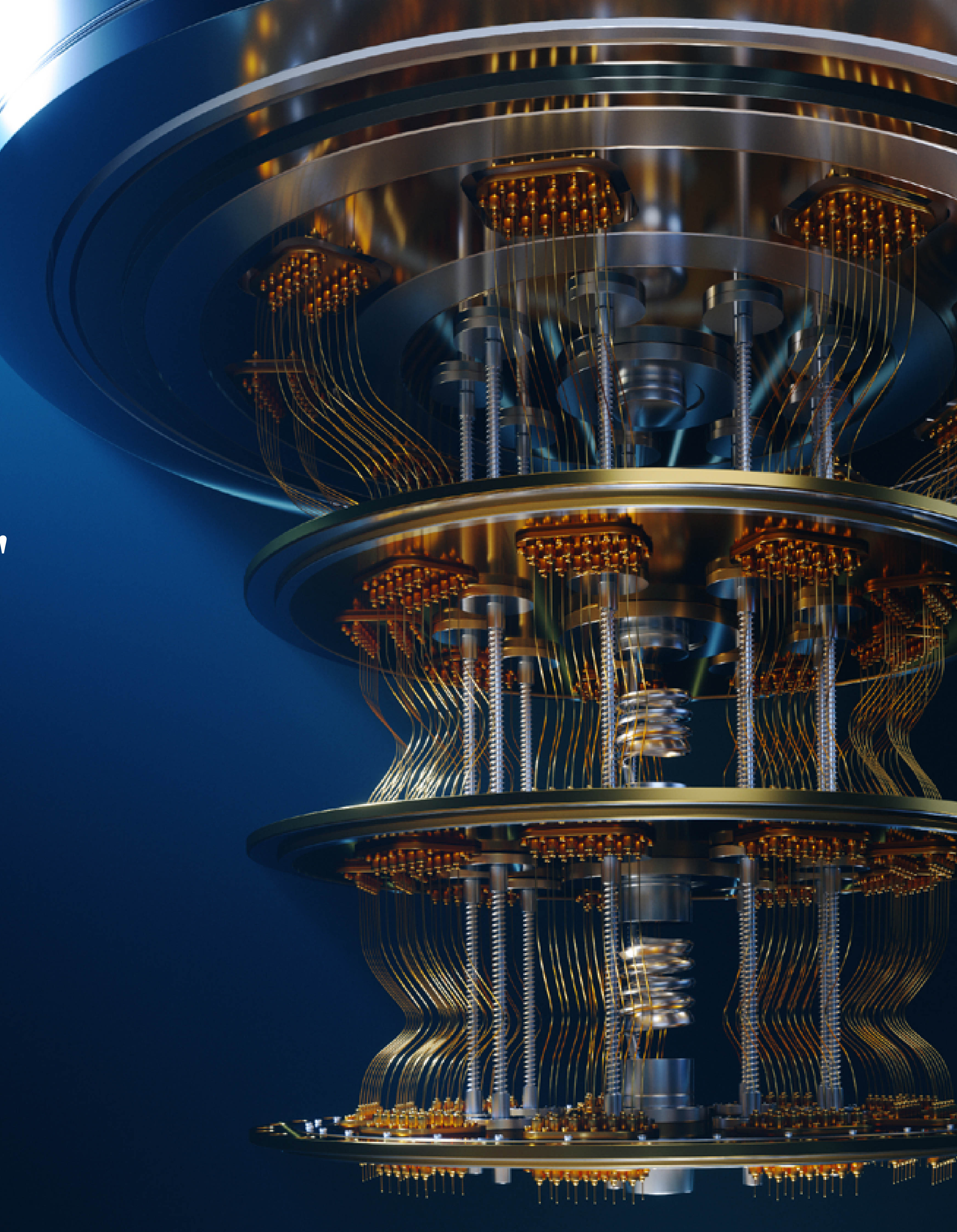
eleQtron aims to offer internationally competitive quantum processing units (QPUs) with high computing power using the promising MAGIC technology. The "MAgnetic Gradient-Induced Coupling" or MAGIC concept, allows the control of qubits using radio frequency technology, instead of lasers achieving record-low crosstalk between adjacent qubits. This unique approach simplifies the required scaling of TIQC hardware towards higher Qubit numbers and complements other scaling strategies. The partners will also investigate a novel, microstructured 3-dimensional ion memory, paving the way for a modular and versatile QPU architecture.

During the development phase, Infineon will provide eleQtron with three progressively improved generations of ion traps, as well as the necessary expertise to adapt them to the MAGIC concept. By employing a co-design strategy, Infineon will enable eleQtron to build ion trap-based quantum computers with successively increasing functionality. These potent quantum computers will later also be made available to industrial and scientific users via cloud access. ☒

"Beware the QUANTUM REVOLUTION! Quantum Computers *Pose Grave Risk* to Digital ID SECURITY."

By Robert Bach, Infineon Technologies

There are rapid developments in the field of quantum computers. The conventional cryptography deployed in current electronic ID documents and smart cards will be affected by the cryptanalysis performed on a future universal quantum computer. Post-quantum cryptography is intended to repel this cryptanalysis, but standardization and market introduction will take many years. Documents, infrastructure including background systems need to be upgraded, but long transition periods are expected. Start the preparation right now!



Unlike conventional computers, quantum computers use quantum mechanical effects for computation. Such a computer uses “qubits” that can exist in what is known as a superposition. Instead of being either 0 or 1 as is the case with conventional devices, they can be in both states simultaneously. Consequently, certain calculations can be performed simultaneously and far faster than ever before. Quantum computers are able to solve problems, which would require computing power that cannot be achieved with conventional systems.

For example, a quantum computer is not optimized to multiply long integers - a multiplication of large numbers is best done on a classical computer. However, with respect to the "prime factorization of long integers” the basis for cryptanalysis - quantum computers are ultra-fast compared to a “classical” computer.

In addition, the computing power they deliver is rising rapidly - year over year. These rapid developments are mainly driven by a multitude of tech companies (including IBM, Google, Microsoft and Amazon) investing in quantum computing.

With operations that are thousands of times faster, quantum computers offer new possibilities, for instance, in searching through large databases, simulation of chemical and physical reactions, and in material design. Although quantum computers will not completely replace classical computers, they can exponentially speed up certain arithmetic calculations.

Quantum computers affect conventional cryptography

Due to their computing method, quantum computers have the disruptive potential to break various encryption algorithms currently used. It is commonly assumed, that quantum computer attacks on today’s cryptography are expected to become reality within the next 10 to 20 years.

The availability of such a "universal quantum computer" will certainly have a game changing effect on the cryptographic security of identity documents like eID cards, especially as they often have a regular lifetime of 10 years and more.

The established and widely used encryption algorithms such as RSA (Rivest Shamir Adelman), ECC (Elliptic Curve Cryptography) deployed in those electronic ID documents and smart cards will be heavily affected by the cryptanalysis performed on such a future universal quantum computer. Equally, quantum computers have the potential to disruptively threaten algorithms like ECDSA (Elliptic Curve Digital Signature Algorithm) and protocols like ECDH (Elliptic Curve Diffie-Hellman).

Evidently not only electronic ID documents, but information and communication technology in general is affected. Various Internet standards like Transport Layer Security (TLS), S/MIME and PGP use cryptography based on RSA and ECC to protect data communications between smart cards, computers, servers, and industrial control systems. Secured communications on “https” sites and “instant messaging” encryption on mobile phones are well-known examples.

While the development of quantum computers is on the rise, there are still a couple of questions that remain unanswered, such as ‘when will a universal quantum computer be powerful enough to break the cryptography?’ and ’ What actual size will this quantum computer have? Will it be a small rack? Has it the size of a large building?’

Today's quantum computers do not provide sufficient calculation power yet, but there are rapid developments and improvements ongoing. Even if the size of a large building is needed – computing time on a quantum computer can be simply rented remotely.

Post-quantum cryptography

Post-quantum cryptography (PQC) aims to repel the cryptanalysis performed on both a quantum computer and a classical computer. Post-quantum cryptography refers to the new cryptographic algorithms (usually public-key algorithms) that have the potential to offer efficient protection against attacks using a quantum or conventional computer. PQC schemes are executed on conventional computers and security controllers and do not need a quantum computer to work.

From the user’s point of view, they behave in a similar way to currently available ciphers (e.g. RSA or ECC). This makes PQC an ideal drop-in replacement offering added robustness against quantum attacks. To afford protection against attacks that currently threaten RSA and ECC, PQC schemes rely on new and fundamentally different mathematical foundations. This leads to new challenges when implementing PQC on small chips with limited storage space.

In 2017, the US National Institute of Standards and Technology (NIST) started its post-quantum crypto project and asked for submissions of post-quantum key exchange, public-key encryption, and signature schemes to a competition-like standardization effort. It is expected that NIST will standardize PQC algorithms in 2024 and that several algorithms will be introduced.

Infineon is pioneering in post-quantum cryptography

Infineon is actively participating in the development and standardization process in order to enable a smooth transition and to address security challenges that may arise in the advent of quantum computers. Infineon’s contributions span case studies, demonstrators, whitepapers and two submissions to the NIST PQC standardization process. Infineon security experts are members of the teams that submitted the stateless hash-based signature scheme SPHINCS+ and the NewHope key-exchange protocol. SPHINCS is currently a Round 3 alternate scheme due to its strong security performance. Although NewHope was not selected by NIST for inclusion into Round 3 of the standardization process, novel techniques introduced by NewHope have been adopted by other schemes.

ROBERT BACH *comes along with a vast experience in the semiconductor industry for chip card IC´s. After finishing his university studies with a degree in industrial engineering and management at the technical university of Darmstadt, Germany he joined the Chip Card & Security IC group of Siemens AG, Germany in 1996. Mr. Bach has held various marketing and strategic marketing positions at Siemens and subsequently at Infineon Technologies AG. Currently, he is responsible for the semiconductor product marketing in the Product Line "Identity Solutions" within the Connected Secure Systems (CSS) division at Infineon.*

Standardization and adoption is needed

The selection and standardization of the first post quantum algorithms will be just the starting point. Besides NIST, other standardization bodies like, for example, the European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO) are also focusing on PQC and are now running study groups. In addition, the standardization work needs to continue finally integrating PQC into all relevant Government ID standards.

Ultimately, the adoption of infrastructure is required. Communication protocols need to be adapted and standardized. Documents and infrastructure, including the background systems, need to be upgraded.

Long transition periods are expected, moving from using conventional cryptographic protocols to the use of “hybrid” protocols, combining conventional cryptography and PQC to an ultimate migration to “PQC-only” protocols.

Approaches towards post-quantum cryptography

There are several approaches towards a quantum computer world. The most obvious option - at least in the short-term - might be ignoring or to start using PQC only once the universal quantum computer is available. However, at a certain point of time in the future, already issued documents might be compromised - as they might be in the field for an additional ten years. Worst case, these issued documents need to be withdrawn and exchanged - a procedure generating significant challenges and costs.

So simply ignoring the quantum computer threat is probably not a valid option.

Of course, the validity period reduction of electronic ID-documents might be a suitable way to go. It is therefore often discussed, to mitigate the potential threat by quantum computers. The shorter the document lifetime, the better the risk position and the less likely a document exchange will be needed at a later stage. For certain use cases, the documents are valid for only a manageable period, i.e. classical payment cards, which are mostly valid for three years only. However, dealing with the extended identity document lifetime of ten years or even more, things become disproportionately complex.

Moreover, reducing the validity period of a governmental document is difficult to be implemented. For some use cases (i.e. signature cards / tokens), it might be easy. For other governmental documents it’s probably not a realistic option.

In the preparation for a migration towards post-quantum cryptography, mitigation needs to be done with a variety of smaller actions - and early preparation is key, as the final implementation will take several years.

Migration strategies towards post-quantum cryptography

Neither the standardization of the PQC-algorithms, nor the standardization of the additional required ID protocols is finished yet, and the finalization will still take some time.

Currently, a possible migration strategy towards PQC is crypto agility. The transition from today’s conventional algorithms to PQC will be gradual. The speed of migration depends not only on the availability of quantum computers, but also on the extent to which security is critical for the applications in question, the lifetime of devices in the field, and many other factors. Additionally, the set of PQC algorithms will change over time, reflecting the latest research insights. How can device vendors navigate all of these uncertainties?

The path to success lies in crypto agility; in other words, enable that devices can evolve to support different crypto algorithms. Looking ahead, adaptability in this dynamic space hinges on the ability to add and exchange crypto algorithms and the corresponding protocols.

Crypto agility @ Infineon

The underlying software update mechanisms must be properly safeguarded for crypto agility to work. Infineon has taken a first step towards providing the necessary safeguards by implementing future-proof, quantum-resistant software update mechanisms on its widely used Trust Platform Module (TPM): OPTIGA™ TPM SLB 9672 .

However, crypto agility needs to be backed by high-performing hardware. Post-quantum cryptography requires significantly more computational power in a security controller. The prevailing majority of today's security controllers are not able to run PQC-algorithms in a "sufficiently fast" transaction speed. While using an ID card for border crossing, citizens are not expected to tolerate an additional time penalty of 30 or even 60 seconds just because PQC is executed. Prior to relying on crypto-agility and field upgrade mechanisms, the underlying solution (chip hardware, Operating system, applets...) needs to be well chosen. Appropriate hardware resources help to maintain adequate transaction performance.

There is also a second challenge: post-quantum cryptography does not only need to be quantum-secured and resistant against attacks with classical computers, but the implementation itself needs to be secured against the classical manipulating, observing and semi-invasive attacks. It is expected, that both secured implementations and certification of PQC-implementations will require learning cycles. Appropriate Hardware resources can support secured implementations.

A good way to start learning, is working on demonstrators and preparing a timely start with first - although limited - field trials. First pilot projects for national eID cards are expected to start soon after 2025. A wide scale rollout of quantum-safe documents is expected to start before the end of this decade.

Important for learning: PQC-demonstrators - i.e. a quantum-secured EAC Passport

In 2022, the German Federal Printing Office (Bundesdruckerei GmbH), the Fraunhofer Institute for Applied and Integrated Security and Infineon demonstrated for the first time a quantum computer-resistant version of the Extended Access Control (EAC) protocol for an ePassport with the objective to showcase the feasibility of a quantum-secured ePassport.

Recommendation: Early preparation is key

Although the first standardized algorithms are expected in 2024, with continued standardization afterwards - the rapid development of quantum computing signals the inevitability of this trend and the importance of early preparation. Knowledge and expertise will be essential to put appropriate and commercially feasible solutions in place in timely manner. Any future migration to new products and technologies, whether it's cryptography or new products, or whatever, will always need considerable time and effort.

Government should begin by

- Learning and collecting the information,
- Making an inventory of which physical equipment and software will need to be upgraded,
- Preparing for the migration in (governmental) projects and start making strategic game plans (How to migrate infrastructure, how to upgrade documents),
- Making plans for first pilot projects (when to start, etc),
- Making infrastructure upgrade plans,
- Analysing the conditions in a project (which PKI is used, how the personalization is done, which cryptographic protocols are used and how, etc).

Moving to post-quantum cryptography affects the whole lifecycle of a document - industrialization, personalization, issuance, operational usage and field updates. ☒

Post-Quantum *CRYPTOGRAPHY on eID Documents*

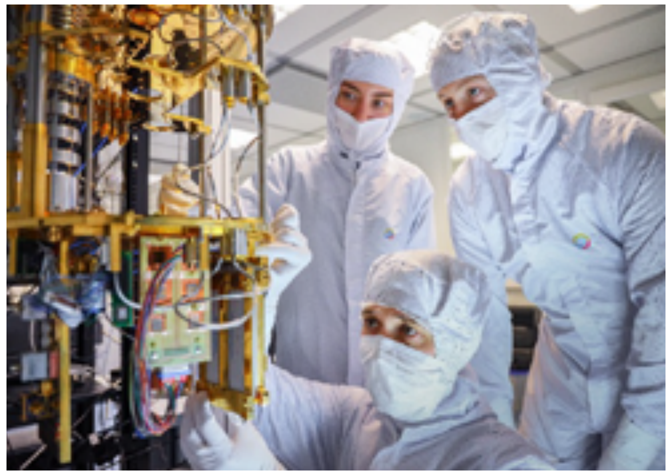
By Vasco Gomes and Klaus Schmeh, Eviden (an atos business)

CRYSTALS-Kyber and CRYSTALS-Dilithium are expected to be the major post-quantum crypto algorithms for the decades to come. Since the two crypto algorithms were declared winners of the multi-year U.S. NIST (National Institute of Standards and Technology) competition in 2022, producers of smart-card chips are evaluating and preparing to implement them. This process is far from being a no-brainer, as CRYSTALS-Kyber and CRYSTALS-Dilithium require more memory, are based on different mathematics and are in some cases slower than the currently used schemes.

KLAUS SCHMEH *is Chief Editor Marketing at Eviden (an atos business). He has published 16 books, 300 articles, 1,500 blog posts and 25 research papers about encryption technology, which makes him the most-published cryptology author in the world. Klaus is a frequent speaker, often using self-drawn cartoons, animations and Lego models for visualization. He has hosted presentations at more than 200 conferences in Europe, Asia and the U.S..*

Post-quantum cryptography

Quantum-computer-technology is still in its infancy, but one day it might be able to break RSA, Diffie-Hellman, ECC and other crypto systems. As these methods are used extensively on many IT platforms, including smart cards, a worldwide security disaster threatens. Thankfully, after years of research, several high-quality quantum-proof alternatives are now available, with CRYSTALS-Kyber and CRYSTALS-Dilithium, winners of a competition held by the U.S. authority NIST, being the most important ones. It can be expected that these two algorithms will become worldwide standards in post-quantum cryptography.



Quantum computers are still in an experimental stage. One day they might be able to break RSA, Diffie-Hellman and other crypto systems.

CRYSTALS-Kyber is an asymmetric encryption algorithm, which can be used in a similar way as RSA encryption. Its main purpose is to exchange a key that is used for a symmetric crypto system, such as AES. CRYSTALS-Dilithium is a method for creating digital signatures, which may serve as a replacement for the RSA signature-generation algorithm. CRYSTALS-Kyber and CRYSTALS-Dilithium are based on high-dimensional lattices, which means that their mathematical foundations are completely different from the ones of RSA.

Performance is an issue

It is difficult to compare the performance of RSA and CRYSTALS-Kyber/Dilithium, especially on platforms with limited resources. Tests performed by Eviden (an atos business) on a Pico Microcontroller show that, as a general rule, encryption with CRYSTALS-Kyber is faster than with RSA, while decryption is slower. CRYSTALS-DILITHIUM signs faster than RSA, while verification is slower. Signature generation and decryption are the more critical processes, as in many application scenarios they are executed on a chip, while signature verification and encryption take place on a more powerful platform such as a PC.

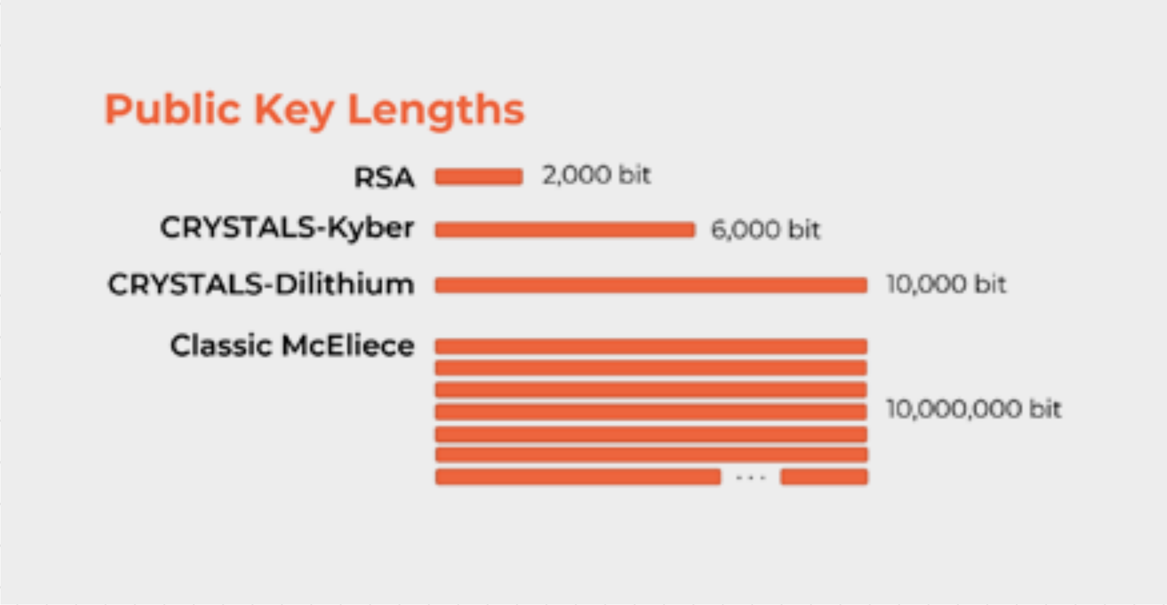


Figure 1: CRYSTALS-Kyber and CRYSTALS-Dilithium require considerably longer keys than RSA. Other post-quantum systems, such as Classic McEliece, come with even greater key lengths, which is unacceptable for smart cards.

__Vasco Gomes__ is Global CTO CyberSecurity Products & Digital Security Offering Technology Lead at Eviden (an atos business). Coming from an Information Technology engineering background, with 22 years of experience in information security, Vasco has helped many customers balance operational constraints versus acceptable business risks. In the recent years he has expanded this experience to help customers look into what the information security landscape might be in the next five years+ and the best way to manage it.

Things are even more complex when it is taken into account that there are many ways to optimize an asymmetric crypto algorithm. So far, implementing RSA in a performant way is much better understood than with CRYSTALS-Kyber and CRYSTALS-Dilithium. While many smart-card chips are equipped with an RSA co-processor, CRYSTALS co-processors are still as good as non-existent.

In addition, CRYSTALS-Kyber and CRYSTALS-Dilithium require considerably more memory than RSA. One obvious reason for this, is that the two CRYSTALS methods need longer keys to achieve appropriate security levels. Figure 1 gives an overview. Some other post-quantum schemes (such as Classic McEliece, which is mentioned in the figure, too) have an even greater key length – sometimes by orders of magnitude. It can be expected that algorithms of this kind will not be applied on smart cards.

Not only do the keys of CRYSTALS-Kyber and CRYSTALS-Dilithium require more memory than their RSA counterparts, but also the data structures that are necessary for the computations. The less memory is available for this purpose, the slower the computation gets. “On current mainstream smart-card architectures, which provide about 16 KiB RAM and 500 KiB flash, it is not feasible to implement CRYSTALS-Kyber and CRYSTALS-Dilithium in an efficient way” says Eviden Expert Arash Safajoo. “For the next generation of smartcards, with 96 KiB RAM, protype implementations already exist.” Contrary to RSA, the signature and the encryption procedures of KYBER are not identical, which leads to additional memory requirements when both are applied on the same chip.

It is clear that the implementation of CRYSTALS-Kyber and CRYSTALS-Dilithium on smart cards and other platforms with restricted resources requires further research. Eviden is currently engaged in projects of this kind. Among other things, specialists of the company are working on performant implementations of CRYSTALS-Kyber and CRYSTALS-Dilithium on Eviden’s CardOS operating system.

Based on announcements by the NSA, the German federal IT security office BSI and other authorities, it can be expected that the use of post-quantum algorithms will be required by law in some areas within the next ten years. This development might also affect electronic identity cards and other smart card applications. Says Arash Safajoo: “Mastering the challenges posed by CRYSTALS-Kyber and CRYSTALS-Dilithium will therefore be a crucial task for the near future. ☒

> *“On current mainstream smart-card architectures, which provide about 16 KiB RAM and 500 KiB flash, it is not feasible to implement CRYSTALS-Kyber and CRYSTALS-Dilithium in an efficient way.*
>
> *– Arash Safajoo, Eviden (an atos business)*

OBFUSCATION vs *ENCRYPTION*: Friends or *Foes*?

Dr. Carmen Kempka & Maurice Heumann, Wibu-Systems AG

So how do you protect information? A cryptologist would say: Nothing offers better protection than provably secure, well-studied methods based on sound assumptions. Kerckhoffs' principle states that security must never rely on the protection method itself being secret. A cryptosystem should be secure even if all information about it – except for a secret key – is known to the public. In contrast, software protection usually relies on obfuscating source code or executable programs as a defense mechanism against reverse engineering, an approach often dismissed as "security by obscurity". But is it always that simple? And how bad can it be in practice?

We will examine software protection, and especially obfuscation, from both a cryptologist's and a software protector's point of view, thereby connecting the two worlds. This will put theoretical results about the effectiveness and limitations of obfuscation to the test of real-life experiences and attack vectors.

Part I: The Cryptologist’s view

On the necessity of obfuscation

Given that well-established encryption methods like AES exist, why do we even bother with obfuscation in the first place?

Of course, executable programs can be protected by the accepted encryption methods. You can even have a more fine-grained protection by encrypting methods separately and decrypting only the parts you need at runtime. But the problem is, at some point, the CPU needs to get executable commands to actually fulfill the program's intended purpose. And points on an elliptic curve or elements of a cyclic algebraic group have the bad habit of not being executable on current hardware. So the curtain has to drop eventually, and a would-be attacker can seize on the plaintext executable statements for analysis. Cryptography cannot help here. At this point, the only line of defense to keep the adversary from trying reverse engineering is obfuscation.

What is obfuscation?

But what is obfuscation? Barak et.al. provided a simple definition they call the “Virtual Black Box Obfuscation” (VBB), which characterizes ideal obfuscation with the three following rules:

- The obfuscated program should not be significantly larger than the original
- The obfuscated program should have the same functionality as the original
- The obfuscated program reveals no more information to the adversary than a black box would

Ideally, the obfuscated program should do the same as the original would, without too much overhead impacting performance or the program size, while all the adversary learns from the obfuscated program is input-output behavior, which they could learn anyway by simply executing the program.

Obfuscation is impossible!

Unfortunately, in the same paper, Barak et.al. proved that it is impossible to design an obfuscator that meets this definition. But is this final proof that obfuscation is, in fact, bound to be no more than the frowned-upon “security by obscurity”?

The intention was never to disprove the purpose of obfuscation, but to explore the limits and possibilities of this, until then, oft-ignored complementary concept to cryptography.

Let us take a closer look at the actual paper’s findings. What it really says is that there is no general obfuscator that can obfuscate every existing program in the VBB sense. This does not mean that “no program can be obfuscated”. It rather means that “there is one program that cannot be obfuscated”. Or, as stated in the paper: “As is usually the case with impossibility results and lower bounds, we show that obfuscators (in the “virtual black box” sense) do not exist by supplying a somewhat contrived counterexample...".

In fact, there are functions (so-called “point functions”) that are obfuscatable in the VBB sense, for example a password check.

But even for other functions, all hope is not lost. An alternative definition called “indistinguishability obfuscation” has been proposed to overcome the impossibility of VBB, and it has been proved achievable with several candidates for obfuscators already constructed. While this was an important step towards closing the gap between theory and practice, these constructions are still quite far from being practical. Running an AES encryption with one of these constructions would, for example, take not less than 272 years and consume several petabytes of storage.

What can we learn from cryptography?

Given that we have all the experience from designing encryption algorithms at hand, how can we use it to close the gap?

Encryption algorithms are usually based on hard mathematical problems, like the problem of factoring large numbers used for RSA or the discrete logarithm problem used in elliptic curve cryptography. To use a similar approach for obfuscation, we need to overcome several obstacles. The result of obfuscation is, for example, usually supposed to be executable on a CPU as it is, while ciphertext has to be decrypted before reading. So we need to find a hard problem for transforming executable code into obfuscated, but executable code that keeps the same functionality.

The good news is that there are actually NP-hard problems that can be and are used for obfuscation. One of these is the SAT problem. In the obfuscation world, this usually comes as opaque predicates or the problem of dead code elimination: the adversary is deceived by a lot of if statements, and needs to decide which of these always evaluate to "false" and are thus never executed. Another example is using different pointers, called aliases, to access the same value.

Unfortunately, these NP problems are difficult only in the worst (or for us, best) case. A randomly chosen instance of the SAT problem, for example, can usually be efficiently solved with a logic solver.

For encryption algorithms like RSA, we have learned how to choose good key pairs, i.e., instances of the underlying problem which are actually difficult for our adversary to solve. For obfuscation, this is still an open problem, and many of the commonly used obfuscation techniques can, if considered one by one, eventually be cracked by attackers. In addition, understanding the complete program might not even be the goal of our adversary, as they might just want to eliminate a license check.

How far are we from what we actually need?

Encryption algorithms are usually designed in a way that the adversary would need millions of years or more to solve the underlying problem, and that there is a significantly low probability of correctly guessing a secret key. In software protection, depending on the use case, we might just want to keep our adversary from cracking anything until a new version of the software is published, or until the bulk of our prospective income has been made with the protected software.

But even if currently known obfuscation techniques don't (provably) achieve the same level of protection as encryption methods, and even if single protection techniques can be broken, the attacker is not necessarily able to crack our software. Multiple obfuscation and integrity protection techniques can be used to protect each other, achieving a very strong level of protection as long as, for each attack technique, there is a protection technique which prevents that attack. This opens the same kind of cat-and-mouse game between attackers and protection that we already know from cryptography, and that we invite you to experience in the rest of this article.

DR. CARMEN KEMPKA *studied computer science at the University of Karlsruhe (TH) with a focus on cryptography and quantum computing. After completing her PhD in 2014, she joined the Secure Platform Laboratories of NTT in Japan for two years of postdoctoral research in cryptography. She moved to WIBU-SYSTEMS AG in 2016, where she is now responsible for R&D projects and supports her colleagues with all questions about cryptography and security.*

Part II:
The Protector's view

MAURICE HEUMANN studied computer science at the Baden-Wuerttemberg State University. He began programming at the age of nine and started working with reverse engineering at 14. Since 2019, he has been working as a protection engineer at WIBU-SYSTEMS AG, where he develops and improves software protection solutions. In his spare time, he reports software vulnerabilities to renowned game manufacturers.

Where does the attacker start?

In contrast to the theory, real-life attackers often begin their analysis by examining programs in a disassembler. To counteract this, software can be packed, using compression or encryption, and then unpacked during runtime. However, as previously mentioned, it is important to note that the application code will eventually need to be decrypted for execution. This creates a window of opportunity for attackers to inspect and dump the memory contents after decryption, allowing them to analyze the code and carry out runtime patches, which is called binary hooking. Without employing obfuscation techniques, it is not possible to prevent attackers from analyzing program semantics.

What does obfuscation look like in practice?

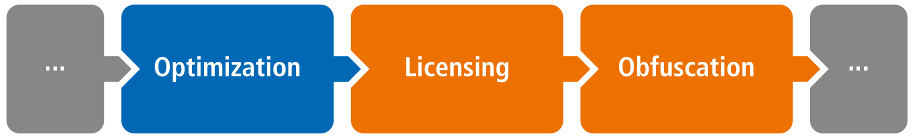
For greater security, attackers should be prevented from actually comprehending the underlying code. One should not rely merely on obstructing their analysis. Simple obfuscation techniques can be employed to help us some way towards this objective. These techniques involve injecting redundant instructions or substituting instruction sequences with more complex forms. By employing such obfuscation methods, it gets harder for attackers to understand the code, providing an additional layer of protection for the program.

Program simplification While simple obfuscation techniques provide some initial barriers, they are rarely sufficient to impede determined attackers from comprehending the program logic in the long term. Attackers can utilize program simplification methods to streamline obfuscated code. This involves lifting the obfuscated code into an abstract language known as intermediate representation (IR). The IR can be subjected to various optimization techniques commonly employed in compiler frameworks, resulting in a simplified form of the program. This optimized representation can be either translated back to assembly code or visualized through decompilation, making it more accessible for attackers to analyze and understand it.

Control flow disguising To address the limitations of program simplification and the performance impact caused by inserting redundant code, control flow disguising techniques offer a viable solution. Instead of substituting instruction sequences with complex forms, dead code is introduced into the program. This dead code can appear arbitrary or resemble the original code. The connection between the dead code and the original program is established through the use of opaque predicates. These opaque predicates take the form of conditional statements whose evaluations consistently yield a fixed result (either true or false). With that, the dead code is never executed, and the performance impact is minimized, with the exception of the opaque predicates themselves.

SMT-assisted minimization To overcome the challenge posed by opaque predicates, attackers can employ SMT-assisted minimization techniques. SMT, short for Satisfiability Modulo Theories, generalizes the boolean satisfiability problem (SAT). By utilizing symbolic execution, attackers can transform

	Patching	Memory Dumping	Hooking	Program Simplification	SMT Minimization	Debugging
Packing	🛡	⚔	⚔			
Simple Obfuscation		🛡		⚔		
CF Disguising				🛡	⚔	
CF Indirection					🛡	⚔
Anti Debugging						🛡
Integrity Checks	🛡		🛡			🛡



What about dynamic analysis?

While the mentioned obfuscation techniques effectively hinder static analysis, dynamic analysis remains a viable avenue for attackers. For instance, reconstructing the program's control flow by debugging it is still possible. As the code must maintain semantic equivalence and all relevant code blocks must eventually be executed, attackers can utilize a debugger to step through the program's execution and reconstruct the control flow. By observing the program's behavior during runtime, attackers can gain insights into its control flow and understand the underlying logic.

To counteract the presence of debuggers at runtime, various anti-debugging techniques have been developed. However, many of these techniques are widely known and considered ineffective, as tools exist that can automatically bypass or disable such anti-debugging measures.

A more robust approach involves the use of integrity checks to protect against code manipulations. By computing a checksum of the code at runtime, programs can verify that their code has not been altered. In the event of a mismatch, appropriate actions can be taken to prevent further execution.

Integrity checks are highly effective in combating patching and hooking techniques, as any modifications to the code are automatically detected. Furthermore, these checks also provide protection against debugging attempts. Debuggers typically insert breakpoint instructions to pause program execution. These instructions are detected by the integrity checks, thereby preventing successful debugging.

How can obfuscation be implemented?

Finding the right defense techniques against attackers is an important task. However, without the ability to incorporate these techniques into software programs, their potential remains dormant.

Leveraging compiler frameworks offers a practical solution to that. Compiler frameworks, such as LLVM, offer the ability to parse, optimize, and lower code for specific architectures. By intervening in the optimization, additional obfuscation and protection techniques can be seamlessly inserted into the code.

Wibu-Systems offers AxProtector CTP, a powerful product that leverages the LLVM compiler framework to achieve efficient obfuscation goals. With AxProtector CTP, a wide range of defense techniques, including those mentioned earlier, can be seamlessly integrated to enhance the security of various applications. Additionally, it provides flexible licensing features supported by trusted cryptographic algorithms. The synergy between licensing, encryption, and obfuscation ensures optimal protection for applications.

Thanks to the versatility of LLVM, AxProtector CTP supports multiple operating systems, architectures, platforms, and programming languages. Compared to other established protection techniques, AxProtector CTP offers non-invasive application security. It adheres to code integrity requirements, such as those enforced by Apple, on Apple silicon machines. This ensures that applications remain secure while maintaining compliance with platform-specific guidelines, even without the need for runtime code modification. ☒

SILICON TRUST DIRECTORY 2023

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

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

AUTHENTON

authenton (a EU + CH + UK registered Trademark and authenton GmbH) is a new (2022) Sales & Marketing arm of AIXecutive, which was founded in 2012. AIXecutive's management and its technology-partners have been an integral part of the global Smart Card industry since the mid 1990s. Since 2012 AIXecutive provides and supports global players with customer specific developments.
The company helps to manage high security Identification & Authentication solutions for Government eID, Mobile-, Payment-, and high secure IoT (IoT SAFE) as well as security certified Web-Authentication solutions (incl. FIDO2.1). The authenton#1 Token is a result of AIXecutive & its technology partners' latest security certified developments for Government eID and Mobile Security. Munich based authenton GmbH represents all Marketing & Sales-activities for the registered authenton brand, its first product -the authenton#1 FIDO2.1 Token – as well as subsequent products.
www.authenton.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

CARDLAB

CardLab is a world leading data and privacy protection and Cyber security company by use of its biometric card technology provided to the powered smart card industry having developed and commercialized ISO 7810 compliant secure card products including:

- Full "System on Card" biometric authentication solution based on Fingerprints™ FPC1300 T-shape™ touch sensor", for payment, ID, Access control, blockchain and Cyber Security.
- Communication controlled RFID cards (Jammer & MuteCards),
- "All In One" card solution platform and other card solutions customized to customer specifications for secure and sustainable card production.

CardLab is a Denmark based card development and manufacturing company with manufacturing partners in Asia and USA and own card lamination factory in Thailand. CardLab offers unparalleled technical design and manufacturing support for card solutions including scalable security levels and existing infrastructure compatibility making implementation cost affordable for end users.
www.cardlab.com

COGNITEC

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

EVIDEN

Eviden designs the scope composed of Atos' digital, cloud, big data and security business lines. It will be a global leader in data-driven, trusted and sustainable digital transformation. As a next generation digital business with worldwide leading positions in digital, cloud, data, advanced computing and security, it brings deep expertise for all industries in more than 53 countries. By uniting unique high-end technologies across the full digital continuum with 57,000 world-class talents, Eviden expands the possibilities of technologies for enterprises and public authorities, helping them to build their digital future. Eviden is an Atos Group business with an annual revenue of c. € 5 billion.
www.eviden.com

HBPC

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

HID GLOBAL

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

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.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.
www.mksmart.com

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.
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

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, secureproducts 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

THALES

Thales is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive. The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, Edge computing, 6G and cybersecurity. Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

www.thalesgroup.com

TRUSTSEC

TrustSec is a Polish information security company, founded by internationally recognized information security and cryptography experts. Through TrustSec's pool of experts and its business-driven innovative solutions, TrustSec offers its unique, in-house developed operating system for smart cards – SLCOS. The company also delivers a variety of products and solutions, that cover software protection, data encryption, OTP, and security hardware (namely PKI tokens and FIDO2 tokens). In addition to its latest fintech innovation CPA and its unique panel of professional services; of consultation, integration, testing, and outsourcing, to help the other companies benefit from the latest available advances in cryptography to improve their products and services.

www.trustsec.net

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

WIBU SYSTEMS

CodeMeter – A Symphony of Software Monetization Tools

- Compose your original code
- Orchestrate your license strategy
- Fine tune your IP protection
- Distribute your work of art

Sounds easy, right?
And it is with CodeMeter

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

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

SECURITY
LICENSING
PERFECTION IN PROTECTION