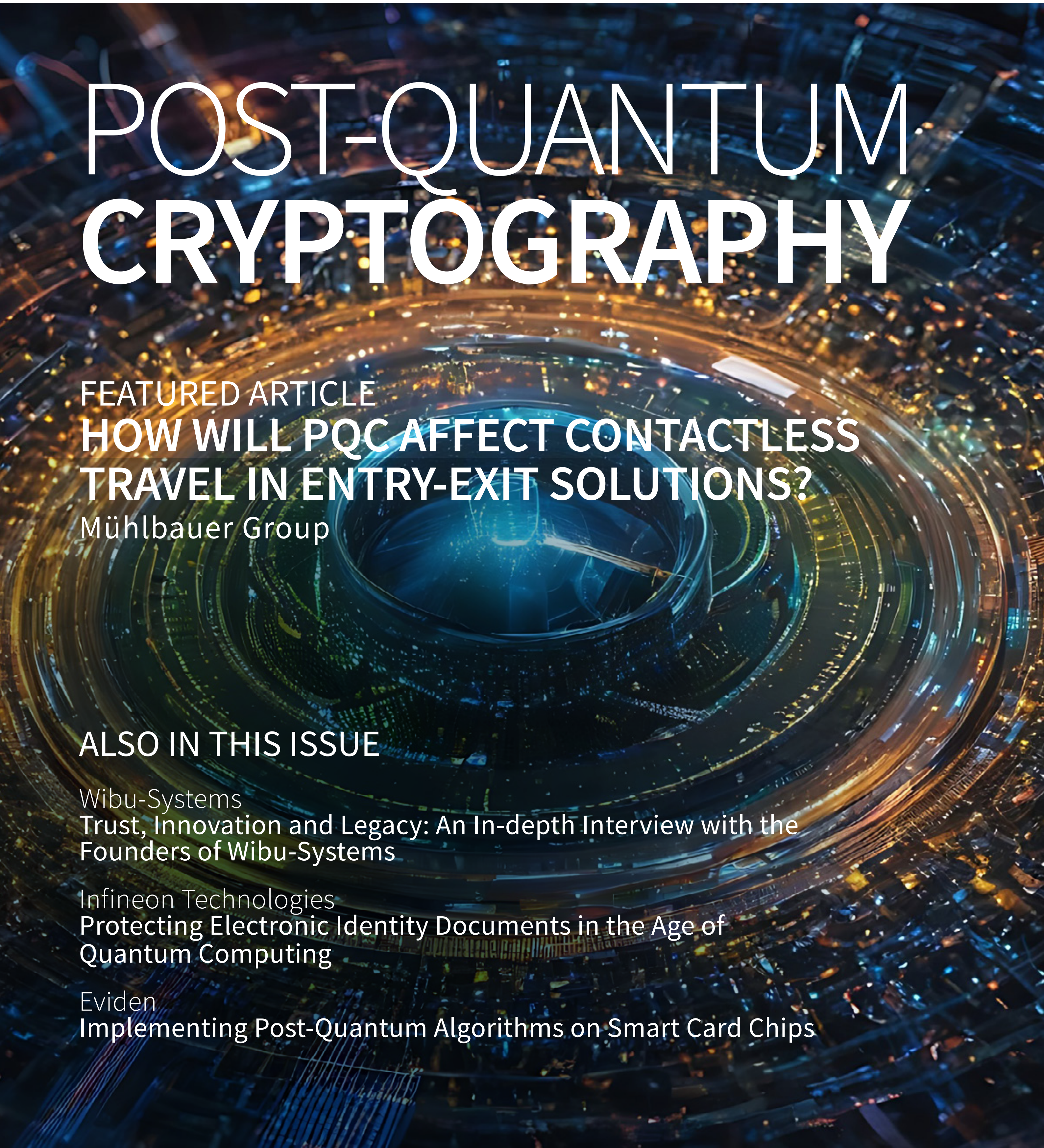
NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

JULY 2024

The VAULT



POST-QUANTUM CRYPTOGRAPHY

FEATURED ARTICLE

HOW WILL PQC AFFECT CONTACTLESS TRAVEL IN ENTRY-EXIT SOLUTIONS?

Mühlbauer Group

ALSO IN THIS ISSUE

Wibu-Systems
Trust, Innovation and Legacy: An In-depth Interview with the Founders of Wibu-Systems

Infineon Technologies
Protecting Electronic Identity Documents in the Age of Quantum Computing

Eviden
Implementing Post-Quantum Algorithms on Smart Card Chips

Contents

Protecting Electronic Identity Documents in the Age of Quantum Computing 4
Robert Bach, Infineon Technologies

How will Post-Quantum Cryptography Affect Contactless Travel in Entry-Exit Solutions? 12
Lutz Richter, Mühlbauer Group

Implementing Post-Quantum Algorithms on Smart Card Chips 19
Klaus Schmeh, Eviden (an atos business)

Trust, Innovation and Legacy;
An In-depth Interview with the Founders of Wibu-Systems 24
Daniela Previtali, WIBU-SYSTEMS AG

Silicon Trust Directory 2024 30

Imprint

THE VAULT ISSUE 40
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Nina Eggemann
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Steve Atkins, Daniela Previtali, Klaus Schmeh, Robert Bach, Lutz Richter
PHOTOS: ISTOCKPHOTO, INFINEON TECHNOLOGIES, WIBU-SYSTEMS, MÜHLBAUER, EVIDEN, FREEPIK AI IMAGE EDITOR, KROWNE COMMUNICATIONS
EDITION: JULY 2024. No portion of this publication may be reproduced in part or in whole without the express permission, in writing, of the publisher.

PROTECTING *Electronic Identity* Documents in the Age of QUANTUM COMPUTING

By Robert Bach, Infineon Technologies

Quantum computers use quantum mechanical effects for computation. They aim for breakthroughs in various areas such as artificial intelligence or chemical simulation, but they equally can be used to perform cryptanalysis. Once available with sufficient computing power, quantum computers can solve certain calculations much faster than today's computers.

In this article, Robert Bach summarizes the key facts of Post-Quantum Cryptography and describes the status of the work on quantum computers and standardization activities. The main part of the article focusses on the consequences for ID documents and ID projects. It was transcribed and edited for readability from an original presentation given by Robert Bach during the Silicon Trust webinar: ***Post-Quantum Cryptography and its Impact upon Identity.*** (April 10th 2024)

"

Dawn of a new era

This article will look at the protecting of electronic identity documents in the age of quantum computer. I will start with a very small introduction based on history, and then I will explain what a quantum computer is, before moving to post quantum cryptography, and then sharing some more insights on the requirements for field implementations for ID projects; but not just for ID projects, a lot of areas are being affected.

If you look at the past one hundred years, we have seen dramatically changes. From data storage, to the managed analysis of data, and now everything has moved to the cloud. In terms of communication, 20 or 30 years ago, we used a landline phone. Now we have mobile phones. Payment was in cash, and now everything has moved to electronics. And in terms of ID topics, signing contracts today can be done electronically as well – and on a worldwide basis. But what did we need to achieve all of this? The invention of the semiconductor.

Without semiconductors, it would not work. It took considerable time to really finish that because the first silicon transistor was there shortly after the Second World War, followed a little later by the first integrated circuits and then later the first non-volatile memories. Today we see a continuing technological evolution with artificial intelligence. However, when we look at quantum computers, the theory is quite old. Quantum mechanics has been around a while, with individuals such as Einstein, Schrödinger, Heisenberg having already worked on the principles. It took quite some time, almost a century, before the first quantum computer arrived. That was back in 1998, a complete quantum computer with two bits! What we see seen in the last five years, though, is a significant development in quantum computers.

What is a quantum computer?

A standard computer relies on binary bits, calculating a zero, a one, and that is a principle which is already quite known. On the other hand, a quantum computer relies on qubits, quantum bits, and based on physical principles, a one quantum bit can have the same status at the same time. It can be equally a zero or one, and only if you examine it and look for a result, it will become a zero or a one. These principles are called superposition and entanglement. You can use various qubits here which you can connect to each other. They can start with a superposition, meaning a lot of qubits can take over a variety of statuses, and only at the end, if you take a look, you will see the result. These principles are rather old.

Albert Einstein once said, “I don't understand everything, but basically it seems to work.” If you use these principles in a quantum computer, then you can do a lot of things because you can solve a couple of problems much better and way faster than using conventional computing power. One examples would be the healthcare industry, finding a medical medication, in chemistry, finding optimised products, and quantum computers are obviously good in prime factorization. In prime factorization, you have a large number, say, 851. It is not that large, but you can increase the size by the power of two prime factors. And now what is A, what is B? The classical computer takes quite some time to find out. When a powerful quantum computer is used, the answer will be there in a very short time. Once we have the universal quantum computer, the elliptic cryptography is affected; everything which is RSA encrypted (including elliptic curves), are relying on the difficulty of factorization.

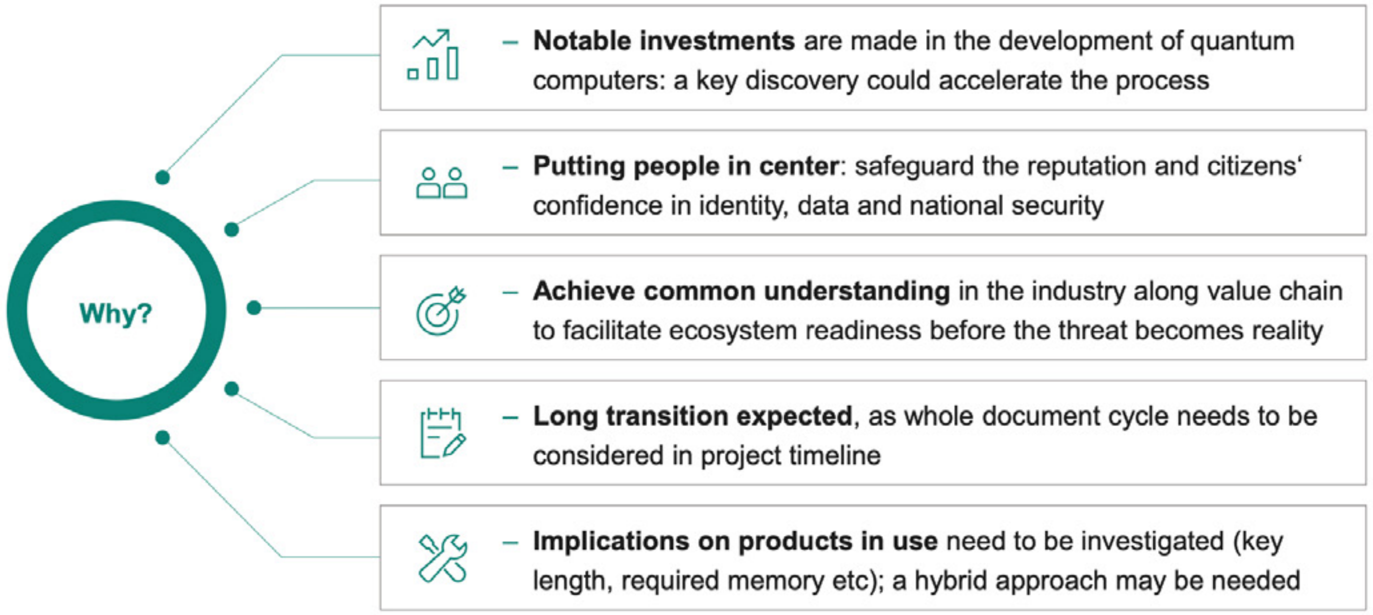
If you have a real large number, this factorization is, with today's computers, not really practical. No one has used a 1K RSA certificate for the past 10 years because classical computers might break this, given sufficient time. However, if you go up in the key lengths 2K, 3K, or 4K RSA, classical computers really have a problem. That is the situation today.

Then there was a person named Mr. Shor who invented, 30 years ago or so, a source algorithm before there was even a quantum computer. By solving this discrete algorithm problem, and in exploiting the full property of the algorithm using a quantum computer (when available) we will see that RSA, ECDSA, Elliptic Curve Diffie-Hellman will have almost no security. Whoever wants to attack these protocols will be ultra-fast. That is a concern because Elliptic Curve, Diffie-Hellman, RSA, Elliptic Curve, and DSA, are protocols which are used in the transaction of ID documents during border crossing. With this being the case, then all asymmetric cryptography on ID cards will be severely affected.

One of the major questions I always get, and I think this has been discussed in the industry for quite some time, is ‘When will be there a quantum computer which is powerful enough to really attack the documents in the field?’ The challenge to attack such documents is that one would need a high number of stable qubits, and very high, in this case, around 4,100 qubits, to be more or less able to attack a 2K RSA. Unfortunately, qubits, because they are relying on quantum mechanics, are quite unstable. Even a very tiny change in environmental conditions, (temperature, pressure, ...) makes them unstable causing qubits to lose their data – called Qubit Decoherence. If you have a qubit, that within a couple of milliseconds becomes unstable, you will have to use a lot of error correction if you really want to scale.

Today, many of the major technology companies in the world work on a quantum computer. IBM was first, in 2016 with a 5-qubit computer. Then one year later, IBM developed the 50-qubit computer followed in 2019 by Google with a 53-qubit computer. You can see the number of qubits is increasing. By 2022 IBM had a 433-qubits computer, and if you remember, I said you would need 4K to crack a 2K RSA. We are getting closer. IBM is predicting to release a 4,158-qubit computer by 2025 and a lot of press releases from smaller companies say 1,000,000-qubit computers will be available by 2030. A word of warning here, though. These are the number of physical bits, physical qubits. These are not the number of logical qubits, the stable qubit. You need roughly between 1,000 and 10,000 physical qubits to create one logical qubit. Bearing this in mind we can see that 4,000 physical qubits is not that big a number of qubits; You would not be able to create an attack on an RSA properly, but the technology is accelerating.

At the end of last year, a small team of developers (including the NIST), published a paper where they claimed that they had, based on a 288 physical qubit quantum computer, created forty-eight logical qubits. This is quite a development in that, despite still not being a productive quantum computer, they reduced the ratio between a physical qubit and a logical qubit to roughly a scale of 1 to 5. This is the so called ‘Red Flag’ that we should acknowledge. Everybody believes it will take some time for development of producing a working quantum computer, but if you have certain technical developments (like the one just mentioned), change and development can be quite fast.



- **Notable investments** are made in the development of quantum computers: a key discovery could accelerate the process
- **Putting people in center**: safeguard the reputation and citizens' confidence in identity, data and national security
- **Achieve common understanding** in the industry along value chain to facilitate ecosystem readiness before the threat becomes reality
- **Long transition expected**, as whole document cycle needs to be considered in project timeline
- **Implications on products in use** need to be investigated (key length, required memory etc); a hybrid approach may be needed

Figure 1:

Threats and Implications

What can we say are the potential threats and implications to governmental ID and digital services? The fundamental idea is to harvest now, even if you are a secret service, and then decrypt later once the quantum computer is there. Some of the excess data available for harvest have a long shelf life. If you store them now and try to encrypt them using older algorithms, then they are endangered.

With ID documents, it is not so much the case. This harvesting is more for military information and military communication systems. For ID documents, the vulnerability of asymmetric cryptography will affect roughly all communication protocols – especially digital signatures. If you sign a contract and afterwards a quantum computer can hack this digital signature, this is not good. Overall, the security of government application will be severely weakened. You may also see identity theft and the consequent misuse of such identities; for governments that is a bad thing to happen leading to a possible loss of credibility in the ID and ID documents and governmental services available.

Post-Quantum Cryptography

Post-Quantum Cryptography is the answer. If you use Post-Quantum Cryptography, once it is standardized, it should be safe. So postquantum cryptography is the cryptographic methods that should not be broken by either a quantum computer, or a standard computer. It needs to be safe against both a quantum and a conventional computer.

After the NIST competition, it was clear we needed a new cryptographic system which is secured. Secured PQC is desirable, but it should at least be affordable. You need a sufficient security. Infineon participated, in this competition as well and we are not just waiting for the result. There were three rounds with the final and first selection of the first candidates with four schemes in July 2022. The first draft standards coming from NIST were sent out to the people in August 2023 and NIST say the first final standards, are targeted for Summer 2024. That would be the FIPS 202, 203 and 204 standards.

We believe that CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA) are best suited for smart cards because a smart card has limited power, limited non-volatile memory, limited resources, and limited performance. You cannot put a supercomputer in the form of a smart card, so we need to use the algorithms which are best suited for smart cards. These being CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA).

Requirements for Field Implementation

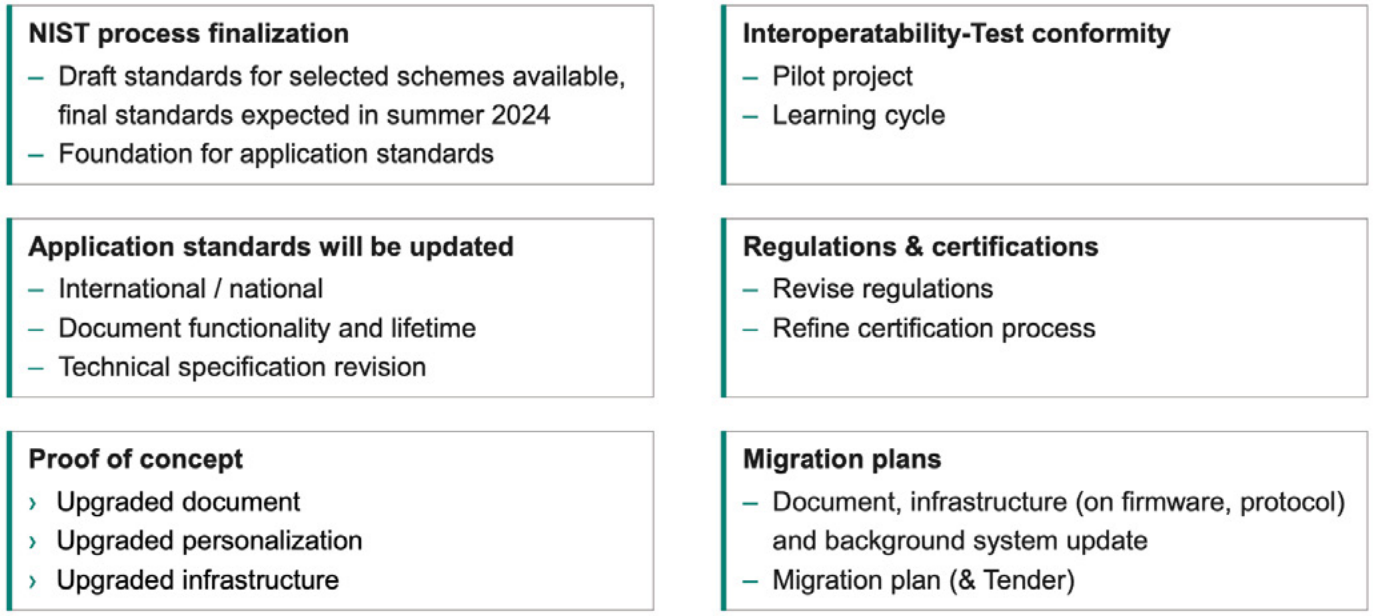
One would probably use a different type of cryptography on a mainframe than in the field because requirements for field implementation are very different. As stated earlier, nobody can really say when a powerful quantum computer will be available. But even without imminent security threats from quantum computers, immediate actions for risk mitigation are highly recommended. (See Figure 1)

All it would take is a key discovery from the more invested companies such as Amazon, Microsoft, IBM, Google, and similar types of technology companies that can make significant investments into the topic. And that's not even discounting governments and their secret services who also have an interest in any move towards a working quantum computer. A key discovery could really speed up the process. The biggest problem with ID documents is that they are out in the field for 10 years. Even if a working quantum computer arrives in the next five years; that is still a high risk because cryptanalysis will be possible with these computers.

For governments, it is extremely important that they safeguard the reputation and ensure that the citizen has confidence in identity documents, in the data and national security. For governments, they really need to act in time, not too late.

During our standardisation activities over the past few years, we have seen a need for a common understanding within the industry to completely to understand the value chain and to facilitate the ecosystem readiness before threats becomes reality e.g., a standardization of worldwide travel.

Based on Post-Quantum Cryptography, initial documents can already be rolled out before a working quantum computer exists. In all government projects, we expect extremely long transition projects because the whole document lifecycle needs to be examined and the infrastructure changes are quite complex. As we will need to look at the products, the infrastructure, key length and required memories, a hybrid approach might be needed for field updates. This would involve current cryptography as well as any new Post-Quantum Cryptography. NIST says we will have the final NIST standards available in Summer 2024. But this is just the foundation for the application standards, because with this document you can start programming but that does not help if you want to have a passport which is able to pass the infrastructure at the border. (See Figure 2)



NIST process finalization
- Draft standards for selected schemes available, final standards expected in summer 2024
- Foundation for application standards

Interoperatability-Test conformity
- Pilot project
- Learning cycle

Application standards will be updated
- International / national
- Document functionality and lifetime
- Technical specification revision

Regulations & certifications
- Revise regulations
- Refine certification process

Proof of concept
› Upgraded document
› Upgraded personalization
› Upgraded infrastructure

Migration plans
- Document, infrastructure (on firmware, protocol) and background system update
- Migration plan (& Tender)

Figure 2:

We need application standards as well, and that means ICAO signature standards. In Europe, we need EU regulations because once again taking an example of a passport, you want to your passport from your country to be accepted in another country as well, and you want to have electronic access to the country and not to be refused. It is not a national problem – it is an international problem. ICAO have already started with their Crypto Agility Working Group. A proof of concept is helpful because any changes in documents, any changes in personalization, any changes in infrastructure are rather complicated. And the sooner a pilot project can run, the better the learning cycles you have. Any new algorithms with RSA and elliptic curve, allow us to use 20 or 30 years of experience on the topic. The new post quantum cryptography algorithms are new. They need to be implemented in a secure way and they need to be certified. In this new process, we need to invest effort to really make it happen.

Summary

In terms of migration plans for any ID system, it is necessary to at least know what you are using currently in terms of cryptography. We recommend a cryptographic inventory, because you will have to change not only the documents, but your whole infrastructure, of software, protocols, and personalization systems. Consequently, a migration plan needs to be developed. Knowing that governmental projects take time, this process could take years. The development of quantum computer might be a lot faster.

We had the first quantum computer in 1998 with just two qubits, but is now really advancing in terms of technology; typical cryptography for ID documents will be really heavily affected. Post-Quantum Cryptography will help in that respect, but still requires standardization and market introduction – not only for the documents, but also infrastructure. This will take time. Considering these long transition periods, our recommendation to all governments and ID document stakeholders, is not to wait until the quantum computer is here, but to start preparation now because there will be a steep learning curve and we move from current-know cryptography and infrastructure towards one that utilizes Post-Quantum Cryptography.

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.*

How will POST-QUANTUM *CRYPTOGRAPHY* Affect *Contactless Travel* in ENTRY-EXIT SOLUTIONS?

By Lutz Richter – Mühlbauer

This article will look at the impact post quantum cryptography has on entry/exit systems, on the topic of seamless travel.

It was transcribed and edited for readability from an original presentation given by Lutz Richter during the Silicon Trust webinar: ***Post-Quantum Cryptography and its Impact upon Identity.*** (April 10th 2024)

The travel process today

Everyone is familiar with the way we travel today. We start with the registration of the traveler at a self-service kiosk. This is normally a passport, or in terms of ICAO, the eMRTD – where the document is read and, ensuring everything is correct according to the specification, the verification of the individual against this travel document takes place. Next, more or less seamlessly, you go to a gate that uses face recognition. The traveler is verified and can cross the border or go to the aircraft and make the boarding process (Figure 1). This is currently state-of-the-art, is established in different setups, and the trust element here is the travel document with the electronic chip and the digital information from a government authority. This is what we call the Trust Anchor.

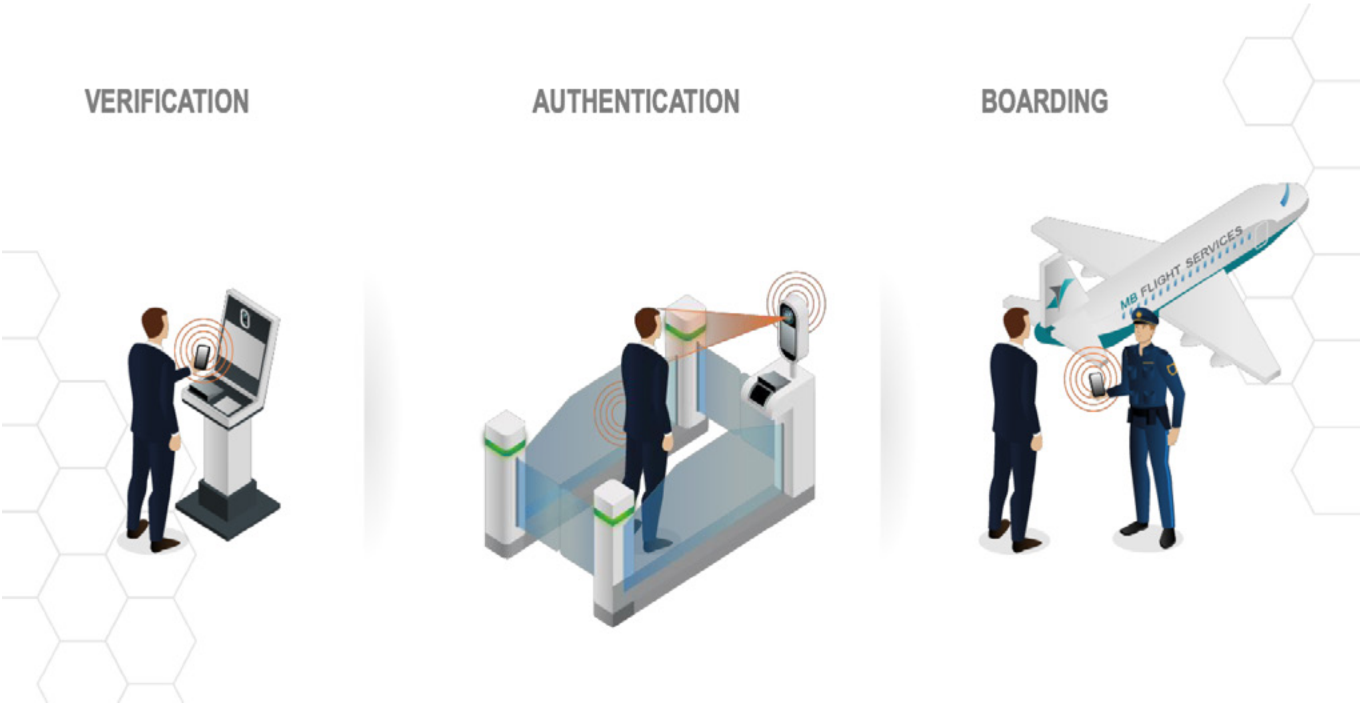


Figure 1 Verification, Authentication & Boarding

But what is behind the establishment of such a system and what do we have to consider as a solution consultant or as a technology partner in this market segment? The basis of this entire system are international standards.

Here, the three main player for international travelling documents is ICAO, which is obliged to standardize all data which is going to a machine-readable travel document such as a passport or ID card, including the chip. And ISO, in turn, concerns themselves with the detailed technical specification for the chip and the data processing. Now for Post Quantum Cryptography, the National Institute for Standardization and Technology in the US is engaged in qualifying the algorithm, with which Post Quantum Cryptography-proven solutions, and solution supplier, have to consider when building up a system or transferring this system to the next level.

What are the challenges?

The hot topic today is Post-Quantum Cryptography. But equally important is cybersecurity, because communication in today's digital world is also the science of secure digital encryption.

This is not only dependent upon architectural guidelines, but also an element of sustainability. When we travel in this digital world, we consume energy. And this energy element should be considered when upgrading such a system; how much energy must we consume while making this area secure? In short, it is a lot, and it's thanks to the Quantum Computer. This type of computer can be unbelievable fast in its' calculations. The Quantum Computer may still be in its' infancy but when it is finally here and established, all standard cryptography will become vulnerable and will be an issue for the unique identity of all citizens in the country and their related documents. More confusing is which sectors and their products will be affected and when?

Some industry observers claim that we will see significant developments and implementations for Quantum Computing in the next five to six years. The first sectors to be impacted are expected to be those such as the public sector, insurance and banking. These are the areas we at Mühlbauer are working with to provide solutions and where digitalization is ongoing.

NIST may make their evaluations for encryption and algorithms as early as next year and as these standards come through, one of the main areas to be affected will be that of the digital signature. For entry-exit system, for travelling document, the digital signature is, of course, crucial for the verification of the travel document and to ensure that the document is issued by known authorities.

How are solution supplier responding to these challenges?

As a solution provider, when we see this type of risk, we make a risk analysis that asks the question; What does this mean for the solution and for the clients, for our government? Here, it's important, especially for any entry-exit system and its' Trust Anchor: the traveler's documents. But today it's more complicated as we see a trend that not only will there be a physical document but ICAO has already started publishing so-called "digital travel credentials", which, simply put, is a copy of the physical travel document on a mobile phone.

In the European Union, we are now discussing the e-Wallet, which will consolidate different mobile application into one wallet for the citizen. We have also this challenge, LDS 2.0, which includes the entry/exit stamps on a travel document, as well as the visa information contained within the same document. Under these circumstances, it's important to know how much of an impact this has on the chip design and on the design of the travel document from the chip perspective. Which chip supplier will be able to provide chips that have a PQC-proof architecture and using specific, recommended algorithm? Lastly, when everything goes mobile, is the mobile phone still trustable? Can the algorithms that are used can be upgraded in the future, and is the secure element ready for that? For a mobile phone, we can say the lifetime is usually two years. Then it gets replaced. But in a government area, we talk about five or ten years. This is the challenge.

LUTZ RICHTER, *Dipl. Ing (FH) for Engineering and Automation, is Head of Information Systems at Mühlbauer ID Services GmbH. He completed his studies at the University of Applied Science for Technology and Economics in Dresden and has been with the company for 20 years now. During his long and ongoing career in the industry, he worked, amongst other positions, as Senior Solution Architect and Analyst for Identification Management Systems. He is responsible for the development of Identification Management Systems, e-Government and Entry-Exit-Systems.*

All this is in line with activities from the IATA, the International Air Transport Association, which has, of course, a requirement to further digitalize the passenger facilitation. They are working currently on a contactless travelling system, which makes the whole journey for a traveler digitalized from the check-in at home (there is no airport check-in counter), to a kiosk, luggage drop-off, and security check. Next step is the entry/exit section, which is government controlled, and then on to boarding. There is a need for digitalization to encourage and facilitate such self-service within the process.

As a solution supplier, Mühlbauer gets asked from governments and clients for Requests for Information (RFI) and Request for Proposals (RFP) that pertain to new systems and the upgrading of current systems. It is currently very hard to incorporate design sections that pertain to PQC when we have so little idea of the time frame involved in the wide-scale introduction and adoption of quantum computers. These RFI's and RFP's are not only focused upon travel documents and their future digitalization. Here at Mühlbauer, we see a continuous trend for mobile driving licenses based on the ISO 1813-5. There's another ISO in development – DTC and LDS, and in the European Union, an initiative for Trusted E-Services, eIDAS, and finally the e-Wallet. Everything together in one hand.

We can, and will, interact more and more with digital services, but will it remain safe under the shadow of quantum computers? When we come to an architecture, PKI is really the trust anchor (the private key). The private key is always stored in the so-called HSM, (High Secure Module). We have different components in the PKI such as the CSCA, the country signer, country authority, and the document signer, which is very important for the issuance of the electronic documents. It doesn't matter if it's digital or mobile.

These very specific components are needed. When the current algorithms are, let's say, violated and cannot be used any longer, then we have to consider the replace of these components because the HSMs, as long as we know, may not be easily upgraded somehow. They would have to be replaced. Both for the master list and the variation list signer that is also within the HSM.

What does this mean in terms of timelines?

When a government entity is working on a tender, we usually see that two or three years is not too long to issue this tender and Request for Proposal. Looking at a fictitious timeline we could say that a tender is published in 2025. Tender processes can take somewhere between six months to one year. So now arrive in 2026. And then the implementation timeline could be between 6 months to 12 months – brining us to 2027, and with a 5 to 10 years' timeline. And then we are easily in the middle of 2030 and the customer will ask, what is your strategy, your architecture, to be PQC protected? Are you able to upgrade the system? Are you able to update the system? These are difficult questions to answer at this point in time.

However, the fundamental starting point for these questions lies with the architecture. It means working with other technology providers from the chip supplier, the HSM supplier manufacturer, all the way to the security infrastructure, because all the components which handle the digital signature and encryptions, get affected by design. We believe that this will not stop because the industry and the market is calling for more and more digitalization – or more self-services.

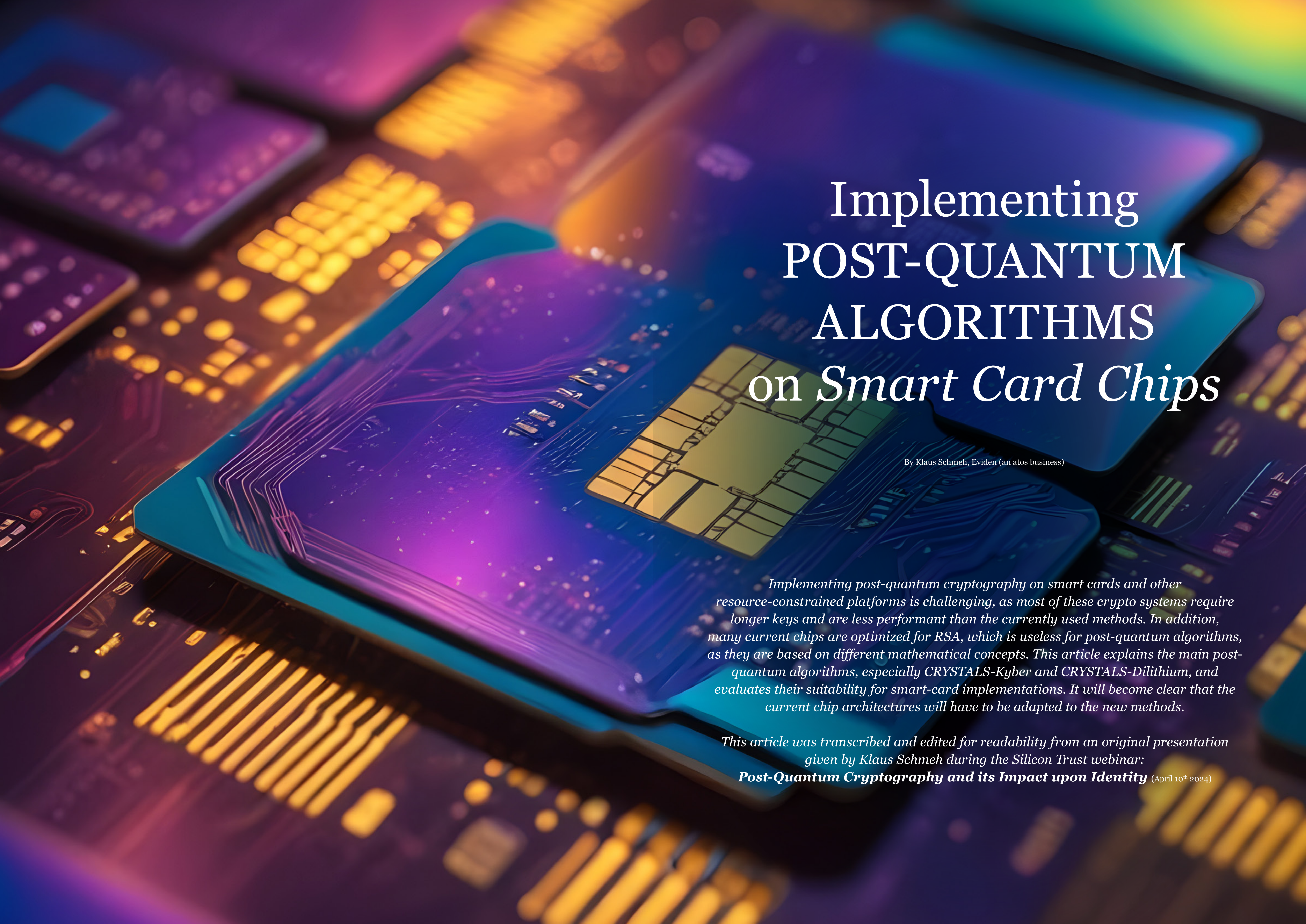
But what does that really mean?

It means having discussions with the relevant parties now, on upgrading digital mobile documents with PQC-proven chips and secure elements. It means working with partners in the near future on upgrading personalization systems from machine to the issuing system, to support PQC and then upgrading the inspection system in total. This will require a new generation of high secure modules, upgraded algorithms for secure communication between the involved system components, and planning for new projects now which will have to run over the next 10 years to be ready for PQC.

As a solutions provider, our clients expect us to be informed about these upcoming changes. It is vital that there is co-operation between interested parties in this field to develop proof of concept papers, field trials and use every platform available to convince audiences those solutions based on Quantum Computers, Quantum Cryptography and Post-Quantum Cryptography are not a fad but an oncoming reality.

Because each of our human identities in any government system is the biggest asset that we, as individuals have. We have to do everything we can to protect it. ☒

Mühlbauer
High Tech International
UNIQUE IDENTITY SOLUTIONS
YOUR GLOBAL TECHNOLOGY EXPERT FOR IDENTIFICATION AND VERIFICATION
www.muehlbauer.de



Implementing POST-QUANTUM ALGORITHMS on *Smart Card Chips*

By Klaus Schmeh, Eviden (an atos business)

Implementing post-quantum cryptography on smart cards and other resource-constrained platforms is challenging, as most of these crypto systems require longer keys and are less performant than the currently used methods. In addition, many current chips are optimized for RSA, which is useless for post-quantum algorithms, as they are based on different mathematical concepts. This article explains the main post-quantum algorithms, especially CRYSTALS-Kyber and CRYSTALS-Dilithium, and evaluates their suitability for smart-card implementations. It will become clear that the current chip architectures will have to be adapted to the new methods.

This article was transcribed and edited for readability from an original presentation given by Klaus Schmeh during the Silicon Trust webinar:
Post-Quantum Cryptography and its Impact upon Identity (April 10th 2024)

What ties together a smartphone, an eID card, a web browser, and numerous other IT systems? The answer is likely evident: they rely on the RSA cryptosystem. However, when considering the advent of quantum computing, a critical vulnerability emerges: quantum computers excel at breaking RSA. Yet, there exists a notable limitation: quantum computers are currently incapable of breaking long RSA keys. While various sources provide differing figures, it is generally understood that the maximum key length susceptible to quantum attacks is merely 5 bits. This limitation renders practical implementation unfeasible, as contemporary encryption standards typically employ key lengths of around 2,000 bits. However, the prospect of future quantum computers with enhanced capabilities looms, posing a looming threat. If powerful quantum computers become widely accessible, the encryption utilized by these IT systems will be vulnerable to exploitation. This stark realization underscores the urgent necessity for Post-Quantum Cryptography.

What Post-Quantum Algorithms are available today?

Indeed, there exists a plethora of Post-Quantum Crypto algorithms, numbering well over a hundred encryption and digital signature methods. However, for the scope of this article, we'll narrow our focus to CRYSTALS-Kyber and CRYSTALS-Dilithium, currently recognized as the two most significant Post-Quantum algorithms. For comparison purposes, we'll also make occasional references to McEliece. Now, you might wonder, what do these methods entail?

CRYSTALS-Kyber functions as an asymmetric encryption algorithm, positioned as a viable alternative to RSA encryption. On the other hand, CRYSTALS-Dilithium operates as a signature algorithm, positioned as a replacement for RSA signatures. In essence, both CRYSTALS-Kyber and CRYSTALS-Dilithium offer themselves as substitutes for RSA. Presently, the primary objective is to translate these algorithms into practical applications. For a deeper understanding or an overview of the Post-Quantum Cryptography migration, I recommend consulting the Migration Guide recently published by Eviden.

Bringing the focus on smart cards

In this article, our focus lies squarely on smart cards, with a key emphasis on understanding the current architectures of these devices. Presently, smart cards typically boast around 16 KB of RAM and approximately 500 KB of flash memory, which is notably limited. Now, the pertinent question arises: how do these new Post-Quantum systems integrate with such platforms? Consider RSA, the conventional system, with a typical key length of 2000 bits (rounded from 2048 bits). Contrasting this with CRYSTALS-Kyber, a new Post-Quantum encryption system, reveals a substantial difference, as it requires 12,000 bits. Similarly, CRYSTALS-Dilithium, the digital signature system, demands even more at 20,000 bits. When we delve into McEliece, while it may not be the most prominent Post-Quantum system, its requirement of about 100,000 private key bits unequivocally exceeds the capacity of a smart card, rendering its implementation on such a platform highly improbable.

Now, let's shift our focus to public keys. Again, RSA maintains a 2000-bit key length, whereas CRYSTALS-Kyber and CRYSTALS-Dilithium necessitate longer keys. For McEliece, the public key extends to roughly a megabyte or potentially more in the future. As before, it's evident that accommodating a McEliece public key on a smart card is unfeasible. However, a noteworthy revelation emerges when scrutinizing the signature and ciphertext lengths: while RSA retains a 2000-bit length, CRYSTALS-Kyber yields a longer ciphertext of 6000 bits, and CRYSTALS-Dilithium produces an even lengthier signature (20000 bits). Conversely, McEliece generates a relatively shorter signature (1700 bits). Such discrepancies in Post-Quantum systems make direct comparisons challenging, as different metrics yield different results, be it private keys, public keys, signatures, or performance.

As a general rule, Post-Quantum algorithms necessitate longer keys than their traditional counterparts, thus requiring more memory. However, the complexity compounds when considering the varying procedures for signature and encryption in systems like CRYSTALS-Kyber and CRYSTALS-Dilithium. Unlike RSA, where a single routine suffices for both encryption and digital signatures, these Post-Quantum systems operate differently, necessitating distinct routines. Therefore, not only do we require additional memory for keys, but also for implementing these distinct routines.

Moreover, the situation exacerbates with the realization that Post-Quantum algorithms typically exhibit lower performance than their traditional counterparts. Thus, the demand for increased memory is paralleled by a need for heightened computational power.

From bad to worse?

Additionally, some experts recommend using hybrid algorithms. These involve employing both quantum algorithms and traditional algorithms simultaneously, requiring an attacker to break both to succeed. However, this approach demands even more memory and computational power.

Implementing all this on a smart card is particularly challenging. Many smart card chips come with an RSA co-processor, and while it is possible to develop a CRYSTALS co-processor, this technology is still in its infancy and effectively non-existent at present. Consequently, the need for increased computational power is even greater.

In summary, there are several reasons why quantum algorithms require more memory and computational power than RSA. Overall, implementing quantum algorithms on smart cards remains a significant challenge.

Research is the real key

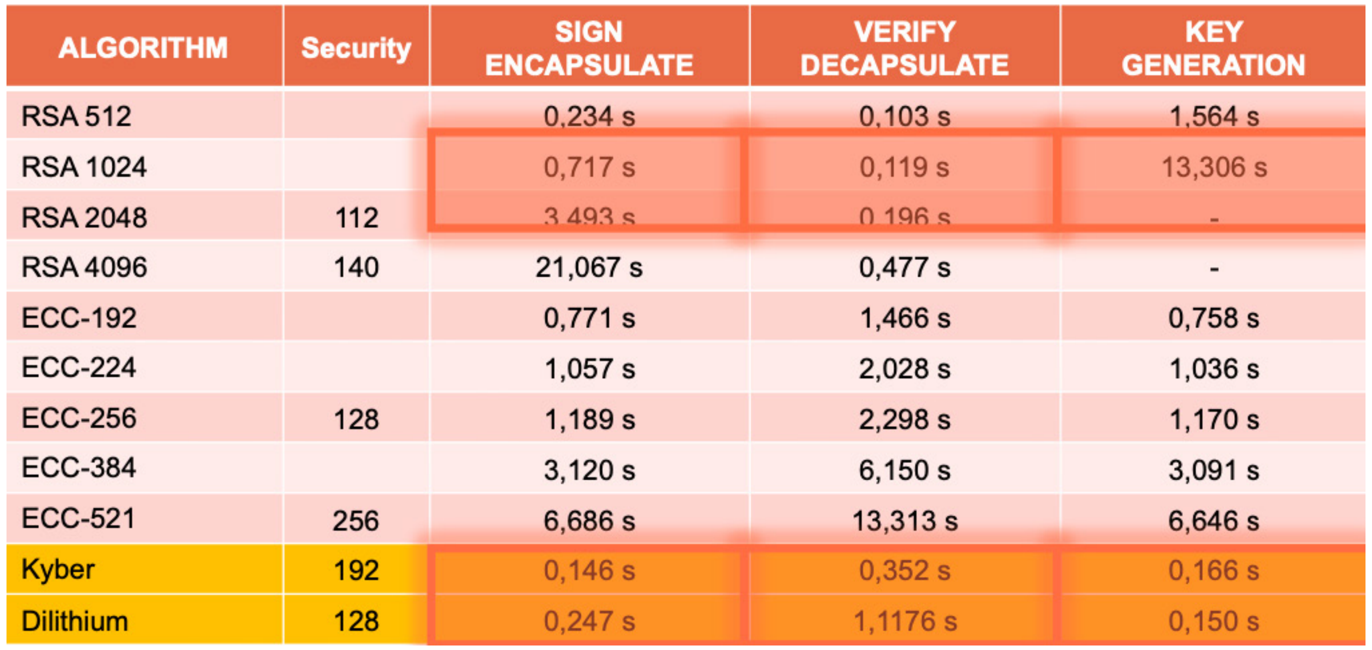
To tackle these challenges, extensive research is necessary to determine how Post-Quantum algorithms function on smart cards and whether they are viable in this context. Fortunately, such research is currently underway. In Germany, the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) is actively funding several Post-Quantum projects. They have established a directive, "Bringing Post-Quantum Cryptography to Applications" (2022), specifically aimed at this purpose. Here are a few example projects:

- **KRITIS3M**
- **Aquorypt**
- **QuantumRISC**
- **FLOQI**
- **SIKRIN-KRYPTOV**
- **PQC4MED**
- **KBLS**
- **QuantumQAP**

Some research projects focus on smart cards and embedded systems, such as QuantumRISC, which includes research in this area. PQC4MED investigates the use of Post-Quantum Cryptography in the medical sector, where smart cards and embedded systems are prevalent, making it crucial to explore the application of Post-Quantum Cryptography. The QuantumQAP project has similar objectives.

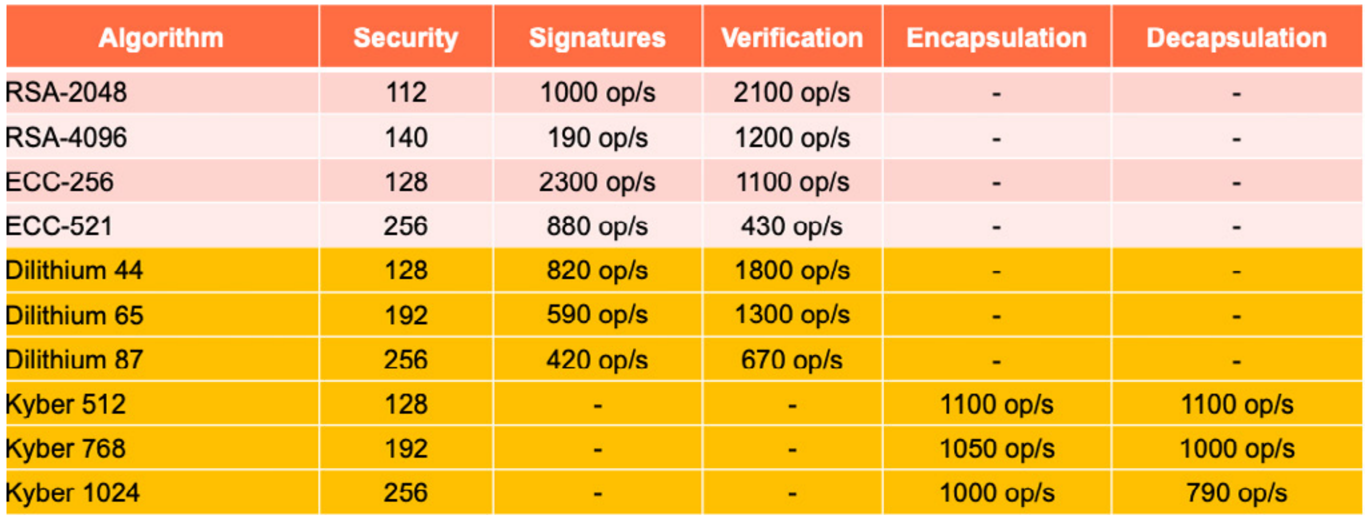
Despite the challenges of implementing Post-Quantum Cryptography on smart cards, there is some good news. Research has shown that existing RSA co-processors can also be used for CRYSTALS-Kyber and CRYSTALS-Dilithium. While the mathematics behind these systems differs from RSA, there are enough commonalities to make use of existing co-processors. Although this approach is less efficient than for RSA, it can still enhance the computation of signatures and encryption processes.

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..*



ALGORITHM	Security	SIGN ENCAPSULATE	VERIFY DECAPSULATE	KEY GENERATION
RSA 512		0,234 s	0,103 s	1,564 s
RSA 1024		0,717 s	0,119 s	13,306 s
RSA 2048	112	3,493 s	0,196 s	-
RSA 4096	140	21,067 s	0,477 s	-
ECC-192		0,771 s	1,466 s	0,758 s
ECC-224		1,057 s	2,028 s	1,036 s
ECC-256	128	1,189 s	2,298 s	1,170 s
ECC-384		3,120 s	6,150 s	3,091 s
ECC-521	256	6,686 s	13,313 s	6,646 s
Kyber	192	0,146 s	0,352 s	0,166 s
Dilithium	128	0,247 s	1,1176 s	0,150 s

Figure 1



Algorithm	Security	Signatures	Verification	Encapsulation	Decapsulation
RSA-2048	112	1000 op/s	2100 op/s	-	-
RSA-4096	140	190 op/s	1200 op/s	-	-
ECC-256	128	2300 op/s	1100 op/s	-	-
ECC-521	256	880 op/s	430 op/s	-	-
Dilithium 44	128	820 op/s	1800 op/s	-	-
Dilithium 65	192	590 op/s	1300 op/s	-	-
Dilithium 87	256	420 op/s	670 op/s	-	-
Kyber 512	128	-	-	1100 op/s	1100 op/s
Kyber 768	192	-	-	1050 op/s	1000 op/s
Kyber 1024	256	-	-	1000 op/s	790 op/s

Figure 2

There's better news

To save memory, one can avoid storing a certificate on the chip. The public key or the certificate of the user doesn't need to be stored on the smart card itself. Traditionally, this has been done because it requires minimal memory, but with the advent of Quantum Cryptography, developers or standardization bodies might opt to store only a hash value instead. Given the ubiquity of internet connections, downloading the public key when needed should not pose a problem.

My employer, Eviden, is also engaged in Post-Quantum Cryptography research. I have discussed with my colleagues and learned about their work. They are testing Post-Quantum cryptosystems on smart cards but use a Raspberry Pi Pico microcontroller to simulate a smart card. This choice, though unexpected, has proven effective.

This approach allows for the simulation of various smart card architectures, leading to several interesting findings. For instance, there is a trade-off between memory and performance when implementing CRYSTALS-Kyber and CRYSTALS-Dilithium. More memory enables faster implementation of these systems, while less memory results in reduced performance. This trade-off is noteworthy because memory and performance are typically considered distinct aspects in cryptography.

When examining a typical smart card architecture with 16 KB of RAM and 500 KB of Flash, I asked my colleagues if it was possible to implement CRYSTALS-Kyber and CRYSTALS-Dilithium on such a platform. The answer was 'No'. This indicates that current low-end smart card architectures are inadequate for these implementations. Even with efficient coding, it is not feasible to use these cryptosystems on low-end smart cards, highlighting the need for next-generation smart card technology.

We need next generation smart cards

For instance, with 96 KB of RAM and 1000 KB of Flash, the outlook is much more promising. According to my colleagues, it is feasible to implement CRYSTALS-Kyber, CRYSTALS-Dilithium, and a few other systems on such a platform with reasonable performance. Figure 1, which I received from my co-workers, provides a detailed table of performance metrics. Despite the numerous figures, it is notable that the performance of CRYSTALS-Kyber and CRYSTALS-Dilithium is not necessarily inferior.

CRYSTALS-Kyber and CRYSTALS-Dilithium are actually faster than RSA for signing and encapsulating (e.g., encrypting). This was initially surprising, but it demonstrates that Post-Quantum Cryptography schemes can sometimes outperform traditional ones. However, when it comes to verification and decapsulation (e.g., decrypting), RSA is faster than CRYSTALS-Kyber and CRYSTALS-Dilithium. Although key generation is typically not as critical since it is performed only once, CRYSTALS-Kyber and CRYSTALS-Dilithium still perform reasonably well in this regard.

Figure 2 presents another interesting comparison, this time involving a hardware security module (HSM) instead of smart cards. The results are similar: CRYSTALS-Kyber and CRYSTALS-Dilithium are slower for signing and decrypting but faster for verifying and encrypting.

The operations performed on the chip, specifically in an environment with limited resources, include signing and decrypting. These are mission-critical operations. Since CRYSTALS-Dilithium signs faster than RSA, it appears to be a suitable choice for smart card signatures. Although the keys are longer than those used in RSA, this is manageable. Consequently, we don't need to be concerned about digital signatures on a smart card chip.

However, the situation is different when it comes to encryption. While Post-Quantum keys are longer, they are not excessively so, and the performance is slower but still acceptable. Generally, this is manageable. The key operation on the chip is decryption, which is slower for CRYSTALS-Kyber compared to RSA. Therefore, we can anticipate that future smart cards will need to offer more resources to support decryption.

In summary, as quantum computers become increasingly powerful, it is crucial to take action within the next 10 to 15 years. Transitioning to Post-Quantum Cryptography is essential, and smart cards must support this technology as well. Implementing Post-Quantum Cryptography on smart cards poses a significant challenge due to its higher memory requirements and, in some cases, lower performance.

Implementing these systems on smart cards seems feasible, but it's important to note that better smart card hardware is needed in the near future. Promising results have been achieved with CRYSTALS-Kyber and CRYSTALS-Dilithium, so we will see what developments occur in the coming years. Overall, with additional research, it appears possible to implement these systems on a smart card in a way that is suitable for practice. ☒

TRUST, INNOVATION AND LEGACY: An In-Depth INTERVIEW *with the Founders of* WIBU-SYSTEMS

As Wibu-Systems celebrates its 35th anniversary (1989-2024), its founders Oliver Winzenried, CEO of WIBU-SYSTEMS AG in Germany, and Marcellus Buchheit, CEO of WIBU-SYSTEMS USA, shared their reflections on their journey to becoming the global leader in secure license management. Their commitment to business continuity, technological advancement, and team cohesion has driven the company ecosystem forward. Looking ahead, they remain committed to financial independence, market expansion, and pioneering innovations that meet their clients' needs.

By Daniela Previtali, Global Marketing Director, WIBU-SYSTEMS AG

Reflecting on 35 years, what was the moment you realized your vision for the company was becoming a reality?

Oliver Winzenried

We saw the first copy protection products on the market, and Marcellus and I had the idea that we could do it much better and much more securely. So, we started developing our solution. The turning point came when we secured our first customer, who ordered 500 pieces of Wibu Boxes. That was the moment we knew we had a viable product.

Our confidence grew even more at our first trade show. In 1990, we attended CeBIT and garnered over 300 leads in one event. This local success was a significant milestone, bringing in many new customers. Our next step was to go international. In 1993, we participated in Comdex Fall in Las Vegas, which attracted many North American visitors and international interest. The demand for our product was clear, with inquiries coming in from distributors worldwide.

We became firmly convinced that there was a long-term need for robust software copy protection for PC software. Although we couldn't foresee the market's evolution towards IoT, embedded devices, and intelligent devices, we knew the market was vast and had room for more than one supplier. This conviction reassured us that we were on the right path.

How has your initial vision changed over the past 35 years?

Marcellus Buchheit

The short answer is that we evolved from software protection to software licensing and then to software monetization. Initially, our focus was on simple dongle-based protection: the software would only work if the dongle was present. However, our customers soon demanded more sophisticated features, like expiration dates for subscription licenses, unit counters for pay-per-use models, and the ability to update the dongle remotely at the end user's site. This need for more flexibility gave birth to software licensing.

When we developed CodeMeter, we made software licensing our central focus while maintaining robust protection features. This led to the concept of secure software licensing, which offered various options that could be seamlessly integrated into ERP systems. CodeMeter License Central became the cornerstone of this new approach, allowing customers to optimize their software sales by managing different licenses tailored to various markets and clients.

This evolution culminated in software monetization, where we now assist our customers in maximizing their revenue by efficiently prioritizing and managing their licenses. Today, we enable our customers to optimize their product sales by leveraging advanced licensing strategies, ensuring they can adapt to the diverse needs of their markets and clients

What is the source of new ideas?

OW
There are two primary sources for new ideas: our clients and our employees. The combination of their insights and feedback helps us develop a core architecture that meets all market requirements.

MB
For example, I initially believed that software-only protection wasn't secure enough compared to dongles. However, our customers expressed a strong need for this alternative within our architecture. This led to the development of CodeMeter ActLicense, incorporating advanced technologies like SmartBind to meet these demands. Later, customers requested a CodeMeter Cloud, and we responded by implementing it.

These innovations demonstrate the importance of listening to our customers. If we had remained solely focused on dongles, we likely would have lost relevance in the market. Instead, by embracing new ideas from our clients and employees, we continue to evolve and meet the changing needs of the industry.

OW
A great example of our innovation is our CodeMeter License Central and License Portal. These platforms enable ISVs and device manufacturers to seamlessly deploy and manage their licenses within their business processes, while also allowing users to self-administer their licenses. The initial ideas for these innovations came from our sales team and were perfected through close collaboration with our customers. This blend of internal insight and customer feedback is the key source of our new ideas.

What were some unexpected challenges, and how did you overcome them?

MB
Oliver and I both come from engineering backgrounds and lacked formal business education. Initially, we underestimated the importance of marketing and proactive sales. We believed that a superior product would sell itself, but reality proved otherwise. We had to pivot quickly to develop our marketing strategies, proactively pursue sales, and establish a robust support system to keep our customers satisfied. These foundational efforts were crucial during the early years of our company.

One significant challenge occurred shortly after our first exhibition at CeBIT Hannover. We received a lawsuit from a company claiming that we were infringing on their name, Wibu, despite us having a trademark for it. Although we eventually won the lawsuit, it was a time-consuming and frustrating distraction from our core business activities.

When we expanded to America, we faced another legal battle over an alleged patent violation, which was unfounded. However, defending ourselves was challenging and ultimately resulted in a costly settlement at a time when our company was still relatively small.

Expanding into China brought its own set of issues. Competitors argued that our cryptographic security device should not be imported into China. After a thorough review, this claim was rejected, allowing us to continue selling our products in the Chinese market.

These experiences taught us valuable lessons in navigating legal challenges and the importance of having a solid business strategy beyond just developing great technology.

Can you share a pivotal decision that significantly shaped the company's journey?

OW
Three pivotal decisions significantly shaped our company's journey:

Going International:
We began our international expansion in 2001 with WIBU-SYSTEMS USA, Inc. and continued in 2003 with WIBU-SYSTEMS (Shanghai) Co. Ltd. This was followed by further expansion into European countries, the founding of WIBU-SYSTMS K.K. in Japan in 2018, and the ongoing establishment of WIBU-SYSTEMS Korea, Ltd. This global presence allowed us to tap into new markets and broaden our reach.

Evolving from Copy Protection to Flexible License Management:
We transitioned from focusing solely on PC software copy protection to providing highly flexible license management solutions for intelligent devices and the cloud. This shift recognized that software is now ubiquitous and needs to be managed dynamically across various platforms.

Collaborations:
Partnering with research institutes, suppliers, and customers has been crucial. These collaborations help us understand market demands more quickly and enable us to develop and implement the latest technologies by combining unique and specialized knowledge from different parties. This collaborative approach has kept us at the forefront of innovation.

Looking back, is there anything you would have done differently?

MB
Not really. Overall, we expanded the company successfully, even though we weren't always sure what would happen. We made mistakes, learned from them, and ultimately improved because

of those lessons. If I were to change anything major from the beginning, I would say no. However, there are minor things we could have done faster. For example, we only opened our first own office 12 years after the company started. Before that, we relied on distributors—some were successful, others not as much. We waited too long to transition from solely using distributors to combining them with our own offices. Having our own offices sooner would have allowed us to better optimize our strategy in specific countries.

What is unique about Wibu-Systems products?

OW
Wibu-Systems offers a comprehensive solution, often described as the Swiss Army knife for software protection, software licensing, and software security. We refer to this as 4D interoperability, supporting various processor platforms like Intel, ARM, MIPS, and PowerPC, as well as numerous operating systems and target platforms. We offer different types of license containers, including hardware dongles, activation-based, and cloud-based solutions.

Additionally, we provide solutions that integrate license deployment into the business processes of ISVs and device manufacturers.

Let me highlight two unique selling points:

Long-Term Availability:
Since we provide our products to integrators who embed our solutions into their own offerings, long-term availability is crucial. We demonstrate our commitment to this by continuously supporting solutions from 1989 to the present.

High Level of Security:
Our solutions have repeatedly proven their security through public hacker contests and have received numerous awards for their robustness. We also assist our customers if they encounter any breaches in software protected by our technology, ensuring continuous security and support.

How should your clients see you?

MB
We view the relationship with our clients as a lifelong partnership. Our goal is for customers who use our products today to continue using them indefinitely. This commitment works only if we proactively listen to their evolving needs and future expectations, implementing these into our products while maintaining the highest levels of security, flexibility, and backward compatibility.

What is a lesser-known story about the early days of the company?

OW
Marcellus and I met at the amateur radio station of Karlsruhe University. Marcellus was studying computer science, while I was studying electrical engineering. It was there that we conceived the idea of creating a better copy protection system with a higher level of security.

Another important aspect to mention is the invaluable support from our families. Our first trade show at CeBIT in Hannover in 1990 wouldn't have been possible without their intensive help. They assisted in setting up the booth, creating the booth design, and even taking care of small details like making silk clothes for our staff at the trade show. This family support was crucial in getting our company off the ground in those early days.

How do you envision the future of the company and the industry?

MB
We aim to remain at the forefront of technology and innovation while preserving our flexibility and backward compatibility. Our successful strategies of the past will continue to guide us. However, we must also recognize new market opportunities. Many smart devices are currently sold as hardware without monetized software, unlike computers today. This presents a significant opportunity for us. We believe that as hardware becomes more standardized and cheaper, the software will become the valuable component, sold through subscriptions, pay-per-use, and other models for which we already have solutions.

We also foresee consumer devices being sold via subscription models. Instead of a high upfront cost, the initial price will cover the hardware, and the software will be sold over time through subscriptions. From a technological perspective, AI is a new focus for us. We plan to protect AI software and AI models where appropriate, and we see AI as an opportunity to enhance our products, making them more secure and flexible.

Additionally, we are preparing for the challenges of post-quantum cryptography. Our software relies heavily on asymmetric encryption, so we will integrate new algorithms currently in development as soon as possible to future-proof our products.

How do you see your role in the company changing in the next decade?

OW
I am committed to ensuring the continuous development and growth of our company while maintaining financial independence and without selling the company in the future. Continuity is crucial for our customers, employees, and partners. By establishing a dynamic young management team, we are evolving the company in line with Marcellus's vision and mine, ensuring sustained innovation and stability for all stakeholders.

MB
Think of the company as a human body. Initially, the founders are the heart—if they stop working, the company might cease to exist. As the company grows and adds more staff, the founders become the brain, focusing more on strategy and vision than daily operations.

Approaching retirement, or even after retiring, the founders remain the soul of the company, ensuring it continues to operate according to their vision. In the next 10 years, I might not fully retire, but I will likely transition from being the brain to becoming the soul, guiding the company's spirit and long-term direction.

What do you hope will be your legacy and that of the company?

OW
My principles revolve around building trustworthy partnerships—whether with customers, suppliers, or employees. A culture of trust within the company empowers our staff to achieve their goals. Financial independence is crucial as it allows the company to make decisions freely. Innovation is essential to address future challenges effectively.

I hope that Wibu-Systems will be synonymous with software protection, software licensing, and software security. Our goal is to provide solutions that not only add business value but also remain ethical, fair, and sustainable. This legacy of integrity, innovation, and trust is what I aspire for both myself and the company to be remembered by.

DANIELA PREVITALI is a marketing veteran who has dedicated more than twenty-five years of her career to the service of world-leading IT security vendors. Throughout her journey in this field, she has covered executive positions in international sales, product marketing, and product management and acquired comprehensive knowledge of both digital rights management solutions and authentication technologies. Working from the German headquarters of Wibu-Systems, she is currently leading both corporate and channel marketing activities, innovating penetration strategies, and infusing her multinational team with a holistic mindset.

SILICON TRUST DIRECTORY 2024

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 an independent company specialized in the development of high-security and operating systems. We provide MTCOS, our Mask Tech operating system, and various included applications for the electronic document and authentication market as license or as a chip and OS package. Our product range includes generic and customized applications for chips of the leading security semiconductor manufacturers as well as security certification services. To date, MTCOS protects more than 400 million eDocuments around the globe. **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

35 YEARS 1989-2024 Propelling Your Business To New Heights

CodeMeter – An Endless Virtuous Cycle for Your Business Growth

PROTECT YOUR SOFTWARE with cutting edge encryption and obfuscation technologies

MEET YOUR CUSTOMERS' demands with a versatile and scalable licensing system

REAP THE REWARDS from your work on a global scale, and repeat the entire process

Meet the EXPERTS!

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

SECURITY
LICENSING
PERFECTION IN PROTECTION