NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

MARCH 2024

The VAULT

AUTHENTICATION & ACCESS CONTROL

FEATURED ARTICLE

NEXT LEVEL BIOMETRIC BRILLIANCE

Infineon Technologies

ALSO IN THIS ISSUE

Contents

Imprint

THE VAULT ISSUE 39
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, Thomas Oberle, Nicole Wagner
PHOTOS: ISTOCKPHOTO, INFINEON TECHNOLOGIES, WIBU-SYSTEMS, MÜHLBAUER, WEPIK AI IMAGE EDITOR, KROWNE COMMUNICATIONS, MIDJOURNEY
EDITION: MARCH 2024.

FLOW *instead* of falter SEAMLESS travel made *easy*

By Katharina Schuldt, Mühlbauer Group

We live in the digital age; all our devices are smart, count our steps, measure our pulse. They remind me to leave my apartment early enough and manage to avoid every traffic jam so that I arrive at the airport on time. Once there, however, neither my smartphone nor my smartwatch come up with a plan B: there is no detour for the way through check-in and security control. The waiting game begins.

After a study from the US luggage storage company Bounce between March 2021 and March 2022, the average security wait time at Miami International Airport – the largest gateway from the US to Latin America – was 24 minutes and 54 seconds. Average passport control wait time was 22 minutes and 3 seconds. That means a passenger was waiting 47 minutes only for these two control stations, not to mention the waiting time to drop off or pick up the luggage and passing through the terminal!

Are there also examples where you can speed through the airport quickly? Indeed, there are! It does not always depend on the airport's size or passenger number how long the travelers have to queue up. The system is crucial. More and more people use electronic passports, but an alarming number of airports and border crossing stations still control every passport manually. Automated border control (ABC) systems though are more efficient and offer higher security, because they avoid human mistakes and match the data within seconds. Flow instead of falter!

> *The benefits of automated border control systems like Muehlbauer's Easy Flow are not only appealing for the traveler. Replacing manual processes saves time and reduces operating costs and personnel expenses.*

Fast check-in at smart kiosks

The German innovative technology specialist Muehlbauer has developed an airport and border crossing solution, where automated security systems take over the verification and authentication of travelers and their identity documents. The MB Easy Flow system allows the passenger to fill out the digital declaration forms before starting the journey via smartphone or computer. At the airport or border crossing checkpoint, the passenger can directly check-in at a smart kiosk. The high-tech kiosk reads the traveler's biometric data from their ePassport or eID and performs a quick presence check via facial recognition, liveness and fever detection. For this purpose, the sophisticated system automatically moves to the height of the traveler's face and uses a built-in camera and thermometer to take the required data and match it with the appropriate database. Officials will immediately be notified if a passenger is considered unfit to pass or has incomplete travel documents. Of course, manual intervention is possible at any time, but the majority of passengers pass through the station without personal contact. This speeds up the process enormously and brings further advantages like contact reduction during pandemic conditions.

Passport control without standstill

The intelligent system automatically passes on the information to the relevant authorities and the flight operator receives a notification when check-in and verification have been completed. After the flight crew gives their OKAY, the boarding gate is activated automatically. To board the aircraft, passengers now seamlessly pass through the last control station: Muehlbauer's smart gate. There is no need for stopping, the traveler just walks through the gate, pointing the head to the integrated camera screen. The gate checks if this person is allowed to access by facial verification on the fly and the passenger can proceed to the aircraft.

The benefits of automated border control systems like Muehlbauer's Easy Flow are not only appealing for the traveler. Replacing manual processes saves time and reduces operating costs and personnel expenses. Eliminating human mistakes protects against forgery and increases data security. As a cloud-based application, the system can be connected with a closed and secured network. This allows the operator to monitor and intervene in real-time from anywhere. These smart solutions can be integrated in the existing infrastructure and do not need expensive alteration. Essentially, we could use and utilize our digital resources and our knowledge about artificial intelligence to offer a satisfying and comfortable experience to both the passenger and the employee. ☒

NEXT-LEVEL Biometric *BRILLIANCE*

By Nicole Wagner, Infineon Technologies

In a world where digital threats loom large, the need for robust and foolproof security solutions has never been greater. Users urgently require stronger and more secured authentication and access mechanisms, offering the highest level of protection to overcome a growing wave of cyberattacks. For widespread adoption, these mechanisms must be easy to setup and easy to use. Authentication solutions using biometrics are the key to secured transactions, giving users the most convenient experience possible while reducing the risk of lost or stolen credentials. Giesecke+Devrient's StarSign® Key Fob is a remarkable biometric product designed to provide both unparalleled security and user convenience for strong authentication and secured access.

Giesecke+Devrient (G+D) selected Infineon's FIDO2-certified USB token reference design to serve as the platform for their key fob as it provides unbeatable security advantages and tremendously accelerates the development of USB tokens and FIDO security keys. Based on the SLE 78 security controller, the reference design powers a device-bound passkey for FIDO authentication and stands as a testament to Infineon's commitment to simple and strong authentication.

Harnessing the unparalleled security features of Infineon's reference design, the StarSign® Key Fob represents the next-generation biometric identity platform for physical and logical access, encryption, signing, payment, and other transactions and sets new industry standards in enterprise authentication, secured transactions, and access control. This joint solution is a further milestone in the long-standing collaborative relationship between Infineon and G+D, reflecting their joint commitment to protecting digital frontiers. As G+D and Infineon continue their journey of innovation, one thing is certain: the StarSign® Key Fob powered by the SLE 78 security controller is not just a token; it is a symbol of trust, reliability, and a safer digital future.

Infineon's contribution: FIDO2 reference design based on the SLE 78 security controller

With all security credentials and applications hosted in the SLE 78 Common Criteria EAL6+ certified security controller from Infineon, the key fob is compliant with stringent security standards, instilling confidence in users and organizations alike. As the reference design is supporting the FIDO open industry standards for two-factor authentication (FIDO U2F) and for strong authentication on the Internet (FIDO2), the StarSign® Key Fob is able to reduce the need for passwords by providing the physical device itself as the first authentication factor, and the built-in biometrics as the second authentication factor.
Featuring the SLE 78, this reference design is the only single-chip solution on the market supporting both a USB and an NFC interface. In addition, the reference design is equipped with a BLE controller for easy upgradability towards triple interface designs. Infineon is the first supplier of a FIDO2 design for FIDO security keys combining enhanced security functionalities with passkey authentication in a cost-effective and compact package.
Equipped with robust hardware security mechanisms, the reference design enables secured storage and processing of cryptographic keys. The design's unparalleled resistance to tampering also secures the integrity of sensitive information, establishing trust among users and organizations. Additionally, it incorporates industry-leading encryption algorithms, guarding the integrity and confidentiality of user data.

Infineon's reference design accelerates certification process by a factor of 3

"G+D tremendously benefits from the reference design as it enables a rapid and cost-effective design of FIDO2-compliant authenticators and security keys", said Christian Vaas, Head of Product Management at G+D. "With Infineon providing the source codes and all necessary documentation, our developers were fully enabled to implement all functionalities that are essential to be compliant with the FIDO U2F and the FIDO2 authentication standards. We were able to remarkably accelerate the development of our key fob and consequently decreased the time-to-market, which would not have been possible without Infineon's highly sophisticated reference design." Building on the reference design, G+D has crafted a FIDO-certified product and was able to easily validate the StarSign® Key Fob during FIDO U2F and FIDO2 interoperability testing, obtain the BLE certification, and secure further device approvals. In less than one month, the company secured the FIDO certifications – which is about three times faster than without Infineon's reference design.

NICOLE WAGNER'S *expertise lies in hardware-bound authentication and access solutions, with a focus on enterprise, government, and predominantly organizational use cases. As a Product Marketing Manager at Infineon Technologies, she oversees the global authentication and the physical and logical access portfolio, which includes the management of Infineon's security controllers for smart card applications, USB tokens, and FIDO security keys. Nicole holds a Master's Degree in Management & Technology from the Technical University of Munich, Germany*

G+D's StarSign® Key Fob

This StarSign® Key Fob is more than just a physical token. It is the first biometric solution combining a FIDO security key (to generate a passkey that is securely linked to the hardware device used for FIDO authentication) with physical access control and payment applications in one single device. The integrated fingerprint sensor provides enhanced security and gives users the convenience of a single touch.
The potential enterprise use cases of this sleek, yet stylish key fob are manifold. It provides authorized physical access to buildings, offices, and restricted company areas. It grants phishing-resistant logical access to company workstations, PCs, laptops, tablets, smartphones, and other IoT devices by authenticating users looking to access servers, drives, company data, and even web and online services.
The key fob seamlessly integrates into existing infrastructures and is supported by a range of communication channels, including NFC, USB, and Bluetooth® Low Energy (BLE). Offering user-friendly interfaces, it brings the power of authentication and access control to the employee's fingertips. Its versatility makes it an indispensable tool, finally bringing fingerprint biometrics to the enterprise market. With its long-lasting hardware and a tamper-protected Secure Element from Infineon, the key fob promises durability and reliability over time.

What is FIDO?

FIDO, which stands for Fast Identity Online, is an industry alliance dedicated to revolutionizing online authentication and reducing the reliance on passwords. The FIDO Alliance, a consortium of industry leaders including G+D and Infineon Technologies, has experienced tremendous success in its mission to establish open standards for stronger authentication.

One of its main objectives is to bring faster, easier, and more secured authentication to all industries. It also aims to establish passkeys that are both resistant to phishing and convenient to use as the industry standard for sign- ins to web platforms and applications across multiple user devices.

With widespread adoption across industries, FIDO has become a global benchmark for secured and convenient authentication methods. The alliance's collaborative efforts have reshaped the cybersecurity landscape, driving innovation and empowering users worldwide. ☒

Ultra-Thin *ELECTRONIC* eDatapage by Coil on Module Revolutionizes Turkish PASSPORT TECHNOLOGY

> *“At Infineon, we are delighted to continue our role as a trusted partner to Türkiye by consistently integrating our security components into the new government identity eDocuments. Enabled by embedded Infineon components, the new eDatapage is only 630 µm thick, making it one of the thinnest in the world. We are very proud of this attractive and reliable product that represents the next level of document security and design.”*
>
> *– Maurizio Skerlj, Vice President Authentication & Identity Solutions at Infineon’s Connected Secure Systems Division*

Ensures exceptional document durability and protection against forger

Türkiye has issued nearly five million next-generation electronic passports with contactless Coil on Module (CoM CL) solution from Infineon Technologies AG. The passport includes a polycarbonate (PC) data page with an integrated security chip, which is embedded in a contactless module based on the reliable CoM technology. The data page contains sensitive personal data of the holder. Due to the security-critical nature of this information, official travel documents must be designed to highest security standards in order to provide reliable protection against tampering and fraud. Infineon’s contactless CoM solution not only increases the robustness of the ePassport, but also enables enhanced security.

Coil on Module technology for enhanced security and reliability

Innovative Coil on Module contactless packaging technology is designed for highly robust and flexible contactless government ID and passport documents. These travel documents require appropriate security and robustness over their lifetime, which is typically up to ten years. This packaging solution is based on inductive coupling technology, which uses a radio frequency link to wirelessly connect the module to the antenna embedded in the document, similar to the link between a card and a contactless card reader. This increases the robustness of an electronic datapage.
In addition, Infineon’s FCOS™ (Flip Chip on Substrate) manufacturing technology enables the production of a module with a thickness of only 125 µm, which is up to 50 percent thinner than conventional contactless modules. This facilitates the production of ultra-thin antenna inlays of approximately 200 µm for passport eDatapages that are approximately 500 µm thick. The reduced thickness allows the issuing state printer to embed additional security layers in the ePassport’s PC eDatapage to meet highest security standards.
Türkiye’s population has grown to nearly 86 million people by 2023 and is still growing. As a result, the demand for fraud-resistant passports is growing. The highlight of the new Turkish ePassports: Enabled by embedded Infineon components its ultra-thin electronic PC data page measures only 630 µm in thickness, making it one of the thinnest in the world. This makes the new Turkish passport stand out from many other travel documents in circulation, not only because of its exquisite design, but also because of its robustness and security features that help prevent fraud. ☒

Making the COMMERCIAL CASE for CodeMeter

By Thomas Oberle, Member of the Management Board, WIBU-SYSTEMS AG

Data in Wibu-Systems' new white paper shows the financial potential of their flagship protection and licensing technology

"Make or buy?" It is the short form of a question that every business will have to ask themselves, again and again. It is a question even our stone age forebears must have asked themselves: Should I spend precious daylight hours that I could be out hunting or flint-knapping to make myself a new arrowhead? Or should I instead trade that shank of meat from the aurochs that I caught yesterday for arrowheads?

In today's hyper-integrated and hyper-complex economy, the question is not as simple as that. From industrial tools to software, businesses can either invest skill, IP, and manpower to "make" them – that is, invent, design, and produce them – or they can invest financial assets to "buy" them. But just like their paleolithic ancestors, today's managers need some solid data to calculate and make their decisions.

Dealing in hypotheticals

One case in hand for software and hardware businesses is protection and licensing technology. No savvy IT manager would suggest trying to do without them. But should precious developer time be spent on creating their own system or patching together something from open-source pools, or should a third-party system be bought? The already complex calculation is made even more difficult by the potential reach of the technology: It is not just a simple question of money spent versus money earned, but a question of dealing in hypotheticals. An effective protection system wards off potential losses to piracy, sabotage, or IP theft, while a smart licensing system can be far more than an add-on bit of security for the regular sales process. It can open up new distribution channels, give access to new user groups, or even empower companies to create all-new business models. On top of actually realized revenue, the calculation becomes even more complex when you factor in the commercial potential left dormant without a licensing system or with an ineffective licensing system.

Wibu-Systems, the IT security, protection, and licensing specialists from Karlsruhe, Germany, is the company behind one of the leading technologies in the market: CodeMeter. With more than three decades of experience invested, CodeMeter has evolved from a powerful, but mission-specific protection and licensing system into a true business enabler. In addition to the award-winning and as yet unbroken encryption technology, the licensing capabilities of CodeMeter have evolved to accommodate virtually any software distribution and usage scenario possible, from the original one-off purchase to modern subscription, leasing, or software-as-a-service formats. A range of license containers, from tough hardware dongles with added protection capabilities to software-only or cloud license containers, is available. Different development and hosting services complete the package for software vendors looking to protect their IP, tap into new sales channels, or completely reinvent how they generate revenue with their software. But even if CodeMeter is worth the money in technological terms, is it a good investment from an accountant's calculated and not easily impressed perspective?

A buyer's guide

Wibu-Systems has dared to ask itself that question and subjected its offerings to a tough and unbiased calculation. Taking real-life data from a sample of its users, the resulting white paper "The Commercial Case for CodeMeter" tries to answer the question of what costs enterprises of different sizes can expect, what benefits they can expect from using CodeMeter, and what the return on investment will be. That ROI is the indicator that will determine the answer to the old question: Make or buy?

The case for a protection and licensing system is summarized in the white paper, drawing attention to the many factors to be considered, from the threat of software piracy to the need to protect IP from theft and unauthorized use to the ever-present dangers facing software security. Cyberattacks and sabotage are increasingly likely, especially in the current geopolitical atmosphere, at a moment in time when more and more nations and entire economies have come to depend on software-enabled services. The rise of AI is not only revolutionizing the IT world and many professions and businesses everywhere, it is also opening up new avenues for attackers.

But can these often shadowy and intangible risks be translated into reliable figures for an ROI calculation? Wibu-Systems' white paper does so by taking data from its own business to understand the three major factors to consider: the start-up costs, the costs saved and the potential revenue increase.

From boutique software developers to major corporations

To properly reflect the diverse nature of the IT industry, the white paper uses four sample case studies as a basis for its ROI calculation. Based on typical actual clients of Wibu-Systems, each case comes with its own commercial needs and financial capabilities.

Going from small to large, the case studies start with a bijou software development agency that supplies specialized simulation technology to industry automation providers. The company needs a simple, but seamlessly integrated licensing solution and expects sales in the region of EUR 0.2 million. Slightly different needs apply in the second case, a maker of 3D printing designs whose print data are at particular risk of theft and illicit use. The company has responded to that threat by using CodeMeter dongles as the tamperproof 'passports', giving its clients access to their designs.

The financial resources at stake increase substantially in the two other model cases. A medium-sized mechanical engineering business represents the third case. Its needs go beyond protecting the IP in its machines and extend to using CodeMeter's granular licensing to allow individual machine features to be paid for and activated at the point of need, reducing the entry threshold for its buyers and creating new channels for its aftersales business. With annual revenue expected in the region of EUR 10 million, the technological and commercial factors at work are more complex, with different development environments, virtualization solutions, and cloud services all involved.

The fourth and largest model business is represented by a company that produces a comprehensive business management solution for corporate clients. Beyond the technological considerations at stake, the challenge lies in ways to create and distribute massive numbers of licenses, ideally with extensive self-service capabilities. Annual revenues lie in the region of EUR 35 million.

Entry thresholds and aftersales corridors

The author of the white paper considers all relevant factors in his ROI calculation for these four model companies. The most straightforward element is the startup cost needed to purchase and integrate the licensing system. The needs diverge immediately beyond this point: While the smaller companies need to account only for the license for CodeMeter Protection Suite itself and for minor development efforts to integrate CodeMeter in their own software, the larger companies may have to call on support from Wibu-Systems Professional Services and Academy. In addition, the integration effort is substantially greater and extends, in particular for the corporate software business, to major changes to the back-office landscape. (Figure 1)

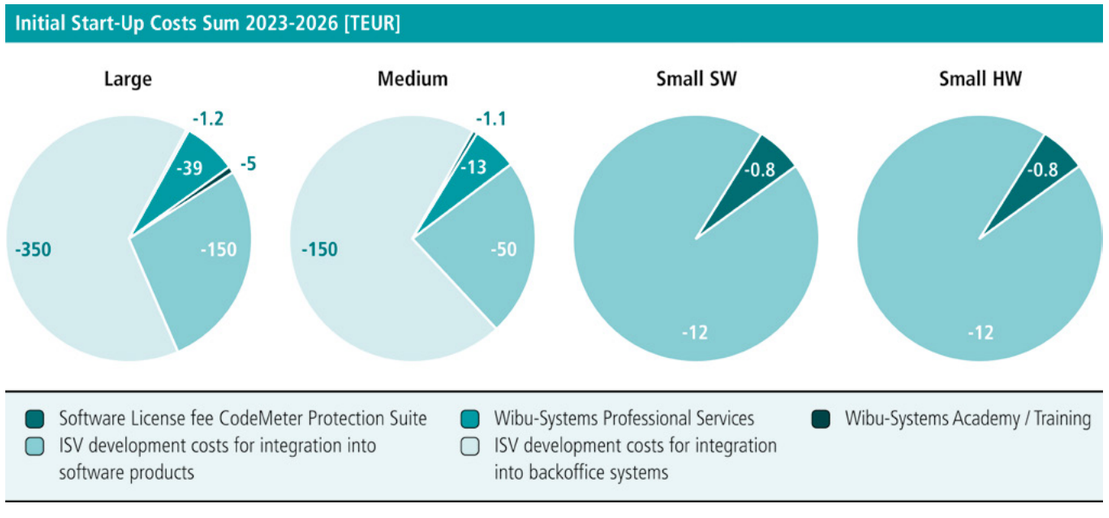

Figure 1: Sum of initial Start-Up costs in TEUR before operation of the licensing system

THOMAS OBERLE *holds a degree in electrical engineering from the University of Karlsruhe. He began his professional career as a hardware and embedded software developer for industrial fieldbus systems, machine controls, and operating devices.*

After completing his postgraduate studies in industrial engineering at the Kaderschule St. Gallen (CH), he moved into management consulting. Working initially as a process consultant for innovation management, product development, and project management initiatives, he then became a senior consultant for production, purchasing, and supply chain management endeavors. As project manager for the implementation of SAP ERP systems, he gained profound knowledge of common best-practice business processes in manufacturing.

At WIBU-SYSTEMS AG, he is a member of the management team, responsible for organizational development, process optimization, and the use of methods and tools, as well as for program and product portfolio management.

The entry threshold therefore can differ substantially from around EUR 12,000 to more than half a million. To this first cost factor, the costs of operating the integrated and fully functional licensing system need to be added. Made up of different license fees and e.g. the costs for physical CodeMeter dongles, operating costs can again range from the low tens to hundreds of thousands or even pass the million EUR mark in the large corporate case.

To counter these costs, companies can expect certain revenues from their choice of a licensing system like CodeMeter. This is where the author of the white paper offers his readers an invaluable insight into the realities of the market. Distinguishing between the revenue that is added simply by avoiding software piracy, the revenue created by expanding the potential market for the protected IP, and the potential kingmaker factors – the revenue created by turning novel and flexible licensing models into new business opportunities – the author offers meaningful figures from his case studies.

His findings are eye-opening: While the prevention of software piracy offers an expected revenue boost that ranges from EUR 10,000 to a full EUR 1.75 million for the corporate business, the ability to create novel licensing-driven business models has a positive impact on revenues that almost equals those amounts. While the smaller businesses can expect to make an additional EUR 30,000, the potential figure rises to over EUR 740,000 for the medium-sized business and over EUR 1.2 million for the largest business – all revenues that are not simply potential losses averted or recouped, but essentially newly created. (Figure 2).

Finally, the simplification of license creation and distribution processes and the entire software logistics process that is offered by a smart solution like CodeMeter has the power to save substantial costs in order processing, development, and support. With the same sliding scale for the four types of businesses, the savings determined by the author of the white paper range from over EUR 100,000 for the smaller businesses to an excess of a million for the largest business. (Figure 3).

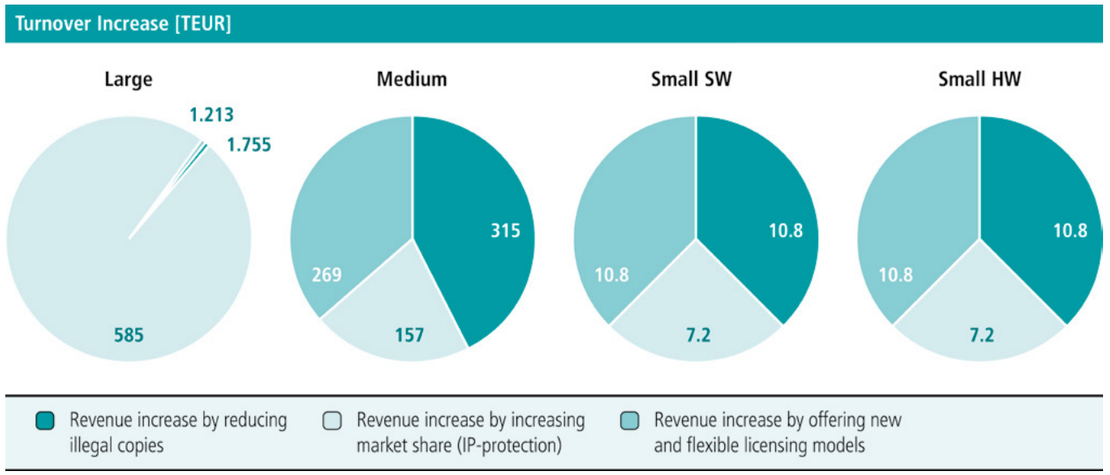

Figure 2: Increase in turnover, 3 years after integration of the licensing system.

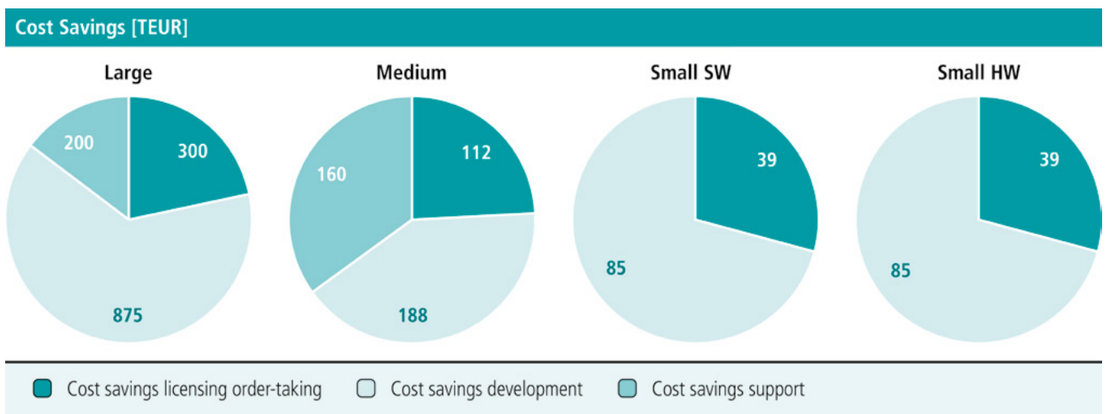

Figure 3: Cost savings, 3 years after integration of the licensing system.

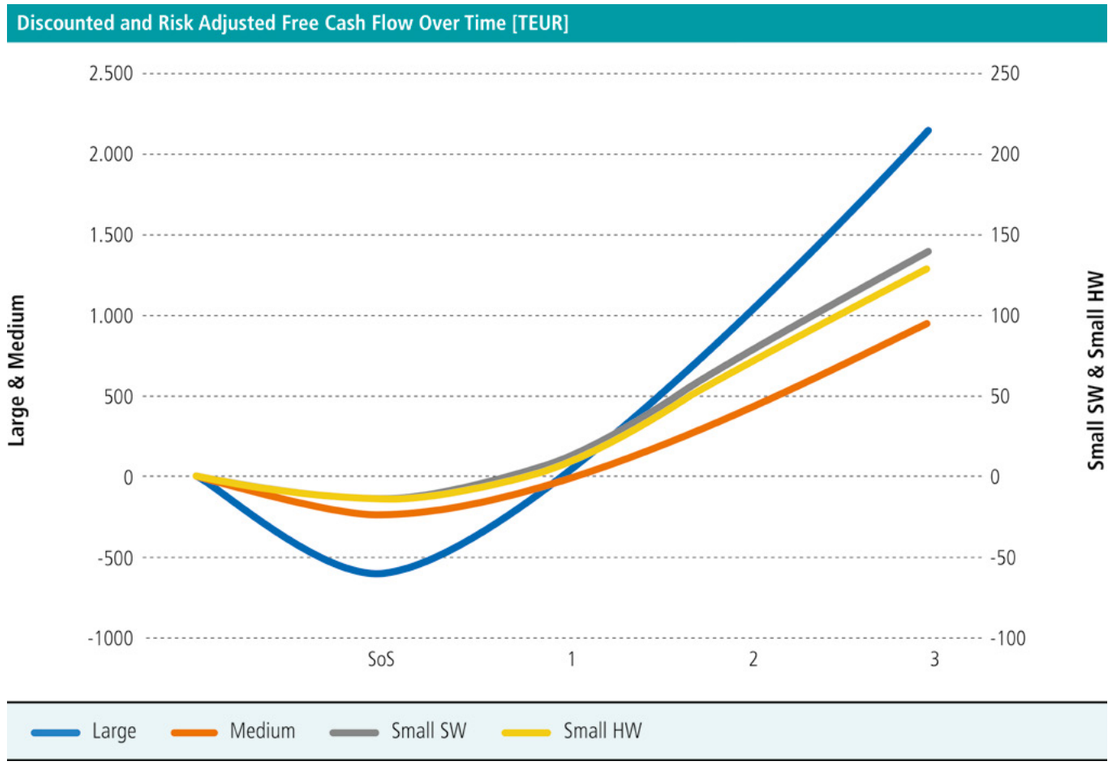

Figure 4: Cash flow during the project, attributed to the licensing system.

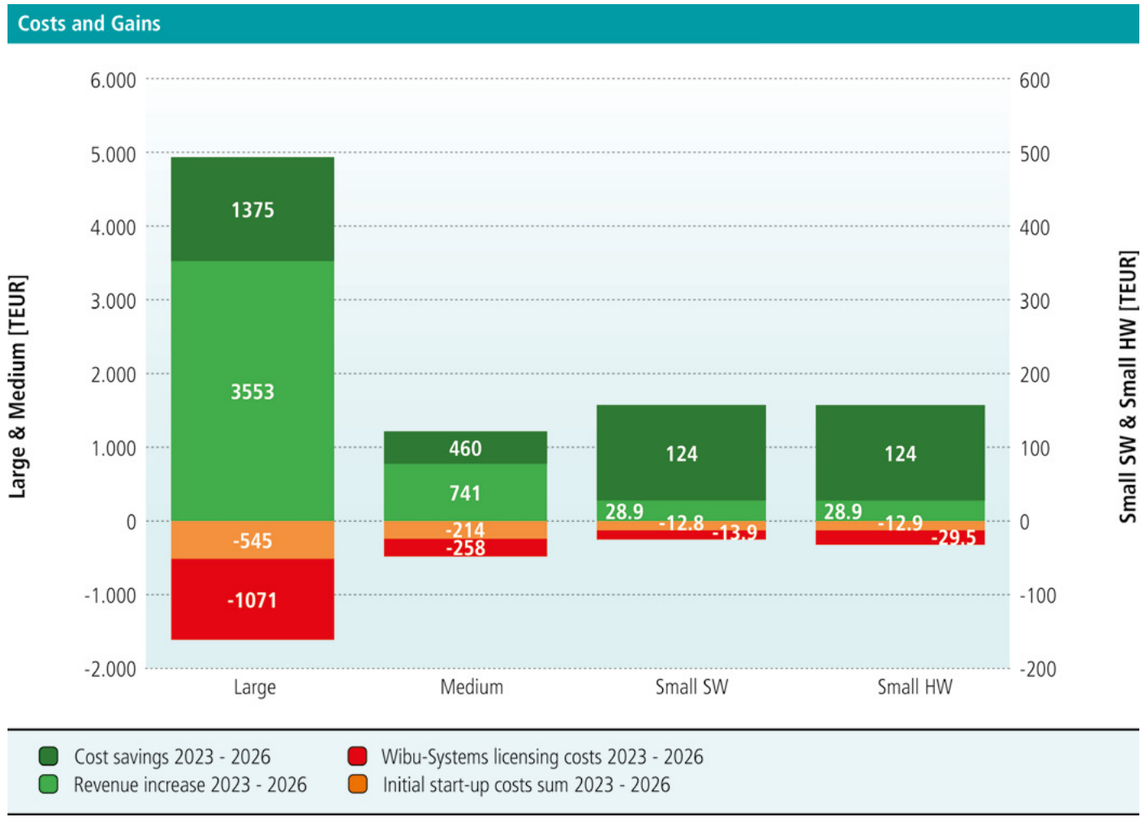

Figure 5: Costs and gains broken down for each customer.

Is it worth it?

Pulling all of the data together, the results of the calculations made by the Wibu-Systems author speak a very plain language: The value of a professionally created and smart protection and licensing system like CodeMeter is immense.

SCAN ME

FOLLOW THE QR CODE TO DOWNLOAD THE FULL WHITE PAPER FROM WIBU-SYSTEMS

The initial ROI calculated by the author for his model corporate-scale business is a full 357% and 405% for the medium-sized business. For the two smaller businesses, that increases even further to no less than 661% and 745%. And that three to sevenfold return on the investment in CodeMeter becomes even better over time, as the initial costs for integrating the licensing system in an established software business amortize over the years and only the regular operating and support costs remain. The author calculates that the breakeven point will be reached reliably within a mere year from buying CodeMeter, and the revenues won as a result continue to grow over the years. (Figures 4 & 5)

Based on these detailed calculations and intensive interviews with actual users, the white paper's conclusions leave no room for any other answer to the age-old make-or-buy question than: "Buy", and then sit back and enjoy the returns. ☒

UNLEASHING the *QUANTUM Frontier*

By Steve Atkins, Silicon Trust

Quantum computing is not just a new chapter in the book of computation; it's an entirely different story. It harnesses the mind-bending principles of quantum mechanics to solve problems previously deemed intractable by classical computers. In this extensive exploration of quantum computing, we will delve into its core principles, theoretical underpinnings, practical applications, current state, and the exciting future it promises.

The Quantum Leap: Understanding Quantum Bits (Qubits)

To embark on our journey through quantum computing, we must first grasp the building block that makes it all possible: the qubit. While a classical bit represents either 0 or 1, a qubit can exist in a superposition of states, effectively representing both 0 and 1 simultaneously. This fundamental property allows quantum computers to process an immense amount of information in parallel.

1. Superposition: Superposition is at the heart of quantum computing. It enables qubits to exist in multiple states at once, exponentially increasing computational capacity. A qubit can be a 0, a 1, or any quantum superposition of these two states.

2. Entanglement: Another remarkable quantum property is entanglement. When two qubits are entangled, their states become interdependent, regardless of the distance between them. A change in one qubit instantly affects the other, a phenomenon that Albert Einstein famously called "spooky action at a distance."

3. Quantum Gates and Circuits: Quantum computations are executed through quantum gates, similar to classical logic gates. These gates manipulate the quantum states of qubits. Sequences of these gates form quantum circuits, where complex computations take place.

Quantum Algorithms and Their Promise

Quantum computing is not just about faster calculations; it is about redefining the boundaries of what's computationally achievable. Several ground-breaking quantum algorithms have emerged, each with unique potential:

1. Shor's Algorithm: Shor's algorithm is a game-changer for cryptography. It can efficiently factor large numbers, a task that classical computers struggle with. This means it poses a significant threat to widely-used encryption schemes, such as RSA.

2. Grover's Algorithm: Grover's algorithm is designed for searching unsorted databases. It can find a specific item in an unsorted list much faster than classical algorithms. This has profound implications for database search and optimization problems.

3. Quantum Machine Learning: Quantum computing promises exponential speedup in machine learning tasks. Algorithms like the quantum support vector machine and quantum neural networks have the potential to revolutionize data analysis, pattern recognition, and optimization.

4. Quantum Simulation: Quantum computers are uniquely suited for simulating complex quantum systems, such as molecules and materials. This has far-reaching implications for drug discovery, materials science, and understanding quantum phenomena.

5. Optimization and Sampling: Quantum computers are poised to solve optimization and sampling problems with remarkable efficiency. Applications span from portfolio optimization in finance to supply chain management.

6. Quantum Cryptography: While quantum computing threatens classical cryptography, it also offers the promise of secure quantum communication through quantum key distribution (QKD). QKD leverages quantum principles to ensure the security of communication channels.

Quantum Hardware: The Nuts and Bolts of Quantum Computing

Quantum processors are the heart of quantum computers, and they come in various forms:

1. Superconducting Qubits: Superconducting qubits are tiny circuits that can carry electrical current without resistance when cooled to extremely low temperatures. They are the foundation of many quantum processors, like those developed by IBM and Google.

2. Trapped Ions: In trapped ion quantum computers, ions are trapped and manipulated using electromagnetic fields. This approach is known for its long qubit coherence times, making it attractive for error-prone quantum systems.

3. Topological Qubits: Topological qubits are more resistant to errors and could become the basis for fault-tolerant quantum computers. Microsoft's approach to quantum computing, using topological qubits, holds great promise.

Challenges in Quantum Computing

Despite the immense promise of quantum computing, significant challenges must be addressed:

1. Decoherence: Decoherence, the loss of quantum information due to environmental factors, remains a significant challenge. Qubits are highly susceptible to noise, and their quantum states can rapidly decay. Extending qubit coherence times is a central research focus.

2. Error Correction: Quantum error correction is a complex process that requires a considerable number of physical qubits to encode a single logical qubit. Implementing robust error correction codes is a key challenge for scaling quantum computers.

3. Scalability: Building large-scale, fault-tolerant quantum computers is a formidable challenge. Overcoming scalability issues requires advances in qubit technology, error correction, and quantum interconnects.

4. Quantum Supremacy: Quantum supremacy, the point at which quantum computers outperform classical computers in certain tasks, is a subject of debate and research. Achieving quantum supremacy demonstrates the practical potential of quantum computing.

The Current State of Quantum Computing

The field of quantum computing is rapidly evolving, and notable progress has been made:

1. Quantum Processors: Leading companies, including IBM, Google, Rigetti, and Intel, have developed quantum processors with tens to hundreds of qubits. These processors are accessible through cloud platforms, allowing researchers and developers to experiment with quantum computations.

2. Quantum Cloud Platforms: Quantum cloud platforms like IBM Quantum Experience and Microsoft Azure Quantum provide access to quantum hardware, allowing researchers to develop and run quantum algorithms.

3. Quantum Algorithms in Action: Quantum algorithms, such as Shor's and Grover's, have been experimentally demonstrated in small-scale setups. They showcase the promise of quantum computing in tackling real-world problems.

4. Quantum Cryptography: Quantum cryptography, including quantum key distribution, has seen practical implementations. Companies are exploring quantum-secure communication methods to address classical cryptography vulnerabilities.

The Future of Quantum Computing

The journey of quantum computing is just beginning, and the future is filled with promise. Here's a glimpse of what lies ahead:

1. Quantum Advantage: As quantum hardware and algorithms advance, we are likely to witness quantum computers outperform classical computers in specific domains. This milestone will highlight the practicality of quantum computing.

2. Quantum Error Correction: Progress in quantum error correction will make large-scale, fault-tolerant quantum computers a reality. This will open the door to solving complex problems across various industries.

3. Quantum Software Ecosystem: An ecosystem of quantum software and applications will flourish, offering solutions for optimization, cryptography, machine learning, and simulations.

4. Quantum Education and Workforce: Quantum computing will require a skilled workforce. Educational programs and initiatives will emerge to train quantum scientists, engineers, and developers.

As well as being the CEO of Krowne Communications, **STEVE ATKINS** *is also the Program Director for the Silicon Trust and Editor of the VAULT magazine (covering hardware-based IC security, biometrics, contactless, blockchain and cloud-based technologies). Even with almost 35 years of experience in the high-tech industry, he is still fascinated with all kinds of technology and the impact it has upon end users. He is currently based in Berlin, Germany.*

5. Quantum-Safe Cryptography: In response to the threat posed by quantum computers to classical cryptography, the development and implementation of quantum-safe cryptographic techniques will become a priority.

6. Quantum Impact on Industries: Quantum computing will have a transformative impact on industries such as finance, healthcare, logistics, and materials science. It will enable innovations, accelerate discoveries, and optimize processes.

The Quantum Revolution

Quantum computing is more than just a technological advance; it is a revolution in the way we approach and solve complex problems. Its potential extends across scientific research, industry, and society at large. As the field of quantum computing continues to grow and mature, it promises to unlock unprecedented computational power and reshape the boundaries of what is possible in the digital age. Quantum computing is the frontier where science fiction meets reality, and its impact will be felt for generations to come.

Quantum Cryptography vs. Post-Quantum Cryptography: Securing Our Digital Future

In an era of rapid technological advancements, the age-old struggle between encryption and decryption has taken on a new dimension. The advent of quantum computing has brought both excitement and trepidation to the field of cryptography. Quantum computers have the potential to crack widely used encryption methods, rendering traditional cryptography vulnerable. In response, a new branch of cryptography, known as post-quantum cryptography, is emerging to address these challenges and ensure our digital security. In this comprehensive exploration, we will delve into the core principles of quantum cryptography, the threat posed by quantum computers, the emergence of post-quantum cryptography, and the implications for the future of secure communication.

Quantum Cryptography: The Quantum Advantage

Quantum cryptography is rooted in the principles of quantum mechanics. It harnesses the unique properties of quantum bits, or qubits, such as superposition and entanglement, to create cryptographic protocols that offer unprecedented security.

At the heart of quantum cryptography lies Quantum Key Distribution (QKD). QKD allows two parties to securely exchange encryption keys, preventing eavesdroppers from intercepting the key without detection. The most famous QKD protocol is the BBM92 protocol, developed by Charles Bennett and Gilles Brassard in 1992.

The security of quantum cryptography protocols is founded on the principles of Heisenberg's uncertainty principle. Attempting to measure a qubit in superposition disturbs its state, making it impossible for eavesdroppers to gain any information without being detected.

The BB84 protocol, also known as the quantum coin toss, is a fundamental quantum cryptography protocol. It enables two parties to exchange a random, secret key over a potentially insecure channel. Any attempt by an eavesdropper to intercept the key will disturb the quantum states, alerting the legitimate parties to the breach.

Quantum cryptography has practical applications in secure communication, ensuring the confidentiality and integrity of transmitted data. It is used in secure financial transactions, government communications, and even in protecting critical infrastructure.

The Quantum Threat: Shor's Algorithm

While quantum cryptography promises to enhance security, the advent of quantum computers brings a significant threat to traditional encryption methods. Shor's algorithm, developed by Peter Shor in 1994, is a quantum algorithm that can efficiently factor large numbers.

RSA encryption, a widely used public-key cryptography system, relies on the difficulty of factoring large numbers. Shor's algorithm can factor large numbers exponentially faster than classical computers, posing a severe threat to RSA encryption.

The potential decryption of RSA keys by quantum computers has raised concerns about the future of public-key cryptography. The security of many online transactions, communications, and data storage systems relies on RSA encryption.

Post-Quantum Cryptography: Fortifying Our Digital Armor

Recognizing the looming threat of quantum computers, the field of post-quantum cryptography has emerged. Post-quantum cryptography aims to develop cryptographic systems that are secure against both classical and quantum attacks.

One of the leading candidates in post-quantum cryptography

is lattice-based cryptography. It relies on the mathematical structure of lattices to create secure encryption schemes. Lattice-based cryptography offers a high degree of security and is considered quantum-resistant.

Code-based cryptography is another approach. It uses error-correcting codes to create secure encryption systems. Even if quantum computers can solve the hidden subgroup problem, a core component of many quantum attacks, they would still struggle to break code-based encryption.

Hash-based cryptography is a robust post-quantum approach. It relies on one-way functions and hash functions to secure data. These cryptographic systems offer a level of security that is believed to be resistant to quantum attacks.

Multivariate polynomial cryptography is based on the difficulty of solving systems of multivariate polynomial equations. Quantum computers would face formidable challenges in breaking this form of encryption.

Post-quantum cryptography, while promising, presents several challenges. It must not only provide robust security against quantum attacks but also be efficient, practical, and ready for real-world implementation. Balancing these factors is a complex task.

Preparing for the Quantum World

As quantum computers advance, organizations and individuals must prepare for the post-quantum era. Transitioning to quantum-safe cryptographic methods is essential to protect sensitive data and secure communications.

Key management is a crucial aspect of preparing for the quantum world. Organizations must develop strategies for securely storing and distributing cryptographic keys. Quantum key distribution (QKD) is one of the promising quantum-safe methods for key exchange.

Security awareness and education are essential for preparing for the quantum threat. Educating users about the implications of quantum computing on data security and privacy is vital. Organizations and governments must invest in the development and deployment of quantum-resistant cryptographic solutions. This involves not only updating encryption methods but also ensuring that hardware and software are ready for the post-quantum era. Quantum-resistant cryptography is a dynamic field that requires collaboration among researchers, cryptographers, governments, and organizations. Ongoing research is essential to stay ahead of emerging threats.

Securing Our Quantum Future

NIST's Post-Quantum Cryptography Standardization Effort

The National Institute of Standards and Technology (NIST) in the United States has taken a pioneering role in post-quantum cryptography. NIST's Post-Quantum Cryptography Standardization Project is an ongoing effort to solicit, evaluate, and standardize quantum-resistant cryptographic algorithms.

NIST's project has attracted a wide range of post-quantum cryptography candidates, including lattice-based, code-based, hash-based, and multivariate polynomial approaches. This diversity reflects the complexity of finding a post-quantum solution.

NIST is currently in the third round of its standardization project, where it has selected a smaller set of candidates for further evaluation. The selection process is rigorous, focusing on security, efficiency, and practicality.

NIST's efforts in post-quantum cryptography standardization will significantly influence the future of cryptographic practices across industries, governments, and organizations. The standardized algorithms will form the basis of secure communication in the quantum era.

The intersection of quantum computing and cryptography presents a remarkable challenge and opportunity. Quantum cryptography harnesses the principles of quantum mechanics to create secure communication methods. However, the advent of quantum computers threatens traditional encryption schemes. In response, post-quantum cryptography is emerging as a robust defence against quantum attacks.

The field of quantum cryptography is at an exciting juncture, with practical implementations and growing relevance in secure communication. On the other hand, post-quantum cryptography is a critical field of study that will significantly influence the future of digital security.

As we move into the quantum era, the importance of preparing for quantum threats cannot be overstated. The transition to quantum-safe cryptographic methods, key management, security awareness, quantum-resistant implementations, and collaboration are essential elements of securing our digital future.

The world of cryptography is evolving, and the key to success lies in adapting to these changes, staying vigilant, and working collectively to ensure the continued security and privacy of our digital lives. ☒

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.microp ross.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

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

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

SECURITY
LICENSING
PERFECTION IN PROTECTION