NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

1999–2024 / 25 YEARS

The VAULT

25 YEARS OF THE SILICON TRUST

Contents

Imprint

THE VAULT ISSUE 1999–2024 / 25 Years
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: Decmber 2024.

THIS *is* *the* END

By **Steve Atkins**
Program Director - The Silicon Trust

It's a little dramatic to begin this final editorial in such a way but hey, Adele started it (opening lyrics to Skyfall) and it does seem appropriate at this time of writing. The fact is – it's true. This is the final issue of the VAULT magazine as it celebrates 25 years. However, it also marks the end of the Silicon Trust Partner Program (to give it its full title).

Why is the program closing down you ask? Well, many reasons, but predominantly it has outlived its usefulness and perceived return on investment to the partners. I cannot blame them – its inception belongs to a time in the industry over a quarter of a century ago that was very, very, different to now.

When we started, no small start-up or mid growth company could afford to compete with the networking and marketing opportunities that existed for the large-scale corporations at the time. The cost of full-scale marketing and promotion was prohibitive and limited resources better spent on new product and technology development. The program offered a way to create credibility by association across different companies and create a push/pull strategy by encouraging end customers to see the benefit of the new technologies on offer and endorsed by a third-party program. But always with hardware-based technology as a starting point for secure applications.

At the start of the program the newest technology we covered was Biometrics. The first product we highlighted was a biometric fingerprint sensor from Infineon (or Siemens Semiconductor as was). The possibilities for this technology seemed endless and we were not above forecasting how these technologies could be incorporated into everyday products.

I, for one, remember vividly, a conversation held at dinner during one CARTES event in Paris in the early days, between Thomas Rosteck, Veronica Preysing and Mark Stafford of Infineon and myself, where we fantasized about the possibility of having a separate biometric sensor installed into the future series of Nokia phones. Little did we know that only ten years later (in 2012) Apple's iPhone 5 would use a biometric sensor in the screen and only five years after that, facial recognition would be installed as a standard security protocol – inconceivable at the time. Sorry Nokia – no-one foresaw Apple taking over your market space.

And that's how it continued. One new technology after another; 32 Bit Secure Controllers, PKI, external secure dongles, Trusted Platform Modules, cyber-security systems, contactless technology, Near Field Communication, IoT, Blockchain, Non-Fungible Tokens, Artificial Intelligence, Quantum Computing, Post-Quantum Cryptography, and so on.

And the markets grew. First with secure documents, ePassports, eID cards, mobile driving licenses and then on to contactless payments, contactless ticketing, border management, and secure access control. The list and opportunities were endless.

The original SECURE Magazine evolved into the VAULT magazine after 15 issues and one rebrand of the program, and continued as the VAULT for the next 40 issues. During this time the program brought out whitepapers, application briefs, geographical specials, video interviews and even a short stint as Security-News TV. Not to mention the numerous product seminars and meeting held over the last couple of decades both in-person and on-line.

Today the situation is very different. Amalgamations and merges have seen small companies pulled into bigger ones. Large companies in the industry became giants and even some of those giants are now starting to divest themselves of their security divisions and business units.

While we continue to see this sea of change in the players and infrastructure within the industry, we have also witnessed the now incredible plethora of available online tools, allowing even the smallest of companies to market their technologies, products and solutions by themselves. Social media, video platforms, networking sites, online analytics, Artificial Intelligence tools – all contribute to bring the promise of market penetration and customer awareness well within the grasp of smaller companies who are looking to go it alone, on their own terms.

Put simply – the Silicon Trust Partner Program, while invaluable in its time, has today a less viable argument for what it can offer as a network. Time and technology will catch up to all of us eventually.

More importantly however, this journey was not made alone. The support and contributions from a number of key partners over the last 25 years have made this experience a little smoother than it would have been otherwise. I would like to single a few of these people out; from Infineon – Ulrich Hamann, Rainer Bergmann, Thomas Rosteck, Ioannis Kabitoglou, Anton Müller, Ursula Schilling, Markus Moesenbacher, Chris Shire, Karin Grassmann, Stefanie Eisele, Camille Gasnier, Florence Raguet, Robert Bach, Dr Peter Laackmann, Markus Janke & Detlef Houdeau. Some of these individuals still work at Infineon, others have moved on, some have even retired – but we wanted to acknowledge their contributions none-the-less.

From our partner side there are Oliver Winzenried, Marcellus Buchheit, Daniela Previtali, Klaus Schmeh, Markus Hoffmeister, Adam Ross, Benjamin Drisch, Dirk Melzer, Susanne Timm, Dr. Hans Hanauer, Lutz Richter, Katharina Schuldt and Dr. Joseph Atick. A big thank you goes out to them for their contributions over the years.

There are, of course, many, many more individuals who have contributed to the program during its time in existance. More than could be mentioned here in this editorial. You know who you are. We know who you are. And so, thank you.

In this anniversary issue, we have looked back through our archives and brought back some articles that were considered fundamental at the time. The issue is divided into three parts; Technology Over Time, Application Evolution and Market Maturity.

We have republished our first guest opinion piece from Ulrich Hamann, talking about the need for hardware-based security, that created the direction for the program. The interview with Intel's security architect David Grawrock explaining TPM and why the TCPA was so important, back in the early 2000's. As was the first time we asked about the growing markets for eHealth cards or looked towards secure travel with ePassports and eID documents. We announced the arrival of NFC and contactless technology, of Blockchain and NFT's, and of the need during, and after, the COVID pandemic for biometric contactless payment cards. We even took a moment (back in 2015), to ask about the current security trends in the semiconductor industry. Just in case our readers thought we were veering too far towards software-based secured solutions and away from hardware-based secured ones.

I was recently told that 'No-one cares about what has happened in the past'. This is certainly a view that many newcomers to the industry embrace. Looking at technology, applications and markets even just five years ago seems almost anachronistic to these individuals, and they may indeed have a point. After all, this is an industry that must, above all else, strive to move forward (if only to stay one step ahead of potential security hacks). But this issue isn't for them. It's for those of us who are now at a point where we can afford to take a moment and see how far we've come.

Just in case though, we have also republished more recent articles looking at AI and PQC – just to keep it within the all-important five-year timeframe. And furthermore, we have two brand new contributions to this issue. Our last guest opinion by Wibu-Systems' Oliver Winzeried and a final look at a topic that became one of our focus markets: Smart Travel (courtesy of Mühlbauer's Katharina Schuldt). Thereby covering the triumvirate of past, present and future.

Before I end though, this editorial would be incomplete if I did not acknowledge the amount of work done by those behind the scenes. Those Krowne Communications members who over the years have also contributed to the program, either in an editorial and publishing capacity or through partner management and event facilitation. Some no longer work at Krowne, having moved on in their career many years ago, other are still around. For their creative services, I would like to acknowledge Wendy Atkins, Stefan Gassner, Andreas Speck, Lana Petersen and Nina Eggemann. On the program management side, I would like to thanks Karen Brindley, Nicole Mountain, Contance Rogg, Veronica Preysing, and Yvonne Runge. These people have been the powerhouse behind the program; keeping it on course from the very beginning. Without their focus and patience, the program would not have lasted as long as it did.

The website continues to pull in an impressive number of visitors and so we will keep our online presence alive for 2025. Should anyone have news or articles that they would like to share online, please feel free to submit them and we will be happy to post them up and let them ripple through our network platforms. You're welcome.

And so, as they say, we have reached the end.

Thanks for sticking around.

It was fun.

Steve Atkins

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.*

Security Hardware – the key to unlocking new markets

By Ulrich Hamann, Senior Vice President and General Manager. Security and Chip Card ICs. Infineon Technologies AG, Munich

Applications such as e-commerce, virtual private networks and many others will only really take off once the appropriate infrastructure of security hardware is in place and we can move around safely in the digital world. System manufacturers must integrate security hardware as standard in their equipment before they can provide their customers with the basis required for the true information age in which sensitive data is safe.

Our world is moving faster today than ever before. It took radio 38 years to reach an audience of 50 million worldwide, and television 13 years, but the Internet has gone from nothing to 50 million surfers in only four years. There are now 300 million people using the Web and the figure is increasing by 200,000 every day across the globe.

Despite these impressive figures, electronic commerce is still developing very slowly. Of course, there may well be the odd content and design error here and there, but they cannot be held responsible as the main reason for the sluggish growth of cyberbusiness. The true reason for surfers' reticence when it comes to e-commerce is the absence of secure data transmission. Manfred Krüger, CEO of Euro Card Systems, a company that manages primarily the brands Eurocard/Mastercard, reports that almost ten percent of Internet credit card transactions are fraudulent, and that the number is increasing. Overall, credit card fraud on the Internet is ten times more prevalent than traditional signature fraud in the real world.

"In the future, each complex system will be able to check its own reliability using the chips integrated in the individual components."

Security in the digital world, i.e. being able to accurately identify business partners and transmit data without it being corrupted, is the only basis on which to establish and consolidate practical Internet business. Just as in the automotive industry, following the introduction of seat belts in all new cars, additional safety features such as ABS, the airbag, ESP, increased passenger safety, etc. became increasingly influential sales arguments, so too will the security hardware of PCs, PDAs and mobile phones become a basic requirement for the consumer - but far more quickly. The chips used for these security features or, more accurately, the security ICs, are not only of great benefit for private e-commerce and safe e-mail, but also for the professional sector. They close the massive security gap that exists at the moment in applications such as VPNs (Virtual Private Network) and remote access. They also have other industrial uses in addition to access control. In the future, each complex system will be able to check its own reliability using the chips integrated in the individual components. Again, we can use the automotive industry as an example, where not only are anti-theft devices of particular interest from a security point of view, but they are also now being used to check that the vehicle is using the spare parts specially designed for it (a concept known as "car system integrity").

"There are no secrets on a standard PC without security hardware."

At the moment, data encryption with PCs and PDAs takes place in the PC or PDA processor itself. These processors are freely programmable and grant every program access to the data in their registers. Since the key must be stored in plaintext in a register of the processor during the encryption process, this type of software encryption almost invites hackers to discover the key. Once a hacker is in possession of the key, he has unlimited access to sensitive data. Just how susceptible PCs are to Trojan horses and viruses was clearly demonstrated by the "ILOVEYOU" virus recently. Indeed, there is one thing that every PC user should be aware of: that there are no secrets on a standard PC without security hardware.

In contrast to conventional processors, security ICs and chip card ICs cannot be reprogrammed, so they represent a virus-free environment for security applications. They permit the secure storage of secret keys and therefore the reliable exchange of non-adjustable data, whose senders and receivers can accurately identify themselves. The identity of the person using the security hardware can be determined by the hardware itself by means of biometry ICs. For example, Infineon's FingerTIP™ reads the fingerprint of its registered users.

It is essential for any cryptographic procedure to keep the data encryption keys secret. For this reason, the key data are only managed and modified in the security hardware when using specific security ICs, whereas with software encryption, the keys are processed in the normal PC processor. It is this that makes software encryption solutions so vulnerable.

Security and chip card ICs from Infineon Technologies also have special built-in protection against physical attacks. Neither statistical analysis of the electromagnetic radiation of the IC or its power supply, for instance, nor extremely costly systematic abrasion and analysis of the chip would reveal the key.

The "public key procedure" can be used for digital signatures to conduct legally binding business transactions on the Internet in exactly the same way as with a real signature on a paper contract. A personal pair of keys, consisting of the public key and the private key, is generated for each user by a trust center or by the random number generator of the chip card controller. While the public key can be issued at will, the user keeps the private key, safely stored on the chip card, secret. Only the chip card, protected against unauthorized access, can be used to decode data encrypted with the public key into plaintext. Data records that have been digitally signed using the private key (discernible with the aid of the public key) can therefore logically only originate from one person, namely the authorized card owner.

Infineon technologies

The chip card ICs that are used for this type of application must fulfill strict requirements. As the first chip card controller worldwide, the SLE66CX160S from Infineon Technologies meets all the requirements of security level E4/"high-level" efficiency according to the ITSEC (Information Technology Security Evaluation Criteria). It is therefore the only chip card controller at present that satisfies the extremely stringent security requirements of the German signature law for digital signatures.

"The "public key procedure" can be used for digital signatures to conduct legally binding business transactions on the Internet in exactly the same way as with a real signature on a paper contract."

Nowadays, we cannot imagine secure data transmission without chip cards with security controllers. If we take a closer look at the latest chip card controller from Infineon Technologies, the 16-bit SLE66CX640P from the 66Plus family, we see that it is a true master of the art of encryption and decoding. It processes RSA algorithms with key lengths of up to 2048 bits in a fraction of a second. It would take several of the most powerful computers, months to convert a message encoded in this way into plaintext.

Of course, in theory, any code or key can be "cracked", but only with infinite time and effort. Together with researchers at the INRIA (National Research Institute for Computer Sciences and Control in France), the Irish mathematician Robert Harley calculated an ECC key encoded with 108 bits. After intensive statistical calculations, which reduced the number of possible keys to a mere tenth of the original volume, the scientists ran 9,300 computers in parallel via the Internet non-stop for more than four months. Extrapolated to one PC with a clock speed of 450 MHz, this gives a turnaround time in the region of 500 years. If the ECC key were converted with 108 bits to the quasi-standard of private key encryption, namely the RSA algorithm, it would still be around 600 bits long. Almost quadrupling the key (to 2048-bit RSA, as with the 66Plus family from Infineon Technologies) however, not only quadruples the turnaround time from 500 years to 2000 years, but also increases it by a multiple. From a statistical point of view, a hacker using a 450 MHz PC would not in practice be able to crack a data packet encrypted with an Infineon chip from the 66Plus family (2048-bit key length).

This example shows that the chips of the 66Plus family are cryptographically secure for day-to-day use both now and in the future. However, in pursuit of their aim to rule out fraudulent attacks altogether, Infineon Technologies will this year launch the 88 series chip card controllers with two 32-bit processors integrated on one piece of silicon, which drastically increases the encryption computing speed.

"From a statistical point of view, a hacker using a 450 MHz PC would not in practice be able to crack a data packet encrypted with an Infineon chip from the 66Plus family (2048-bit key length)."

When it comes to encrypting large volumes of data online, however, the chip card is stretched to its limit, as it only communicates with the outside world via one serial 115 Kbit/s interface. It is at precisely this point that the USB token attacks the security chip. In principle, this is the entire security hardware, as on a chip card. Instead of the slow serial interface, the USB token has a monolithically integrated USB interface which enables data exchange at 12 Mbit/s. The USB token is therefore also suited to the online encryption of large data volumes. If secure data transmission with a PC that runs under Windows 98/2000 is required, the USB token is a fast and, ultimately, cost-effective solution, since the USB interface already exists, whereas the chip card would require a separate reading device.

The Bayon™ security chip is even faster: it permits all the data on the hard drive of a computer to be stored encrypted. The cryptographic keys for the hard drive data are saved on the owner's personal chip card with which the Bayon™ communicates in encrypted form. Should unauthorized access be gained to the hard drive, the data stored on it is still inaccessible because the key stored securely on the chip card is required. The advantage of the Bayon™ is that because of its high data throughput, it is possible to work normally and quickly with the PC. As more and more notebooks are stolen on business trips, the Bayon™ is particularly interesting, since the hard drives of such computers normally contain extremely sensitive data.

Until now, most applications have required a PIN (Personal Identification Number) in addition to the security hardware (chip card, USB token or other security ICs). The FingerTIP™ sensor from Infineon Technologies considerably increases the level of security, as only the personal fingerprint permits access to the chip card. It is therefore no longer necessary to remember various PINs or write them down in supposedly safe places such as diaries, or on bits of paper in a briefcase. This sensor already has multiple uses today, ranging from physical access control, e.g. to a house or car, and logical access control to networks (intranet, Internet, etc.), right through to ensuring that each person only uses a particular service once, a functionality that is of particular interest for social welfare offices.

The next step is to produce a 10 µm, flexible chip for the FingerTIP™ sensor, which gives the ICs characteristics more akin to a piece of paper than an IC. This physical flexibility enables the FingerTIP™ sensor, despite its large surface area of approximately 1.5 cm^2, to be integrated on a chip card without the risk of destroying the sensor when it is used. Thin chips are not only about flexible silicon; they also provide additional security. By "stacking" and "sticking" (vertical system integration) individual wafer-thin ICs manufactured using different technologies, the structures of the complete module become even more complex and thus more resistant to physical attacks.

In the future, new technologies and processes will facilitate the manufacture of even smaller chips, whose production costs will be much lower than they are today. Such chips are predestined for one-time applications, such as in a day-to-day business environment, or specially programmed chips that are integrated in normal paper and fulfil a range of security functions such as effective copy protection or even simply a tamper-proof "watermark".

Thanks to new technologies and wafer-thin ICs, the chip card of tomorrow will include far more components than simply the security controller and a FingerTIP™ sensor (and an antenna with contactless cards). Soon, a display, a keypad, a loudspeaker, a battery, a solar cell or other biosensors will be integrated in the card. Infineon Technologies is already moving in this direction, as was evident at the Card Tech / Secur Tech 2000 show in Miami, where the prototype of a chip card with integrated FingerTIP™ sensor and liquid crystal display was presented for the first time. If we consider the synergies between polymer electronics and displays, as well as between polymer membrane batteries and sensor elements, the possibilities are even more exciting. For example, moving away from segment display to full-card graphical display: not only will it be able to show video images in very good quality, it will also act as a touch screen.

Secure hardware (security ICs, chip cards, etc.) offers the basis for secure movement in the digital world but needs the appropriate security software. The software should no longer be oriented simply towards a particular operating system, but generally towards open platforms, and should be compatible with the most diverse applications. It is ultimately the market that decides which of the many applications emerge victorious. For this reason, Infineon Technologies security and chip card ICs support not only Java but also Windows for Smart Cards and Multos.

"The great advantage of the new ICs with open operating systems is that any suitably qualified engineer can develop applications that can be used worldwide."

In future, there will be more and more open operating systems for Smartcards, instead of the predominantly proprietary ones found today. Infineon Technologies is assuming that the open platforms will have a market share of over 50 % in a few years' time. To support this open software concept, the controllers of the 88 family, for example, have a Memory Management Unit (MMU) to partition individual applications and manage them separately. Thus they can also function independently alongside each other.

The great advantage of the new ICs with open operating systems is that any suitably qualified engineer can develop applications that can be used worldwide. For example, applications can be downloaded via the GSM network if the card or the chip is installed in a GSM telephone. A typical scenario of the chip card of tomorrow could be a traveler who downloads a ticket for, say, the London underground system either via the Internet at home or via the chip card in his mobile phone on the way to the airport. The downloaded electronic ticket, obviously already paid for, is then read directly by the access control system in London. This on-site access control could even be offline, as it would only be able to read the anonymous ticket and would therefore not require a connection to a central computer.

The market for security solutions will grow tremendously - even more than in the last few years. Between 1987 and 2000, the worldwide turn-over for the overall market for security and chip card ICs grew from 13 million Euros to 1.3 billion Euros, which corresponds to an annual growth rate of around 42%. By the year 2005, though, it will have grown by a further 50 % every year, so that in 2005, the overall market value in security and chip card ICs will be 9.7 billion Euros. Europe's share as a sales market will decrase from the current 55% to 30%, but Asia will experience a particularly large increase in the market for security and chip card ICs: although only small volumes are supplied to Southeast Asia and Japan at present, these regions will have a market share of 21% (Asia-Pacific, in excess of 2 billion Euro) and 12 % (Japan, around 1.2 billion Euro) in the year 2005. For this exponential growth to be possible, Infineon Technologies engineers across the world are currently working hard with our own teams and those of our customers to develop revolutionary solutions.

It must never be forgotten that security is not static, but dynamic. Security means being at least two generations ahead of even the best hackers. For this reason, Infineon Technologies is already working on tomorrow's security solutions, ensuring that the amount of time and money required for a'successful' attack will systematically eradicate them altogether.

Bill Gates, Microsoft and Ulrich Hamann, Infineon Technologies meet at Redmond after Microsoft announces its entry into the Smart Card arena with its Windows for Smart Cards (WfSC)

Preparing for THE FUTURE of *CYBERSECURITY: Navigating* NEW FRONTIERS and *protecting* what MATTERS

By Oliver Winzenried, CEO and Founder, WIBU-SYSTEMS AG

As technology evolves at an unprecedented rate, groundbreaking innovations such as quantum computing, synthetic biology, and brain-computer interfaces (BCIs) are set to reshape industries and redefine everyday life. However, each of these advancements brings new cybersecurity challenges that, if unaddressed, could have serious implications for individuals, businesses, and society.

In this article, we delve into six emerging technologies on the horizon, exploring the opportunities and cybersecurity risks they bring, and examining how Wibu-Systems can support and protect these developments with innovative solutions.

1. Quantum Computing

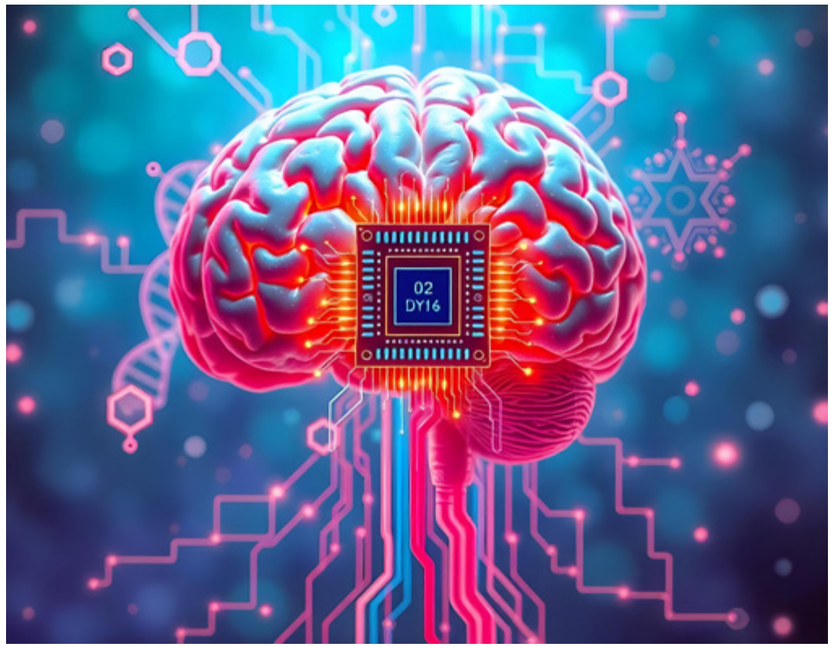
Quantum computing promises to be one of the most transformative advancements of our time, offering the potential to solve complex problems beyond the scope of traditional computers. Fields such as cryptography, climate modeling, and drug discovery could be revolutionized by its speed and processing power. However, quantum computing's power also presents risks: existing encryption standards, the backbone of modern cybersecurity, could become vulnerable.

The impact of quantum computing is twofold. In an ideal scenario, organizations proactively adopt quantum-resistant algorithms to keep data secure while benefiting from quantum's computational capabilities. However, if the development of quantum outpaces defense measures, it could lead to a cybersecurity crisis, potentially exposing sensitive information on a global scale. Wibu-Systems is actively preparing for this future by exploring quantum-resistant encryption for its solutions. By enhancing CodeMeter, its flagship technology, to counter quantum-based threats, Wibu-Systems is committed to ensuring data security for the post-quantum era.

2. Synthetic Biology and DNA Data Storage

Synthetic biology and DNA data storage represent a frontier in biotechnology, with potential applications in healthcare, environmental restoration, and data preservation. Through synthetic biology, scientists can design new organisms to address specific challenges, from waste consumption to resource production. DNA data storage, meanwhile, offers vast potential as an efficient, long-term medium with low energy needs.

However, synthetic biology raises concerns about intellectual property and biosecurity, as any vulnerability in the systems managing engineered organisms or storing DNA data could lead to unauthorized access or misuse. A future where synthetic biology is widely used could mean that sensitive bioinformatics and proprietary engineering techniques require protection from cyber threats. Wibu-Systems could secure synthetic biology applications and DNA storage solutions by managing access to software used in these fields, ensuring that only authorized users can interact with sensitive bioengineering processes or retrieve data from DNA storage.



3. Neuromorphic Computing

Neuromorphic computing, modeled after the human brain, enables highly efficient processing and self-learning capabilities. This technology has potential applications in autonomous vehicles, robotics, and real-time IoT, with the ability to process data quickly and with low energy demands. However, neuromorphic systems face unique cybersecurity challenges, as they require specialized security measures that go beyond traditional computing.

In the best scenario, neuromorphic computing enables smarter, faster systems across industries without compromising security. However, if neuromorphic devices lack adequate protections, they could be susceptible to unauthorized control or data manipulation, particularly in applications like autonomous vehicles or industrial machinery. Wibu-Systems can support the secure deployment of neuromorphic systems by managing licenses and access to applications running on neuromorphic hardware. CodeMeter can also facilitate secure updates, helping manufacturers and operators protect neuromorphic devices from cyber threats as they become more integral to daily operations.

4. Brain-Computer Interfaces (BCIs)

Brain-computer interfaces (BCIs) are emerging as a transformative technology that enables direct communication between the brain and digital devices. BCIs have potential applications in healthcare, gaming, and beyond, offering new ways to assist individuals with disabilities or enhance human cognition. However, BCIs also introduce a unique set of cybersecurity risks, as they involve sensitive neural data that could be manipulated or accessed by unauthorized parties.

With secure deployment, BCIs could improve accessibility and provide users with new capabilities. But in a worst-case scenario, cybercriminals could exploit vulnerabilities in BCI systems to manipulate or extract neural data. Wibu-Systems could play a vital role in securing BCI applications by using CodeMeter to manage licenses and protect access to software controlling BCIs. This ensures that only authenticated, authorized users can interact with these sensitive systems, protecting both the user's privacy and the integrity of neural data.

5. Tokenized Economies and Decentralized Autonomous Organizations (DAOs)

Tokenized economies and DAOs are redefining how communities and organizations govern and participate in economic activities. By using tokens and blockchain technology, DAOs enable decentralized decision-making and allow participants to hold a direct stake in the organizations they engage with. However, as DAOs and tokenized economies grow, they face new cybersecurity challenges around smart contract security, fraud prevention, and data integrity.

In a positive scenario, tokenized economies could offer new models for governance and economic participation, making communities more inclusive and resilient. However, without adequate security, DAOs could be vulnerable to hacks and fraud, potentially leading to financial loss for participants and instability within these digital communities. Wibu-Systems could support the secure operation of tokenized economies by providing solutions that protect smart contracts and manage licenses for DAO-related software. By ensuring that only verified participants can interact with these systems, CodeMeter can help preserve the integrity and security of tokenized ecosystems.

6. Critical Infrastructure and Cyber Resilience

The increasing digitalization of critical infrastructure—such as power grids, water systems, and transportation networks—has improved efficiency and service reliability. However, it has also introduced new vulnerabilities, making these systems prime targets for cybercriminals and state-sponsored attacks. A breach in critical infrastructure can lead to widespread service disruptions, with severe consequences for public safety and economic stability.

In a secure future, critical infrastructure would be cyber-resilient, ensuring that essential services remain operational even under attack. But without sufficient defenses, these systems could become highly vulnerable, jeopardizing public safety and disrupting entire communities. Wibu-Systems is well-positioned to support critical infrastructure providers with CodeMeter's robust software protection and access control capabilities. By embedding security within software licenses and enforcing strict authentication, Wibu-Systems helps secure critical infrastructure and protect essential services from potential cyber threats.

OLIVER WINZENRIED *began his entrepreneurial career immediately after completing his studies, and focused on electronic and ASIC design, hardware, microcontroller and embedded application development for consumer electronics, automotive and industrial engineering. With Marcellus Buchheit at his side, he founded Wibu-Systems in 1989, and remains the company's CEO to this day.*

Securing the future demands a foundation of trust, collaboration, and proactive security.

Trustworthy AI, reliable electronics, and human-centric security and cyber hygiene practices will empower individuals and reinforce confidence in technology. Meanwhile, securing the supply chain and implementing Zero Trust Architecture will prevent vulnerabilities across complex digital ecosystems. Digital sovereignty will allow organizations to maintain control over critical data and infrastructure, enhancing resilience. Achieving these goals requires sustained research and development by both private and public sectors, driving innovative cybersecurity solutions. Together, these efforts will shape a secure and trustworthy digital future. ⊠

Faster *PROCESSING* through SMART SYSTEMS

By Katharina Schuldt, Muehlbauer Group

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

Muehlbauer's Seamless Travel Corridor represents a groundbreaking approach to border crossing, allowing travelers to navigate security with minimal interaction and no need to show documents. Travelers simply walk through the corridor without stopping – and perhaps without even noticing, and are recognized and identified by the smart frame. This innovative system utilizes advanced machine learning, artificial intelligence technologies and image processing for efficient background processing, employing facial identification and person re-identification with tracking capabilities.

Designed for a small footprint, the Seamless Travel Corridor can be easily deployed across various locations, including airports, land borders, and seaports, all while prioritizing security and privacy by design. The system uses multiple high-resolution cameras – typically three –, which provide high-quality images with fast transmission speeds (less than 30 milliseconds possible). Ensuring flexibility in deployment, it supports various standard protocols such as USB and RTSP, as well as a specially developed Muehlbauer high-speed protocol that communicates over a 10 Gbps network and can handle video streaming in 4k without any compression on the image. With low communication latencies, the visualizer software enables near real-time image monitoring via tablet or computer using a web service.

Its ability to capture individuals in random group formations – regardless of active cooperation – greatly enhances its effectiveness. The system can detect persons at distances of up to 12 meters, track and match faces up to 8 meters away (with a standard of 7 meters), achieving throughput rates three times greater than traditional eGates within the same physical space.

The pre-registration prior to crossing the corridor is possible with electronic Machine Readable Travel Documents (eMRTD) or digital IDs (such as mobile Driver's Licenses, Digital Travel Credentials, or Digital Travel Authorizations). The Seamless Travel Corridor can be seamlessly integrated with existing Border Management Systems (BMS), ensuring a smooth transition to more efficient border control practices.

Moreover, this system is cost-effective, using compact hardware for processing without the need for a full server. The corridor can be installed in blocks or segments, allowing for customization based on spatial configurations, and the models are self-trained using data that is completely free of licensing costs.

This innovative solution not only revolutionizes border management but also enhances the overall travel experience, ensuring both security and efficiency. ☒

SmartUSB The Integrated Solution for Personal IT Security

By The Silicon Trust

Today, Smart Card products mainly provide personal IT-security. These Smart Cards give access to corporate IT-networks and support RSA-cryptography for digital signature purposes. Although Smart Cards are quite cheap, the final cost of ownership is much higher due to the fact that each PC and workstation need to have a Smart Card reader installed to communicate with the Smart Card. A readerless solution could significantly reduce the cost of ownership and at the same time drastically increase the market demand for such solutions.

USB-Tokens also known as USB-Dongles are one alternative. Another solution will be USB-Smart Cards. Both devices can be connected to a PC using the standard USB-interface, which is widely spread in all PCs installed in the field and implemented in every PC currently shipped. Thus the need to install an expensive Smart Card reader does not exist anymore. The USB-Dongles can be directly plugged into a PC's USB-port while an USB-Smart Card only needs a simple and cheap connector to be connected to USB.

Schlumberger announced the rollout of the first dual-interface USB/ISO-Smart Cards during the second half of 2001. USB-Dongles are in the field already. The market lift-off of this new form factor is currently taking place.

The success of both form factors – USB-Smart Card and USB-Dongle - mainly depends upon solving the problem of the integration of an USB-interface into a secure Chip Card controller. SmartUSB is Infineon's solution to this particular problem. SmartUSB will significantly reduce the bill of material for USB-Dongles. This is the basic prerequisite for the market success of USB-Dongles. But SmartUSB will also allow the simple integration of an USB-interface on a Smart Card.

SmartUSB - The Product

SmartUSB combines the security of Infineon's ITSEC E4 High certified SLE66CX640P Controller with the speed of USB. The integration of a USB-interface provides a powerful single chip solution for USB-Tokens such as Dongles and USB-Smart Cards.

Beside the USB-interface there is still the standard Smart Card ISO7816-interface available. The combination of both interfaces on one chip allows a simple integration of a Dual-Interface USB/ISO-Smart Card. Such a Smart Card will be fully compliant to ISO7816 on the one hand, while on the other; the USB-interface will provide easy and high speed-connectivity to the IT world. So the requirements of both current existing infrastructures – Smart Card and IT-infrastructure – can be satisfied using one single device.

SmartUSB also provides all relevant hardware accelerators for symmetrical and asymmetrical cryptography. The ACE (Advanced Crypto Engine) supports RSA cryptography for bit lengths up to 1024 bits. Bit lengths of 2048 bits can be supported using the Chinese Reminder Theorem. Beside this, the ACE architecture can also calculate elliptic curves (EC) cryptography according to GF(p). The DES engine provides DES and 3DES cryptography as well as EC cryptography according to GF(2n). A dedicated high-speed hashing accelerator supports SHA-1 and MD5 algorithms.

New applications

Today the main applications of Smart Cards and USB-Dongles are authentication or PKI applications. In these cases the secure controller is only used for secure key storage, digital signature and key exchange for symmetrical cryptography. All symmetrical cryptographic functions, where huge data packages with according data rates are generated, are implemented on the host platform. This is, of course, the only feasible solution today, due to the fact that the standard Smart Card ISO7816-interface does not offer sufficient data rates for bulk encryption/decryption.

The USB-interface might be able to change the current situation. Effective data rates of up to several Mbit/s are possible. Just as a comparison - that's the typical speed for widely spread Ethernet-implementations (10 Mbit/s). Another example: Many companies use E1/T1 lines with 2 Mbit/s to connect several company locations within a VPN. Typical home Internet access solutions provide data rates ranging from 56 kbps (analog modem) via 64 kbps (ISDN) up to 1-8Mbit/s (ADSL or SHDSL). Having a fast USB-interface does not necessarily mean that there are no other bottlenecks anymore that would limit the maximum data rates supported by an USB-security controller.

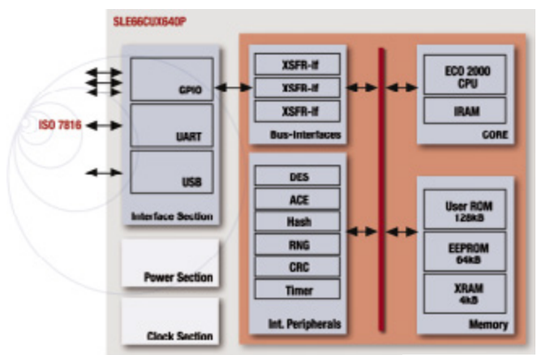


Figure 1- Architecture for the Smar

However, through the use of the Infineon crypto-accelerators, these data rates can be supported as well. Symmetrical cryptography up to data rates of 1 Mbit/s is not a problem at all. Hashing accelerators are even faster. Using such devices, new applications beside PKI and finance applications could easily be provided to the end customer.

Such applications could be:

- Highly Secure Digital Right Management Solutions.
- Fast, smart, portable and Secure Flash Memory Dongles with storage capacities of several 100 MByte, no bigger than a typical USB-Dongle today.
- Encryption/Decryption devices for teleworkers
- Complete Firewall solutions including encryption/decryption accelerators for home applications

The market potential is huge. The hardware costs using USB-Dongles are quite small considering the high security advantage brought about through such hardware solutions.

Let's take the example of a firewall on an USB-Token to give a better feeling of what's possible.

Let's assume that you use a PC based on a secure platform as defined within the TCPA-initiative (Trusted Computing Platform Alliances). The goal of this initiative is to provide a hardware or PC platform, which is able to verify the data integrity at least every time the platform is booted. Meaning that any contamination of the platform with viruses or any unauthorized changes of the platform can be easily detected. Infineon provides a device that is specified to TCPA standards and specifications, called the Trusted Platform Module, or simply TPM. Together with an efficient firewall solution based on SmartUSB, hackers and virus attacks from external networks and from contaminated data storage devices such as CDs can be blocked.

Sounds difficult - or even expensive? Not at all! SmartUSB as well as TPM are low cost devices, compared to current hardware solutions for IT-security. Additionally they provide a leading edge and field-proven security architecture. In fact, it's time to re-evaluate the target applications of security controllers. They're not just Chip Card controllers anymore. Their target applications range from simple authentication or access control, up to networking or communication applications and beyond. You could almost say that the Chip Card controller is finally growing up – it's definitely becoming smarter!

Protecting Your Platform

An interview with David Grawrock, Security Architect, Intel Corporation

On a very hot day in June, SECURE caught up with David Grawrock, Security Architect with Intel, at the Infineon Technologies headquarters in Munich, to talk about the TCPA, Intel's role, the TPM modules and what it's going to take to make the benefits of a secure platform obvious to the average guy-in-the-street.

SECURE - David, what would you say are the benefits of the TCPA* and TPM products?**

First, it increases your level of trust in your platform. This starts with a measuring process, so you now know what's happening on your machine. The next step is that it then gives you a way of taking those measurements and reliably reporting them. After that, you can validate those measurements, and finally there is a way to monitor data (and other things) that are stored on that particular platform, that is tied to those specific measurements. So you can say, "I only get this value back when everything is in the same configuration."
For a manufacturer, these are the now the basic building blocks that allow you (as a manufacturer) to build applications that use those facilities.

SECURE - That's great for the chip manufacturers, but what about the man in the street? How will end consumers react when they are told that the machine they are about to purchase has security products on board that were defined by the TCPA?

Personally, I hope that they don't know about TCPA at all! In the sense that I would like them to believe that the systems themselves are simply more secure than they used to be; primarily because security is hard for end consumers to see.

They get [their machine] and go, "Why is this one more secure and this one less secure?" So what you would really like to do is build up the brands [of the machines], so that the PC manufacturers (or whoever), can say this one is more secure than the last one we produced. And consumers get to the point where they believe that their information is going to be properly protected because this particular platform is more secure than the previous platform. That's the end user benefit – an increase of faith in their machine to protect their data.
Today's machines are pretty good, however threats are increasing. Consumers need to have confidence that the platform will protect their data and work properly. And so the idea here is to start giving system manufacturers the ability to make better building blocks and produce better systems, so that the end consumer can say, "Oh, I trust that this machine will work properly."

SECURE - Does that mean then that the people who will get the real benefit from the work of the TCPA is not the Infineon's and the Intel's of this world, but the IBM's and the DELL's. In fact any platform maker, because the end consumer only looks at the platform as a whole and not at the fact that it has a TPM chip on board?

D.G. – The customers will get the real benefit. I think you will see the benefit first with the IBM's and DELL's. I guess

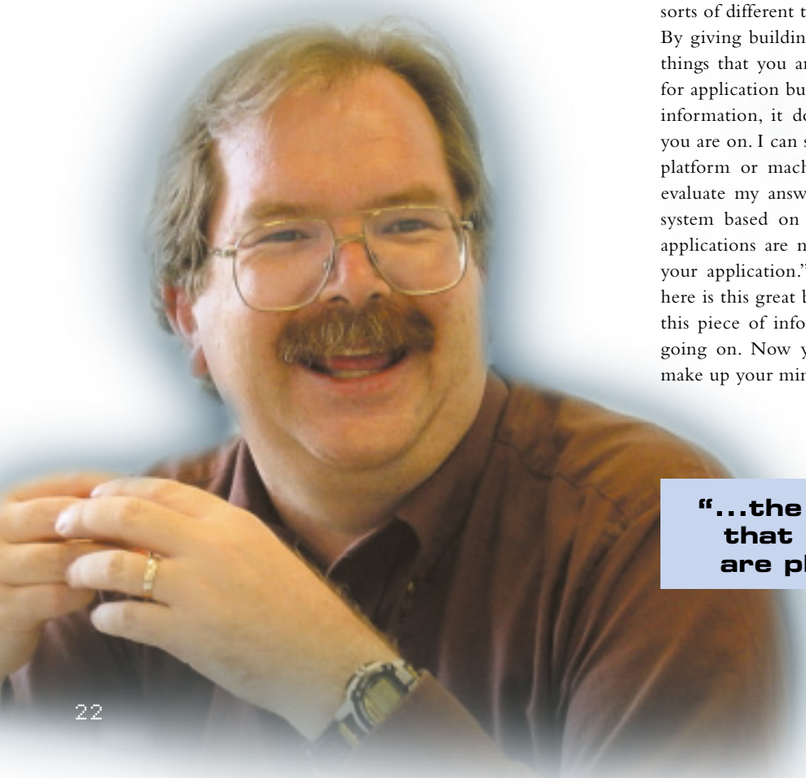
"At the start the (TCPA) logo will be a little more visible, to differentiate this platform (secure) from the other platform (unsecured)."

* TCPA: Trusted Computing Platform Alliance
** TPM: Trusted Platform Module
See page 58 for more background information.

that there will probably be a TCPA logo on the machine somewhere. It's interesting when you look at how information is distributed about the machine through logos and stickers. If you look at a machine today, there are loads of stickers giving information about the machine but many of them are now on the bottom of the machine. Those on the top are the ones that are used to differentiate one platform from another in today's market environment.
I think this is how it will start with TCPA. At the start, the logo will be a little more visible, to differentiate this platform from the other platforms, so the end consumer will be able to say, "Oh this is one of the machines that was built with one of these security things on board. This is a secure platform, so I can trust this platform more." So what we see is that there is a step up. It moves everything forward.

SECURE - Why did Intel want to be a part of the TCPA? Is it simply because it's the next big marketing thing?

D.G. - Oh, I don't think it's the next big marketing thing. I'm a security person from way back and I believe that security should have been looked at a long time ago. It's a realization that we need to make things better for the consumer. And better in this case means more trustworthy. Not that things are not sellable and usable right now (from a security point of view) - they are. But end consumers would like to see an increased level of trust. And I think that is what we are trying to provide. Our mission statement is about providing building blocks for the Internet. Some of the building blocks we need to provide are provided by the TCPA – it's providing more building blocks.



Security is a difficult thing to differentiate on, sometimes it's very hard to say, "I'm more secure than you are." But I think that's what is important to say to the consumers (be they IT or someone at home), that these are more trustable platforms. That's important, that's what drives us. You can have a greater degree of trust now and in the future.

SECURE - Can you give me an overview of the TCPA guidelines for different applications? Are we talking about one platform or many?

D.G. - One of the guiding principles of TCPA was that we didn't want to be tied to one specific platform – we didn't want to say that this was a PC effort. (Laughs). Granted, that when you see who the original promoters were, it drives the point home that PC's were what we thought about first and this is where we went. But the main specification that we wrote is platform agnostic. We don't talk about things that are on a specific platform, because we think that this concept of providing a level of trust through measurements and reporting and so on, is valid on whatever platform you are dealing with; whether it's a PC or a PDA or a cell phone or a router or any of those types of computing platforms. They all have the same requirements. What am I dealing with? What is its current configuration? How do I store things securely on that platform? So we went and made sure that the specification said that these functional requirements were on all platforms and so let's make sure they are available; let's make sure this is done. And then on top of that, we said "Fine. Let's look at how you would take this generic definition and make sure it was implemented properly on a specific platform." And the first one we did was the PC. But the idea is that these specifications are very generic and usable building blocks on all sorts of different types of platforms.
By giving building blocks and saying this is the base level of things that you are going to do, that gives us the guidelines for application building. When you are using standard generic information, it doesn't matter what application or platform you are on. I can send this, the same command on any type of platform or machine and get the same answer back. I can evaluate my answer and decide on my level of trust to that system based on that. So the guidelines we are giving for applications are not in the sense of "Here's how you build your application." What we are doing is that we are saying here is this great bottom level building block and it gives you this piece of information and it will tell you reliably what's going on. Now you as an application, make your decision; make up your mind.

"...the main specifications that (the TCPA) wrote are platform agnostic."

"That's the end user benefit – an increase of faith in their machines to protect their data."

Once you get that information, there are a whole bunch of things you can do. And so the guidelines for an application are going to be "use the facilities, the building blocks as they are designed and it will give you a whole new world of things to do."

SECURE - Are TPMs available today?

D.G. - Yes, they are shipping. You can look at the membership list and find out who is doing that. But there are platforms that are shipping today that have TPMs on them.

SECURE - Any immediate feedback from the market about the TCPA and the TPM products or is it still a little too early?

D.G. - Honestly, it's a little too early for that right now.

SECURE - What are the problems in taking a subject like this from theory to practice and on to implementation?

D.G. - Huh! Do I start at the beginning or at the end? (Laughs).

Going from a spec to something that actually happens is a long process and what you have to make sure happens first, is that what you provided really is something of value. And then you have to be able to find either your own internal company's or an external company's part of the organization that is willing to do the work necessary. People have to take a risk. If its not been done before, you are out there all of a sudden implementing something that you don't know if it's been done properly, you don't know if it's complete and you don't know if there are any other problems on it. So you really have to find people who are willing to take a risk and develop it and suddenly find a problem and still be willing to go back and make some changes. So it's a process that requires a lot of give and take by everybody. You have to be willing to sit there and say, "This is what I have designed, and this is what I have produced for everybody." And if there is also a mistake, you also have to be willing to say, "Oh sorry, I made a mistake – I'll make that change." You have to be very flexible on that process.

SECURE - What does it take to make security an everyday item?

D.G. - We have to continue to tell people that this is something they need - whether they realize it or not. And we have to continue to tell them. But part of the problem is that manufacturers in the past have made security too visible. We have made security something that you see, as opposed to something that works in the background for you. It should be something that is easy to use. Human error is normally what breaches security protocols or causes crashes. What's happening now is that we are trying to make everyone a security expert (even if all they want to do is buy something with their credit card over the web!), whether they want to be or not. Now we have unknowing, untrained, unknowledgeable, and uncaring people who are supposed to be security experts. It's not going to work.

So our job really, is to make sure these people do not have to become security experts. We have to take it out of their hands, because they are not going to do it right. And if we depend upon them to do it right, we are going to be in trouble. So we have to make sure that the security we provide people is so simple to use, that they do not understand they are becoming security experts and that the technology works all the time, every time - without their knowledge and for their benefit.

SECURE - Could something like the TCPA have happened without the credibility and presence of the likes of Microsoft, IBM and Intel and other industry movers?

D.G. - No, I think that if you had tried to do this as an individual company, even if you were Microsoft, IBM or Intel, you would not have had the power or the ability to move things like a large organization does (in this case the TCPA) where people work together. If you get a collection of passionate people out there pushing the same idea and they are

in different companies and they can get together and get things done, then the whole thing grows and multiplies and pretty soon you have that critical mass. I don't know what the number is for that critical mass, but it is very hard to start something like this in one company and get it out there. There have been lots and lots of products from single companies in the past that haven't made it. They have done a good job, have worked well, but they withered on the vine.

SECURE – So what is it that makes all these months of work within the TCPA a success; that TPM products are a success? What's the one little item that makes it all worthwhile?
D.G. – (Laughs, as do other Infineon people in the room).
It's on every single machine out there! (Pauses).
Although it's a nice idea – that's not really likely. (Pauses again).
Probably the success criterion is that it's in use and that the TPM or its successor is still in use five, ten years from now. If that's the case then we are a success.

SECURE – Final question. How do you see the TCPA evolving over time?
D.G. – (Laughs). That's an open question right now, because from one side I think that security is not the point. You don't stick a stake in the ground and say, "Hey, I'm secure. I'm done." Security is a process; it's always about give and take. I set a barrier, the attackers go over it. I set a new barrier; they go over that one too. However, hopefully, as we set new barriers, we take out a whole section of attackers – they are no longer able to play, and you move forward.

However, crypto algorithms change, procedures change, all these things are events that occur and I think that if you are going to try and provide long term trust in a platform, then you are going to be saying: "what am I going to look at and how can I evaluate how this platform is viewed right now? What do I do to make it more trustable in the future?"

So that says you are moving forward. Now what does it say towards the organization? I'm not sure. That's a business issue, not a mechanical issue of how we manage that. But what it is not saying is that we are going to do this once and then throw it over the wall and forget it. I don't think that's going to happen. We have to go forward and look at features and see what we need to change. So I think we are going to have to baby-sit this thing and watch it for a while. How long that while is – I don't know.

Munich, Germany – June 2002

Biography

David Grawrock is a Security Architect for the Desktop Architecture Lab of Intel. He designs and evaluates security protocols and systems for Intel products. David has been involved with TCPA since 1999. David has worked in the computer industry for 25 years, holding positions with Central Point, Symantec and Lotus.

For information visit:
www.trustedcomputing.org

☞ CONTACTLESS – AS SAFE AS HOUSES?

By The Silicon Trust

There's nothing some of the world's media likes more than a bad news story. And anything involving public money, security flaws or a system failure is likely to have them salivating over their laptops as they write their latest exposé. But what does this have to do with us? Surely a contactless card is something that sits discretely in our wallet and is used only when our minds are on something else, such as getting to work on time, buying a newspaper or waiting for a train.

Think again: you might be surprised how much contactless is now part of everyday life. Take, for example, a simple trip to the airport and you'll see how ubiquitous the technology has become. Traveling there is likely to involve use of some kind of contactless token, such as a Shenzhen Tong or London Oyster card. Once there, you decide you'd like a cup of coffee or candy bar – bought using a contactless payment card. And before you can board your flight, you'll have to show your ePassport. The reason why we don't think too much about our contactless cards and documents is because they work: they enable us to access a wide range of services and products quickly, conveniently and securely.

But there's a lot of work going on behind the scenes to ensure the technology works, that travelers can rely on their cards and that they trust them. Get security levels right, and travelers won't notice as they dash through the airport departure lounge with their double mocha in one hand and travel documents in the other. Get them wrong, and things can quickly come to a grinding halt, instantly eroding consumers' trust and damaging reputations.

Implementation

To get security levels right, you need to ensure system implementation is carefully planned and fully thought out. What types of security are in place? How convenient is it? Have you achieved end-to-end security – or are there weak links that are susceptible to attack? How do you ensure your stakeholders are aware of the security measures you've adopted so they have confidence in the system? What are the risks of a security breach? And what are the rewards of cracking the system for a fraudster or a hacker? For example, if it's the ability to access a transport network for free rather than paying a US$2 fare, the benefit to criminals is significantly less than gaining access to secure premises to carry out other types of crime. ☞

To get security levels right, you need to ensure system implementation is carefully planned and fully thought out.

☞ The mechanics of the system also need to be considered. The chip in the contactless token, card or ePassport needs power to function and as the document has to communicate with the reader device, a connection to the outside world is required. With contactless technology, this connection is established using an etched antenna or wire coil sealed in the contactless device and connected to the chip. Using contactless communication, no physical contacts are required. If the document is put close to a reader, the reader will supply the chip with current, and only at that point will it be possible to send and receive data.

This means organizations must consider at what distance the contactless card or device is going to be read. There's been some concern expressed about whether it is possible for a contactless card or document to be hacked when data is being transmitted between the document and the reader and for a forged or cloned chip to then be produced. A contactless payment device conforming to ISO 14443 is typically designed to operate at a very short range of less than 2-4 inches from the Point of Sale (POS). Other contactless standards, such as ISO 15693 for vicinity cards, may offer a read distance of 1-1.5 meters, which is necessary for applications like ski passes, however vicinity read range is not suitable for ePassports or contactless payments where much shorter read distances are advisable.

As contactless transmission usually takes place over a distance of just a few centimeters, for an eavesdropping device to work it would have to be installed very close to a document reading machine – and so should be easy to spot. But it has to be assumed that, however unlikely it is to occur, it is possible to hack this

ePASSPORTS AND eID CARDS

ePassports and eID cards require high levels of security. Consequently, chips used in these documents tend to conform to Common Criteria Evaluation Assurance Level (EAL) 5+ (high). For example, the chips used in Germany's ePassport received Common Criteria EAL5+ (high) certification from "Bundesamt für Sicherheit in der Informationstechnik" (BSI).

data during transmission. So data exchanged between a document and a reader is protected by additional countermeasures such as encryption. Furthermore, the data integrity is checked for attempts at manipulation, such as identifying whether information stored in the chip have been changed.

Behind most contactless schemes is an IT system which stores and authenticates personal user information.

Security levels

Organizations also require assurance that the technology provides rigorous levels of security, something best achieved by choosing certified products that have been independently evaluated. Within a contactless program, this could include certified operating systems, database management systems, firewalls, smart cards and chips.

Organizations also need to consider the personalization process. The document holder's personal data is introduced during personalization. Once this has been completed, the data is locked in the chip's hardware to prevent unauthorized alteration. But how should an individual's document be personalized and delivered to them? Is it necessary for them to visit their local bank or a government authority to sign for their contactless card or eID document? Or can it be mailed securely?

IT system security

Behind most contactless schemes is an IT system which stores and authenticates personal user information. These have to establish and maintain security in four key areas:

- Secure authentication – ensures that only legitimate users can access certain data or perform specific actions;
- Data confidentiality – ensures that personal or sensitive data is protected from illegitimate users;
- Data integrity – ensures that data is not purposefully changed by illegitimate users;
- Data availability – ensures that data is made available to the right person whenever necessary.

☞ These measures are normally achieved using different forms of security. For example, authentication can be carried out using a password, a PIN, a biometric or a smart card, while confidentiality and integrity can be maintained through encryption and firewalls.

Protecting the end user

In the financial sector, where security is important for promoting a positive brand image, as well as protecting the bottom line, multiple levels of security are added to reduce risk for all parties involved in a transaction. These may include encryption, online authorizations, risk management and fraud detection technologies to flag up any potential fraudulent activity on a card, as well as liability protection. There are also rules governing floor limits – and this is where the trade-off between security and convenience really comes into play. For example, many contactless payment schemes have a £10/US$20 floor, which offers a good level of security, but may be too low for bars or restaurants where the average spend is likely to exceed this limit.

Post implementation

Having implemented a scheme, security must continue to be at the forefront of all planning. One thing's for sure: any barrier aimed at defeating attacks will weaken over time as new hacking methods are developed. It is therefore essential to take advantage of new security techniques that emerge to ensure a system stays ahead of attackers.

Large numbers of contactless documents being transported nationwide could also be susceptible to attack, something which actually happened in the UK in July 2008, when a van containing thousands of ePassports was hijacked. However, it is important to remember that manufacturers equip security chips with transport keys. If chips are stolen while they're being transported from the chip manufacturer to the document producer, thieves would be able to write their own data on them only if they knew the relevant transport keys.

Industry groups on board

Industry groups are also behind a host of security initiatives. For example, the Near Field Communication (NFC) Forum's Security Technical Working Group handles security and data protection issues within the organization, and provides security-related guidance for all its other technical activities. These activities include:

- Defining a modular security architecture for NFC-based communications;
- Providing support and guidance to other working groups on security-related topics;
- Defining common security requirements, and describing threat models relevant to NFC-based communications;
- Defining, as needed, new NFC-related security specifications.

Industry body GlobalPlatform launched its Mobile Task Force last year to facilitate new business opportunities between the mobile sector and other industries. It has also worked with the European Telecommunications Standards Institute (ETSI) for several years on security aspects, such as collaboration with the Card Committee on the development of the Confidential Card Content Management Amendment to the GlobalPlatform Card Specification v2.2, which enables application providers to confidentially and independently manage applications while using a third party communication network. During 2008, it has been developing the Contactless Services Amendment to the GlobalPlatform Card Specification v2.2, again working with the Card Committee, to support new requirements related to contactless and NFC technology. The main objective is to facilitate the deployment of contactless applications and services in a Secure Element located in a mobile handset. The multi Secure Elements aspects of this work will be carried out by a Secure Element sub-Task Force.

Although nothing can be guaranteed to be 100% secure, the industry is working hard to stay ahead of the game. With the media hungry for stories of security breaches it's in every stakeholder's interests to ensure that all parts of the process are secure. Just as houses need not only doors but also windows to be securely locked to achieve good levels of security, so contactless technology requires a similar, seamless approach where there are no weak links. If this can be achieved, the media will have to look for bad news elsewhere, leaving transport operators, governments and financial organizations free to carry on making everyday transactions as quick and convenient as possible for consumers. ■

Step aside, smart cards – NFC is entering the identification arena

By The Silicon Trust

2011 has turned out to be a defining year for Near Field Communication (NFC). Most mobile phone manufacturers have announced plans to include NFC functionality in the next generations of their mobile phones. With up to 280 million people carrying NFC-enabled phones by 2013, new applications will develop rapidly. Credentials such as keys, access cards, tickets, business cards, plastic loyalty cards and payment cards could rapidly disappear in favor of a single personal credential on your phone. Does this seem a little radical? Well, let's take a step back first.

☐ Complexity of managing increased number of credentials

Unprecedented levels of movement, migration, travel and international commerce are the norm for our generation. The phrase "global village" may be an annoying oxymoron for some, but it is a living reality for the more than one billion people who travel, building friendships, connections and business with others across the globe. Our need for identification and privileges management has exploded in volume and complexity. We carry drivers' licenses to drive and, in the US, for general ID purposes such as domestic travel or checking into a hotel. We carry passports to travel internationally; we carry health insurance cards for access to medical treatment or to obtain medication; we carry frequent flier cards, bus passes, library cards, bank debit and credit cards, even ski passes and loyalty cards for every tenth coffee. We also carry badges or cards to get into our office building, college dorm, parking structure, company cafeteria or gym. We sometimes use cards or tokens to gain access to a website or to log on to a network; we also use a multitude of passwords that we must try and memorize. Passwords are driving us all crazy as we are forced to include symbols and characters and to change them every ninety days or so. For extra security we are sometimes even forced to use an external password generator, provide a fingerprint or allow an eye scan, either alone or in a combination with an ID card, fob or PIN.

There is mounting irritation and confusion as we have to deal with so many different ways to prove that we are entitled to whatever it is we are trying to access: our money, healthcare, the workplace, the ski slope, a private airport lounge, a travel website, online banking, a social or company network. We deal with disparate systems, each with its own key, its own lock. So we walk around burdened with numerous keys and cards, trying to remember many different passwords with different rules. All of them dedicated credentials and methods of ID, used on proprietary systems and applications.

The phrase "global village" may be an annoying oxymoron for some, but it is a living reality for the more than one billion people who travel, building friendships, connections and business with others across the globe.

Move towards convergence of credentials

In some areas there has been a strong drive towards converging multiple functions onto one card in order to increase security by having a single point where credentials can be issued, managed or revoked. The U.S. Government, for example, has been engaged in a multi-year effort to replace the plethora of cards issued for access to physical buildings and the dedicated smart card for network access used by employees and contractors with one single credential, known as the personal identity verification, or PIV card. Enterprises are also beginning to converge their employees' credentials so that both physical sites and computer networks can be accessed with the same card. On the technology side, miniaturization has made it possible to transfer the security benefits of smart cards to RFID cards, creating what is known as a contactless smart card, so that user convenience is further enhanced with the ability to just touch one's identity card to a door or computer reader to gain entry. While this convergence of physical and IT access control in the workplace requires significant upgrades to the various systems involved, it also offers the employer the ability to manage different types of privileges on one, single smart credential.

NFC offers user-based control over which application we choose to read from or write to, and where or to whom we wish to make our presence known.

NFC creates one, simple-to-use system for everyone

NFC technology is a revolutionary development that promises to provide the convenience of a single, contactless credential for each of us – and a lot more – by enabling a highly secure personal credential to be built into our mobile phones. An NFC-enabled phone such as the Google Nexus S or a Nokia N9 incorporates all the functions of a secure contactless smart card, comparable in its level of security and sophistication to highly secure electronic credentials such as electronic passports, credit cards or expensive electronic tickets. What makes NFC phones really powerful is the convenience of enabling them anywhere, anytime through secure mobile connections, to act as our personal credential for an endless number of possible mobile applications. We can use our NFC-enabled smart phones to help us sign on to different websites, networks or loyalty programs, thus eliminating the need to remember all those multiple passwords. We can download a ski pass to our phone, or tap our phone to workout machines to log our fitness routine or map our run.

We can also use our NFC phones as a reader or scanner. Just as we use the camera to take photos, we can use the NFC reader features in our phone to download data such as merchant coupons or restaurant reviews from smart tags or smart posters. We can buy and download our Charlie, Oyster, BART, MARTA or other transit pass on our NFC-enabled phone and just hop on the bus or subway using a machine-to-machine transaction between our mobile device and the ticket-issuing machine. We can follow organizations or people on Twitter and Facebook or receive RSS feeds by simply using our smart phones as readers. NFC also supports more secure transactions. In many countries, online banking transactions are required by law to use the strong authentication of a one-time password, or OTP, generated from a card or token issued by a bank. NFC-enabled phones, however, can do the trick without the need for carrying an additional battery-powered device dedicated to reading out an OTP.

What makes NFC phones really powerful is the convenience of enabling them anywhere, anytime through secure mobile connections, to act as our personal credential for an endless number of possible mobile applications.

Choice, convenience, cost, security and above all fun and simplicity will determine what kind of world we will shape with our NFC phones in a new era of electronic consumer empowerment. So in this new brave, connected world, we move towards an integrated multi-application, multi-use credential and a secure multi-use, multi-application reader, both incorporated into our NFC-enabled phones; an inevitable move to a more integrated, more connected world.

Finally, as is the case with any new wireless technology, there may be lingering concerns about the security of vital data and communications. NFC is actually very secure. Because it operates only at very close ranges (1 to 4 cm), it is difficult to hack the data being transferred using NFC signals. The usual precautions of passwords or prompts before launching new applications on a smart phone apply with NFC just as they do elsewhere. And NFC-enabled phones don't require activation of GPS or global positioning, or even a cellular connection; they require a deliberate use by the consumer to read or be read. Therefore privacy concerns are abated as most NFC transactions take place within the mobile phone users' reach. NFC offers user-based control over which application we choose to read from or write to, and where or to whom we wish to make our presence known. The level of security can also be put in the user's hands. Settings can be changed to make a transaction automatic with a touch, require an app to launch first (i.e. must push a button), or even require entry of a pin code. The user can set the level of security based on his or her own personal comfort level with individual applications and use cases.

Privacy concerns are abated as most NFC transactions take place within the mobile phone users' reach. NFC offers user-based control over which application we choose and where or to whom we wish to make our presence known.

NFC represents a paradigm shift in how we live, making everyday activities easier and more convenient by building on existing systems and human behavior. It will make accessing new media and content services more intuitive; make it easier to pay for things; easier to discover, synchronize and share information; and easier to use transport and other public services. How will NFC ultimately change our lives? In more ways than we can imagine. ☒

Cloning the *UNCLONABLE*

By Marcus Janke and Dr. Peter Laackmann, Infineon Technologies AG

Uniqueness, in many forms, has been used for the purpose of security since thousands of years: From seals impressed on clay tablets, the unique distribution of fluorescent fibers in banknote paper, to the scattering of laser light on randomly manufactured surfaces on protected documents, uniqueness created authenticity. In the world of semiconductors, uniqueness also served as a task for engineers since decades, as it is a value which can be used for generating secrecy and authenticity.

One of its subgrups causes some upset, given the name 'Physical Unclonable Functions', or PUF. 'Unclonable', of course, is a teasing word for security experts who know that nothing is uncloneable by nature, like nothing is one hundred percent secure. Nevertheless, the term yields a good occasion to venture a glimpse into these technologies, in order to separate opportunities from tripwires.

Creating uniqueness

Uniqueness is usually created by processes containing randomness – which, in nature, is always available in abundance. The well-known unique fingerprint of each human often serves as a prominent example. But 'fingerprints' can also be taken from objects. Paper manufacturers know that the orientation of a single cotton or wood fibre in a piece of business paper cannot be predicted, but will be fixed after manufacture. Diving into the microscopic or nanoscale world, uniqueness is even more a factor, also including silicon chips. Single elements of a chip, like transistors, may differ from each other. As a consequence, each chip differs from each other. Usually, these small deviations are so minor that they are not significant for the proper function of a chip design. Nevertheless, through amplification, the differences can be measured, and even used in a chip to create unique data, keys or a unique algorithm.

'Strong' unique functions

The original ideas of using a chip's individual uniqueness as a source for secrets were born and implemented decades ago as so-called 'hardware watermark' procedures. Input data was pushed into an electronic circuit which, chip-individually, would produce different output values with low, or even no, predictability, like a secret algorithm unique for each chip. This concept would be called the 'strong' variant today, as no key or algorithm is directly stored on the chip, and also no key is directly processed in the chip. In older times, when keys were stored in the chip's memories, at first sight, such concepts seemed very promising.

Unfortunately, the characteristics of the chip-individual deviations, as they are very small, also came with severe disadvantages: The electrical differences are also heavily influenced by the environmental parameters (e.g. temperature, voltage, light, radiation and many others) and are subject to chip aging, resulting in strong reliability hazards – in other words, the designer could chose between security and reliability. To overcome these weaknesses, another variant of unique functions was created, the 'weak' but more robust version.

'Weak' unique functions

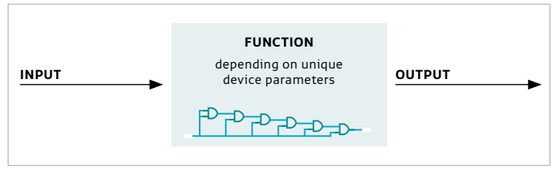


Figure 1: 'Strong' unique function

As the information, which is generated by one unique element, would be prone to environmental changes, solutions were needed. The simplest solution was to use redundancy: If, due to aging, information could get lost, simply more information was used as a 'backup'. Typical systems therefore collected the information from many unique elements and joined it together to form a more robust data set. Even if some of the unique elements would switch their behaviour, the result would stay constant. Being a nice solution at first sight, such 'robust' unique functions showed a totally different behaviour in terms of security. For the sake of robustness, security

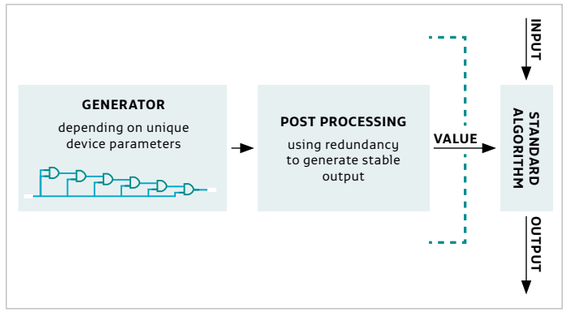


Figure 2: 'Weak' unique function

has to pay a heavy price: Now, the secrets are used and processed in the chip, and they are present. The original idea of unique functions suffers significantly, and therefore such variants are also called 'weak' unique functions today.

Physical 'Unclonable' Functions do not provide a security feature by themselves. Instead, they provide an extra functionality. This in turn means that extra doors for potential attackers may be added by the implementation.

If the secrets, which are used in digital form in the chip, would be extracted, subsequent cloning of the chip would be possible again by simple emulation. Extraction could be done, in turn, especially by probing attacks, but also observing and semi-invasive attacks must be taken into account. Therefore, as mentioned, the word 'unclonable' can be vastly misleading. Nevertheless, even 'weak' functions can be used for applications like the ones that are based on logic chips as a source of individual secret keys. For example, even a pure logic chip, like used in automotive or RFID, can be enabled to utilize chip individual encryption or other purposes now.

Attacks

Physical 'Unclonable' Functions do not provide a security feature by themselves. Instead, they provide an extra functionality. This in turn means that extra doors for potential attackers may be added by the implementation.

There are few functions that attracted such a vast dimension of potential attack vectors than the 'Physical Unclonable Functions'. In the last few years, dozens of new attack scenarios have been developed to overcome these functions. Today's existing attacks were derived from all three major attack groups (manipulating, observing and semi-invasive attacks). Also, logical/mathematical approaches were developed to break the underlying mechanisms. All these methodologies are called 'PUF-specific attacks'.

At first sight, a layman would think that Fault Attacks would rather turn the implementation unusable – which would be not more than a denial-of-service approach. But an intelligent attacker could do much more than this: By influencing the PUF related error-correction logic, data dependent leakage of secrets could be induced through a newly generated additional side channel. Also, fault attacks against so-called 'helper data', which is used by some PUF implementations, are known, and must be considered. First countermeasures have been developed since these attacks are known. If the PUF is directly used for cryptography on the chip, it should be also considered that an attacker would try to induce the use of a weak key that in a second step could be easy to break by conventional methods. Fault attack methods may include the use of radiation (alpha radiation, laser or electromagnetic localized impulses for temporary influence, X-rays, beta rays, UV irradiation, temperature exposure or gas diffusion to induce permanent changes).

The Side-Channel Attacks, which are well known in the form of SPA/DPA (Simple/Differential Power Analysis), take a full revival in the area of Physical 'Unclonable' Functions. Practically every electronic circuit's behaviour depends on the data processed therein. Through observation of the chip's power consumption, its electromagnetic emanation, local optical emission or laser voltage probing, an attacker can try to spy out confidential data. Techniques like Time-Resolved Emission analysis (TRE) and the use of infrared emission analysers with Solid state Immersion Lenses (SIL) allow the use also on modern, very small chip technologies. One would first suggest that side channel attacks, therefore, could be mainly applied to the error correction processes or extractor functions that are typically used in a PUF implementation. Nevertheless, meanwhile several experts demonstrated publicly that side channel attacks also could be used as an effective weapon against the PUF 'heart', the origin of the characteristic data, itself.

An intelligent attacker could do much more than this: By influencing the PUF related error-correction logic, data dependent leakage of secrets could be induced through a newly generated additional side channel.

Even the Physical Attacks, like probing or forcing signals with small needles placed on the chip, Atomic Force Microscopy (AFM) or Focused Ion Beam manipulations (FIB), may still be used effectively. One of the most interesting targets by using physical attacks is to induce the attacker's own data into the key generation, so that decryption of the complete chip content would be easy in a second step. Furthermore, many implementation options of PUF could make the error correction and extraction circuits a very interesting target for snooping data.

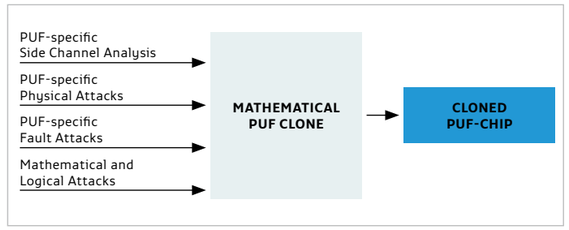


Figure 3: How to Clone the 'Unclonable'

Besides the typical three attack groups against hardware, the implementation of a PUF may allow the use of Mathematical Attacks as a backdoor to its secrets. To understand this threat, it is important to realize the difference between physical and mathematical clonability of a PUF. This means that even if it would be hard to clone the exact physical characteristics of a specific circuit, the chip itself could easily be cloned, as it usually does not matter at all to the outside world, how the PUF data is generated inside. If the reaction of a PUF circuit to an unknown input would be predictable, the attacker could implement his own solution to generate such data, and produce cloned chips. Unfortunately, typical PUF are NOT mathematically unclonable, so that a high risk may emerge:

Today, in the area of PUF, the so-called 'modelling attacks' were most prominent up until now. For a modelling attack, input and output data is first collected and then mathematically analysed. From that analysis, a computer model is generated that can give a prognosis for the PUF behaviour to an unknown input data. Today, every private person has access to large amounts of computing power, so that modelling attacks using machine learning, using for example 'logistic regression' techniques, could serve as a very dangerous tool. Countermeasures, like trying to prevent direct access to the PUF input and raw output, could succumb to a combination of the mathematical attacks with a physical attacks or side-channel analysis.

One of the most frightening aspects would be a potential misuse of PUF technologies for granting Hardware Trojan Backdoor Access to a security chip. In this case, the PUF function would be integrated into a chip to serve an additional purpose – an intended, dangerous security backdoor that could be very hard to detect. First publications covering this topic already appeared in the public, raising concerns in the light of globally distributed chip manufacture.

Conclusion and outlook

Unique functions for the generation of on-chip secret keys and individual algorithms have been researched for decades now. Especially in the last years, increased research has been applied to silicon-implemented logical circuits that would use the chip's individual characteristics to generate individual keys. Today, devices that by technological restrictions do not allow to use certified true random number generation, nor secure key derivation, could first benefit from PUF implementations. Pure logic circuits, for example, can be equipped with unique coding, or even combined in a system together with security microcontrollers.

Idea and implementation, on the other hand, are different parts. While allowing new functionalities for good reasons, carelessness, on the other hand, may open new doors for attackers. For a new PUF implementation, at least the relevant attacks known today should be carefully investigated for a proper security evaluation. Equipment for PUF-specific attacks should be at hand while developing appropriate attack countermeasures. Unique functions may serve as a source of security – if they, themselves, are properly protected against various attacks from amateurs to professionals. Although there seems to be a consensus that even today's technologies allow a reasonable use in selected applications, experts call for quantum-physics PUFs to achieve enough security, and strongly demand to invent new PUF construction principles. ☒

One of the most frightening aspects would be a potential misuse of PUF technologies for granting Hardware Trojan Backdoor Access to a security chip.

Literature

F. Armknecht, R. Maes, A-R. Sadeghi, F-X. Standaert, C. Wachsmann, "A Formal Foundation for the Security of Physical Functions", 32nd IEEE Symposium on Security and Privacy, 2011.

D. Schuster, "Side Channel Analysis of Physical Unclonable Functions (PUFs)", Diploma Thesis, Technische Universität München, 2010.

D. Merli, D. Schuster, F. Stumpf, G. Sigl, "Semi-Invasive EM Attack on FPGA RO PUFs and Countermeasures", Proceedings WESS2011 Workshop on Embedded System Security, ACM, New York 2011.

D. Merli, D. Schuster, F. Stumpf, G. Sigl, "Side Channel Analysis of PUFs and Fuzzy Extractors", Proceedings TRUST International Conference on Trust and Trustworthy Computing – Pittsburgh 2011, LNCS 6740, Springer 2011.

D. Karakoyunlu, "Differential Template Attacks on PUF Enabled Cryptographic Devices", Proceedings IEEE WIFS International Workshop on Information Forensics and Security 2010.

U. Rührmair, C. Jaeger, M. Algasinger, "An Attack on PUF-Based Session Key Exchange and a Hardware-Based Countermeasure", LNCS 7035, 2012, 190–204.

R. Plaga, F. Koob, "A Formal Definition and a New Security Mechanism of Physical Unclonable Functions", Federal Office for Information Security, Germany, 2012.

U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber "Modeling Attacks on Physical Unclonable Functions", Proceedings CCS2010, 17th ACM Conference on Computer and Communications Security, ACM New York 2010, 237-249.

J. Sölter, "Cryptanalysis of Electrical PUFs via Machine Learning Algorithms", MSc Thesis, Technische Universität München 2009.

Z. Gog, M. X. Makkes, "Hardware Trojan Side-Channels Based on Physical Unclonable Functions", in Proceedings WISTP 2011, LNCS 6633, 2011, 294-303.

VIRTUAL TOKEN – *A smart card alternative* that makes SENSE?

By Klaus Schmeh, cryptovision

Why use a smart card, if a secret key can also be stored in a virtual token, i.e. a protected hardware module built into a PC or smart phone? The Trusted Platform Module (TPM) and Intel's Software Guard Extensions (SGX) are two technologies that can be used to build solutions following this approach. Will virtual tokens make smart cards obsolete? Or are they useless, as they miss the point of what smart cards are all about? As will be shown, the truth lies somewhere in between.

The times when a smart card was just a plastic card bearing an integrated chip are long gone. Meanwhile, over a dozen smart card form factors are available, ranging from USB tokens via microSD cards to contactless chips integrated into wristwatches. In addition, it is possible to give up the concept of storing a key on a small item the user can carry with him and, instead, keep this secret information in a protected module inside the end user device (usually, a PC or smart phone). In other words, the key storage place is transferred from the user's pocket to the motherboard. This approach is referred to as "virtual token". A virtual token represents a smart card form factor of its own.

Virtual tokens

A technology that is well suited for implementing virtual tokens is the Trusted Platform Module (TPM). A TPM is a protected hardware module available in most current computers. TPMs are mainly known for supporting software attestation, which is an important countermeasure against malware. In addition, storing secret keys in a protected way is one of the base functions of a TPM. To turn a TPM into a virtual token, a smart card emulation software is necessary that grants access to the keys via a standard card interface. Using a TPM as a virtual token is already common practice and by far the most popular solution for this purpose is Virtual Smart Card (VSC), a technology provided by Microsoft.

Just like a TPM, Intel's Software Guard Extensions (SGX) are suited to realize virtual tokens. SGX is a proprietary set of features supported by many Intel processors. The general purpose of SGX is to provide protected areas (enclaves) to programs running on a PC. Data stored in an enclave are not accessible from outside, not even for the owner of the computer. Typical applications of SGX include malware protection (data stored in an enclave cannot be manipulated by a malicious software) and digital payment with an enclave providing a tamper-resistant environment for handling money transactions.

In addition, SGX supports storing secret keys in a protected environment. If an appropriate emulation software is used, an application program can interact with an SGX-protected area, like with a standard smart card. SGX thus becomes the core

> *“smart cards are indispensable when it comes to implementing electronic identity cards, company cards, digital signature cards, or multi-application cards. On the other hand, a virtual token is the more pragmatic solution – cheaper and more user-friendly.*

part of a virtual token and even has some technical advantages over a TPM in terms of the crypto algorithms supported.

However, SGX-based virtual tokens are still in their infancy, with no market-ready solution being currently available. Ralf König, Product Manager at smart card specialist cryptovision, says: “At cryptovision we have plans to change this situation. We expect to have an SGX-based virtual token ready by 2018.” As a first step in getting familiar with the SGX technology, cryptovision has implemented a credential storage based on SGX together with Intel. It is one of the first SGX applications on the worldwide market.

It goes without saying that a virtual token is not a one-to-one replacement for a conventional smart card. It can even be said that a built-in security module that is not removable contradicts the basic idea of a smart card, which is to separate the key from the device that uses it. It is clear, for instance, that a key stored in a processor register or TPM of one computer cannot be used on another. If a computer is stolen, not only the device, but also the key is compromised. For this reason, a virtual token is considered less secure than a conventional smart card.

On the other hand, storing keys inside a computer device – yet within the borders of a protected module – has a number of clear benefits. Essentially this approach saves money, as it relies on existing hardware, while a smart card solution always requires purchasing one card per user. In addition, virtual tokens are more user-friendly, as a user doesn’t have to bother with a card and he can’t lose it. Finally, although a virtual token is deservedly not considered high security technology, it has some security benefits. For instance, it is a lot more difficult to steal a built-in hardware module than a smart card and as a further benefit, smart card sharing, which is illegally practiced in many organizations, is a non-issue.

Two approaches that don’t compete

A look at these arguments makes it clear that conventional smart cards and virtual tokens should not be regarded as competing technologies. Instead, each variant has its benefits. Smart cards, including form factors like USB tokens or proximity tokens, are to be preferred if a mobile key storage device is desired and if high security standards need to be met. For instance, smart cards are indispensable when it comes to implementing electronic identity cards, company cards, digital signature cards, or multi-application cards. On the other hand, a virtual token is the more pragmatic solution – cheaper and more user-friendly.

cryptovision Product Manager Ralf König states: “Pragmatic solutions have always been successful in the IT security world. We therefore take virtual tokens very seriously.” In spite of these new form factors, Ralf doesn’t see conventional smart cards under threat. “We expect that billions of people worldwide will be equipped with electronic identity cards in the decades to come. For this purpose virtual tokens are not an option.” ☒

“Integrity Guard” – PROVEN *security* for the *NEXT* DECADE

By Steve Atkins, Program Director, The Silicon Trust

A security chip must be able to store security-critical data – for example keys, personal data or biometric information – and be able to protect the system in a wide range of totally different application fields. Until now, companies have focused on protecting on-chip data from criminal attack by concealing it. Sensors have been used to recognize such attacks and to protect sensitive data from consequent manipulation. However these methods no longer meet the very high security requirements that exist today.

Back in 2008, to protect data more effectively, Infineon developed a completely new approach to security with “Integrity Guard”. This now proven technology is based on digital security and displays two revolutionary innovations. Infineon engineers have succeeded in creating a security technology that not only encrypts the data on the security controller but can also process the data while it is encrypted. Even if malicious attackers “eavesdrop” on the data signals, they only receive encrypted, and therefore incomprehensible, information.

“Integrity Guard” is a security technology that has been inspired by the information storage and information processing of a living cell; the actual inspiration for the concept was the double helix of a human cell. The idea behind it is simple enough - every biological cell is comparable to a “secure computer” that must safely store and process genetic information.

The technical realization of this innovation equips controllers with robust digital mechanisms to protect secure data and to monitor security conditions. Utilizing the “Integrity Guard”, the controller reacts autonomously on security threats. At the core of this self-checking design is a double CPU that performs a continuous self-check of all operations. This self-checking actually results in ‘integrity protection’ – hence the name “Integrity Guard”.

Another key element of “Integrity Guard” is the comprehensive encryption over the whole data path, leaving no plaintext on the chip.

“Integrity Guard” encryption goes much further than conventional concepts and for the first time in chip card history, even calculates with encrypted numbers in the CPU itself.

In addition to the complete encryption of the entire data path (CPUs, memories, caches and buses), these high security controllers have two CPUs and a refined error-detection system. The two units continually monitor each other, and should a unit detect that an operation has not been properly executed due to a criminal attack, it initiates the corresponding countermeasures. In this case, the chip immediately stops the ongoing processes and triggers an alarm. This makes it possible to ward off the most varied kinds of attacks.

New Digital Security features

Thanks to the totally new scope of their digital security features, controllers with “Integrity Guard” meet very high security requirements. Their robust design overcomes the disadvantages of analog security technologies. Full on-chip encryption, including encrypted calculation in the CPU itself and full error-detection capabilities over the complete core architecture, provides the basis for the efficient protection of sensitive data against external attacks.

Full Error detection

“Integrity Guard” security chips are the first of their kind to be equipped with a full error detection capability for the complete data path. A dual CPU approach allows error detection even while processing – the CPUs constantly check each other to establish whether the other unit is functioning correctly. Relevant attack scenarios can be detected, whereas things that would not lead to an error are more or less ignored. Thus the risk of false alarms – a significant disadvantage in conventional solution concepts – is significantly reduced. The approach includes error detection and correction throughout the entire system.

Total encryption

The security controllers with Infineon’s “Integrity Guard” are equipped with full encryption over the complete CPU core and the memories – meaning no more plain data is left on the chip. It is the first time ever in commercial security controllers that the two CPUs have utilized fully hardware-encrypted calculation, and with different dynamic secret keys. This process is only possible because Infineon, which allows the integration of real encrypted operations, has implemented the CPUs from scratch.

Signal protection

In signal protection, the main objective is to reduce to the minimum the attractiveness of the signals for the attacker. This is done by means of full encryption. Attackers can neither manipulate nor eavesdrop on encrypted signals. Nevertheless, in every chip there are signals that are more important than others, so an Infineon-specific shielding, combined with secure wiring, has been developed. With this method, first all the signals are classified according to their value for the attacker. In a second step, during the design of the chip, the more interesting signals are automatically routed under less valuable lines. Subsequently, an intelligent shielding algorithm finishes the upper layers, completing the so-called I2-shield (Intelligent Implicit shield).

Towards durable security

For the challenges on the path toward durable and lasting security, a professional approach is necessary in order to evaluate the future of attacks and suitable countermeasures. When developing new product families, the planned and anticipated lifetime needs to be kept in mind. As is the case for electronic passport chips, there is often a span of ten to fifteen years between the design and end of the product's lifetime in the field.

Infineon's own security laboratories therefore focus on researching what will appear next in terms of known or even completely new attack scenarios. Localized attack methods aim at finding secret keys in the very heart of a chip – the CPU. Unencrypted CPUs make access to sensitive data easier; they can be analyzed by an attacker using today's state-of-the-art methods, such as optical emission analysis or electromagnetic emanation attacks. It has been shown that conventional, scenario-specific countermeasures not only drive the cost spiral upwards, and lead to tedious security updates, but also no longer serve the requirements of applications with a high security demand.

The advantages of "Integrity Guard"

"Integrity Guard" offers a multitude of important advantages, which fully pay off in the development of secure products.

Customer-friendly security

Today, providing top-level security often means investing great effort and high costs – not only for the chip manufacturer, but also for the Operating System and application SW developers. Adding security often decreases flexibility in conventional applications or is even decreasing the performance. In Infineon's security controllers with "Integrity Guard" technology, almost all security features are automated. Infineon theorizes that because of this self-checking (automated) feature there is approximately 30% less development time taken due to less coding requirements. Once again reducing total cost of ownership.

"Customer-friendly security" means that security features are easy to use and ensure confidence along the entire value chain – from chip manufacturer and chip card manufacturer to system integrators and the customer. This customer-friendly security results in significantly lower overall costs over the product life cycle.

Designing with "Integrity Guard" for a secure solution reduces total cost of ownership through R&D efficiency for application development and so ensuring a shorter time to market for end customer products. Its open architecture will also accommodate future hardware extensions leaving room for expansion of products and their product life spans.

Thanks to their robust design, security chips with "Integrity Guard" technology can also be used in difficult and demanding environments. Their digital features neither have to be adjusted nor calibrated, which makes the chips even more resistant. Conditions that do not directly harm the chip itself will therefore not affect its correct functioning.

Mathematically modelled security

Error-detection codes and digital security features can be mathematically modelled. This facilitates the security evaluation and certification both internally and when performed by third parties.

"Designing with Integrity Guard for a secure solution reduces total cost of ownership through R&D efficiency for application development and so ensuring a shorter time to market for end customer products.

Self-checking security

Security chips with "Integrity Guard" have self-controlling security mechanisms. The most important element is the comprehensive digital error detection over the complete core architecture, including memories, buses, caches, and the dual CPU.

Attack-repellent

The design of the security chips alone impedes attacks. Full encryption is used for CPU, memories, and buses, covering all stored, processed, and transferred data. These mechanisms are automated and facilitate the software implementation and use.

Accreditation and testing

"Integrity Guard" security technology has been evaluated by the accredited and internationally recognized TÜViT testing and certification authority.

The Federal Office for Information Security (BSI) confirmed the high security of Infineon's "Integrity Guard"-based security chips according to "Common Criteria", the internationally recognized standard for the rigorous assessment and certification of security chips. Furthermore, the security controller meets the security requirements for payment cards from EMVCo

Infineon's SECORA™ID *accelerates* eID *PROJECT* EXECUTION

By Markus Moesenbacher, Infineon Technologies

The ID market growth is mainly driven by electronic identification, electronic health cards and electronic driving licenses with strong variations to reflect local flavors. In addition, the request for multi-application is increasing for electronic ID cards.

To meet these demands a flexible product is required which allows the customization of the application according to local requirements.

Java Card™ Technology

Java Card technology is based on JAVA which was invented by SUN (now Oracle Corporation). Java Card only uses a sub set of JAVA and is enriched with security functions and with communication protocols, which are relevant for the Smart Card industry.

It has been invented and patented by engineers of Schlumberger (later GemPlus, Gemalto and now Thales) in 2003. To be allowed to use JAVA technology SUN claimed a Java Card license for the usage of Java Card technology which is still the case today with Oracle. Java Card is used for SIM cards, credit cards and Government ID cards and now more and more relevant for Internet of Things (IoT)

The latest version which is relevant for Smart Cards is Java Card version 3.0.5 Classic.

Java Card version 3.1 includes additional features, which are relevant for IoT.

The evolution of Java Card technology is driven by the Java Card Forum[1], which is a collaboration of key contributors from the smart card industry. The Java Card Forum provides recommendations for the Java Card specification to Oracle, which publishes the specification on the Oracle homepage[2].

Oracle provides the specification for implementating JavaCard as well as the protection profile, which allows a security certification according to Common Criteria.

Claims to the Java Card specification are security, certifiability, compactness and standardization. All this is enabled by the Java Card technology.

Compactness means that a highly complex security application needs to fit in a security controller with low memory and comparable low performance (about 12kByte RAM and about 500kByte NVM and a CPU with about 50MHz). Compared to a state-of-the-art personal computer, which has a CPU frequency which is about 60 times higher with the overall performance even higher, this is a challenge. Security controllers though, are experts for cryptographic calculations, as they are equipped with coprocessors for symmetric and asymmetric calculations.

The certifiability is granted by the protection profile, which is part of the Java Card specification framework.

Java Card Forum

Key technology companies come together to specify and develop the security platform for a variety of advanced digital services – from traditional to IoT use cases in the Java Card Forum. Any Java Card licensee can be a member of the Java Card Forum. In terms of SIM card applications that are based on Java Card, figures show approx. 65% market share in 2019 (3.6bn of 5.5bn total market),[3] while 43% of the whole security chip controller IC market (mostly Government applications and credit cards and an increasing volume of IoT devices) are based on Java Card technology with an increasing volume.[4]

Infineon SECORA™ brand – how it started

In 2017 Infineon launched the product SECORA™ Pay, which is designed for EMVCo compliant credit cards to support different payment brands. Based on SECORA™ Pay, in addition SECORA™ W has been introduced, which is used for wearable use cases (e.g. wrist-bands, watches and other form factors).[5]

SECORA™ ID is the Infineon solution allowing easy eID introduction

SECORA™ ID is a new flavor of the SECORA™ brand. Infineon developed SECORA™ ID on the code base of SECORA™ Pay, extended by the additional features, which are required for Identification solutions.

SECORA™ ID is an enablement platform that allows security printers and card manufacturers to continue their path towards digitalization. The solution supports contact based, dual interface, as well as contactless applications to allow a smooth migration from contact-based to contactless reader infrastructures.

Infineon Technologies has developed all the components of SECORA™ ID: The chip hardware, the packages, the OS platform, as well as the Applets. Consequently, the OS is implemented in a way to reach maximum performance. In addition, Infineon can offer best in class support for each card component.

SECORA™ ID is designed based on the latest Java Card standard for chip cards, JC Standard version 3.0.5 Classic and compliant to GP (Global Platform) version 2.3.1.

The Solution components

- **Chip Hardware:**
  SECORA™ is based on the SLC52G platform which is a sophisticated real 16 bit Intel platform with the Infineon double CPU security technology (Integrity Guard) SOLID FLASH™ and VHBR (Very High Bit Rate) up to 6.8 Mbit/sec. SLC52 is CC EAL 6+ high certified according to Common Criteria. The security controller has been developed by

Infineon Technologies in Munich and in the contactless competence center in Graz.

- **Package (Module):**
  Infineon Technologies provides a comprehensive packaging offering. The most innovative package technology is Coil on Module based on flip chip technology, which allows easy integration of contactless and dual interface inlays in cards, as well as in electronic passports. Coil on Module is based on inductive coupling. Inductive coupling between card antenna and module antenna does not require a mechanical contact connection between antenna and module, which increases durability and robustness of smart cards.[6]
- **OS Platform:** SECORA™ ID
- **Applets:** Applets from Infineon and several vendors.

SECORA™ ID Offering

SECORA™ ID is a lean operating system with planned security certification CC EAL 6+ with two configurations:

- With SECORA™ ID, Infineon offers comprehensive Applet choices for the major eID applications from different well-known and acknowledged vendors: The Infineon in house developed “Infineon Applet Collection”, the “ePasslet Suite by cryptovision GmbH” as well as the “Applet Collection by Masktech GmbH”. The Applets will be CC EAL 5+ certified according to the relevant protection profiles.
- For maximum customization, Infineon provides Java Card development tools based on Eclipse to enable the customer to implement their own Applets according to proprietary or local requirements. The development tools contain a simulator, as well as personalization scripts for standardized applications like eMRTD according to ICAO 9303.

SECORA™ ID portfolio comprises the S and X variants.

- SECORA™ ID S is designed for use cases like e.g. electronic ID cards, electronic passports, digital signature, electronic driving license, health card.
- SECORA™ ID X, the high-performance version for ID applications is optimized for use cases with multi-application, as well as for the support of LDS 2.0.[7]

Use Case Examples

eID (electronic Identification) with ICAO 9303 eMRTD:

A basic eID which is used to store personal data consisting of personal information, facial image and optional fingerprints can be used for local identification and border crossing between dedicated countries, which have a common travel agreement.

This use case can be enabled with SECORA™ ID in combination with the ready to go Infineon Applet Collection.

eID with ICAO 9303 eMRTD and digital signature:

An eID based on an ICAO 9303 eMRTD Applet, which is used to store identification data. In addition, digital signature is used for authentication, which could be applied, for example to authenticate at a governmental web service.

This use case could be supported with SECORA™ ID S in combination with the ready to go Applet Collection by Masktech GmbH.

eDL (electronic driving license) based on ISO 18013:

The electronic driving license contains personal information and the license for the different vehicles the user is allowed to use.

This use case can be supported by SECORA™ ID S in combination with the Infineon Applet Collection.

High end multi-application electronic ID card with post issuance:

Requirements for this use case are as follows:

- eID card for identification and authentication, which can be extended during its life time with an e-health card application once the specification is in place.

- The ePasslet Suite by cryptovision GmbH could support this use case as this solution is optimized for multi-application. The Java Card platform allows post issuance, which is necessary to extend the functionality of the card in the field after issuance of the card.

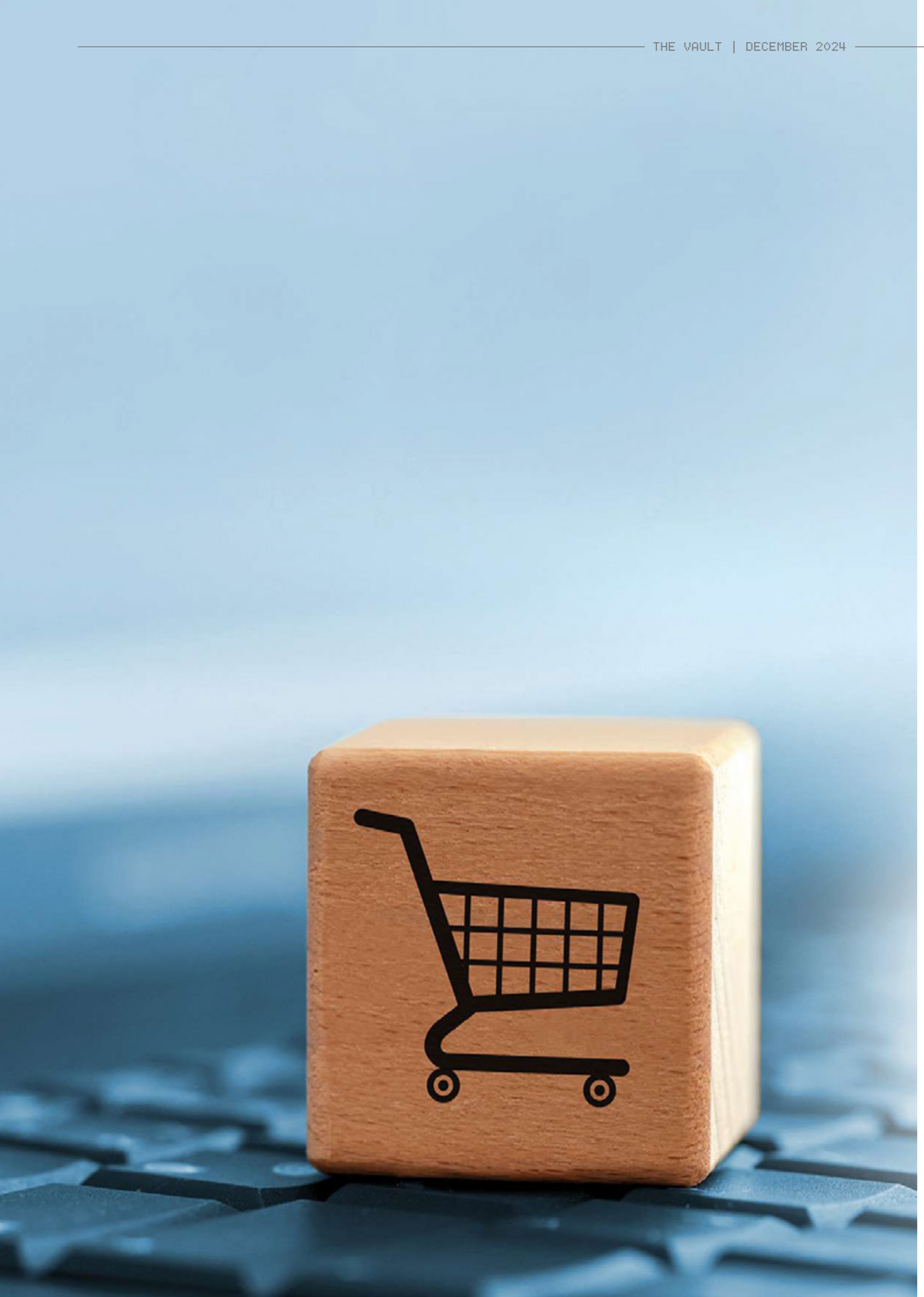
Conclusion

SECORA™ ID is a flexible solution for eID applications, which allows maximized customization for local needs. All components of the solution, like chip hardware, packages and software, comes from one vendor, which simplifies the process and enables a rapid eID project realization.

SECORA™ ID will be launched by Infineon Technologies at the Trustech event in Cannes in November 2019 (https://www.trustech-event.com). ☒

Sources & Notes

1. Java Card forum: https://javacardforum.com/
2. https://www.oracle.com/java/technologies/java-card-tech.html
3. Source: ABI research – SIM Cards report
4. https://blogs.oracle.com/javaiot/java-card-forum-20-years-anniversary
5. https://www.infineon.com/cms/en/product/security-smart-card-solutions/secora-pay-security-solutions/
6. More information about Coil on Module Technology is available here: https://www.infineon.com/cms/en/product/promopages/coil-on-module/
7. Find more about LDS 2.0: https://www.infineon.com/cms/en/applications/security/government-identification/electronic-passport/



DELEGATED Authentication – ABANDON *FRICTION*, NOT the *cart*

Megan Shamas, Senior Director of Marketing, FIDO Alliance

Online sales surged in response to pandemic-related closures of brick-and-mortar shops and global ‘stay home’ restrictions. However, as restrictions have eased, changes to consumer behaviour have endured, with the convenience of shopping online set to stay.

Fraud has also grown at a frightening pace. The European eCommerce market is expected to hit $465bn this year, 30% more than before the pandemic struck. Losses as a result of fraud however have risen by a staggering 87% in parallel.

Robust security is more important than ever. But while several financial services players have implemented additional authentication methods to improve security, there is still much work to be done, and we are also seeing a secondary knock-on effect that is damaging the user experience. ‘Step-up’ verification processes - such as push notifications and SMS one-time passwords (OTPs) are inadvertently exacerbating an issue that is top of any online merchant’s mind - cart abandonment (which nearly 40% of consumers cite as a likely outcome when they have account login issues).

What are the common challenges ‘step-up’ authentication creates? And how can new authentication alternatives offer merchants better security and more control of the user experience?

The authentication problem - fighting fraud with friction

Legacy ‘step-up’ authentication methods have become widely used in response to strong customer authentication (SCA) mandates, but have added more friction to the checkout process. Disruption during the checkout means as many as 22% of all payments verified via EMVCo 3D Secure – the online payments security specifications used by most major banks – are not completed.

70% of users prefer an authentication solution based on its convenience - something OTPs and passwords are not known for. In fact, 64% refuse to use SMS OTPs altogether. Similarly, push notifications to the user’s banking app also create drop-offs in the

> *Delegated authentication enables qualified merchants or wallet providers to use their own authentication or log-in processes to approve purchases.*

payment chain, as users have to switch to a different app. This method has limited reach too, as it's estimated only half of users have the app installed.

Forrester research suggests brands can lose over $18bn a year from cart abandonment. Complex checkout and registration processes are also driving more consumers to guest checkout options – something even more likely if using a smartphone. This means less valuable customer data captured, a lost chance for loyalty and on average, lower spending, as registered customers usually spend more.

Legacy 'step-up' doesn't solve the security problem

The added security benefits of these 'step-ups' are limited, too. SMS OTPs are still susceptible to social engineering, meaning fraudsters can trick consumers into divulging their codes directly. A more advanced technique called 'SIM swapping' whereby information found publicly and / or divulged via social engineering is used to impersonate the victim to mobile network operators and take control of the number. A high profile example of this hit the headlines recently as a Canadian teen used the technique to steal $36 million dollars of cryptocurrency. Moreover, the banking apps we are directed to via push notifications are still often underpinned by legacy 'secrets' such as passwords rendering them ultimately less secure.

A new solution called delegated authentication is emerging as a direct response to these issues, enabling merchants to take control of the authentication process and achieve that rare combination of stronger security with a better user experience (UX).

What is Delegated Authentication?

Delegated authentication is a new and innovative solution in the payment and authentication industry that leverages open standards from industry bodies such as FIDO Alliance and EMVCo -- standards that reflect broad contributions from industry platform and payment stakeholders such as Apple, American Express, Google, JCB, Microsoft, Mastercard and Visa.

Delegated authentication enables qualified merchants or wallet providers to use their own authentication or log-in processes to approve purchases. For the first time ever, it allows merchants to link customer accounts with the 3D Secure payment verification process used by banks. This makes it possible for users to securely log into their merchant account and simultaneously authenticate themselves with their payment provider or bank in advance of making a purchase.

This means that once enrolled, checkouts couldn't be simpler for end users. They just need to log-in and select the card or payment type they want to use when making a purchase. Because they have already been automatically verified by their payment provider or bank when logging in to the retailer, there is no need for any additional 'step-up' verification when checking out.

Why Delegate?

Comply with PSD2 SCA

Europe's financial services industry is acutely aware of PSD2 (Payment Services Directive 2) and its mandate for SCA, requiring two factors of authentication (2FA) for banking services or payments.

Delegated authentication can link the incoming bank challenge message with the transaction details to enable customers to verify themselves in line with 2FA in one action:

- **Possession.** The consumer possesses an authenticator that is either in a general-purpose (e.g. smartphone) or separate device (e.g. smartcard, security key). As such, authentication validates possession, thanks to the use of a private key securely held in the device.

- **Biometric data or knowledge.** The second element consists of either an inherence factor like biometrics or knowledge, such as a PIN or geometric pattern, verified locally by the authenticator.

Improve user experience

2FA doesn't need to mean two steps to verification. With delegated authentication, users can demonstrate two factors of authentication with a single gesture.

Using new delegated authentication industry standards gives consumers the choice to use different form factors such as an authenticator integrated into their smartphones; and their preferred gesture, such as fingerprint, facial verification, or a PIN. This harmonizes the user experience across sites, and avoids the need to use a different type of authentication method when different exemption criteria apply, such as transaction value.

Build customer relationships

Offering authentication from your own platform is invaluable to merchants, as it not only enables a better, passwordless checkout experience for customers, but it also encourages customers to make purchases while logged in. This fosters greater customer loyalty, decreases guest checkout usage, and results in higher spending with logged-in customers estimated to spend around 10% more.

Strengthen security

Selecting leading open standards such as FIDO means delegated authentication can benefit from a privacy-by-design approach and have a strong resistance to phishing and man-in-the-middle attacks, whereby attackers interrupt an existing conversation or data transfer by inserting themselves in the middle.

Depending on the implementation, delegated authentication leverages the robust hardware security inherent on the device – in a smartphone, this is the trusted execution environment (TEE), for PCs it typically is a TPM. This use of hardware security is a key element of FIDO's approach - no sensitive data is ever shared with third parties, protecting privacy, merchant liability and security.

Abandon friction, welcome sales

Strong authentication doesn't have to mean introducing unnecessary friction. Delegated authentication offers merchants and wallet providers the opportunity to take their SCA compliance to the next level with a better user experience that doesn't cost them sales. While solutions like passwords and SMS OTPs may tick the box of compliance today, delegated authentication will better safeguard merchants and users now and in the future, as less secure authentication methods may come under further scrutiny and be written out of regulation as not safe enough.

In a thriving market for online retailers, it's the perfect time to act. Offering a better checkout experience now can ensure merchants build better relationships with customers, and do not let sales needlessly slip away. ☒

Can we TRUST *Artificial INTELLIGENCE*?

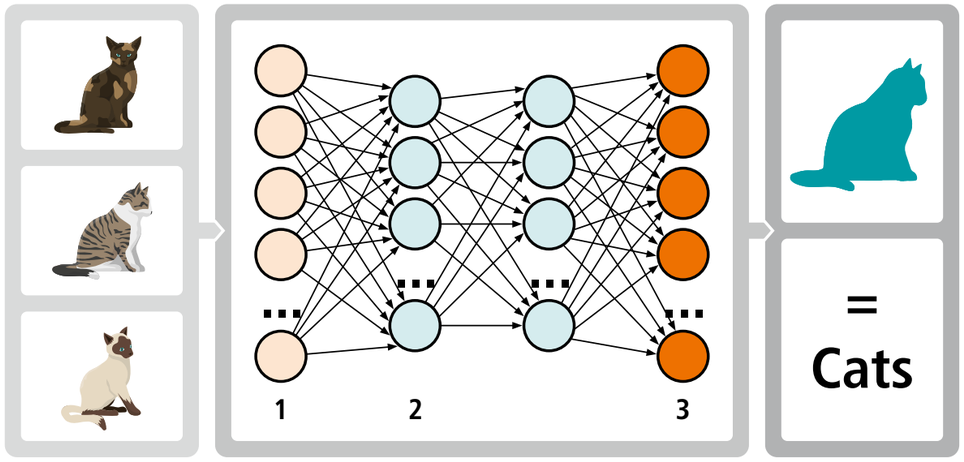
By Dr. Carmen Kempka, Wibu-Systems

The possibilities of artificial intelligence and machine learning seem endless. Neural networks and deep learning techniques are utilized nearly everywhere. Their actual or potential use cases range from speech recognition, malware detection, and quality testing to applications that could be critical for people's lives and limbs, like driver assistance systems or medical diagnostics.

In safety-critical environments like these, it is essential to use new and untested technologies in a responsible manner, especially those like AI that are not yet fully understood. An attack on an AI application in this context, or even a simple malfunction, could have life-threatening implications. An incorrect classification could lead to a wrong medical diagnosis and, by implication, incorrect treatment or, more directly, get a driver assistance system to cause the car to crash.

Moreover, especially in the medical sector, AIs are trained on sensitive patient data for which confidentiality and the patient's anonymity are paramount. This data could be a CT or MRT scan, or information about the patient's medical history. In addition, AI models are often trained with complex training parameters which, like the trained model itself, contain intellectual property.

All in all, protecting the machine learning lifecycle against tampering and unauthorized access to functions and data is a complex undertaking that requires sophisticated solutions. But before we look deeper into the attack surfaces and necessary protections for the machine learning lifecycle, we first need to investigate one important question:



The cat graphics created by macrovector / Freepik

Figure 1

How intelligent are AIs, really?

Neural networks and deep learning algorithms have been designed to imitate the way the human brain learns things. However, each AI is trained on a very limited selection of data – compared to a human being, at least. A neural network does not have the same experience as the human brain. It has no lifetime of adventures with all their ups and downs to process. It has no common sense to work with. It gets a very limited set of input data, tailored to a specific use case, like images of animals, traffic data, or CT scans, for which it learns to provide some classification.

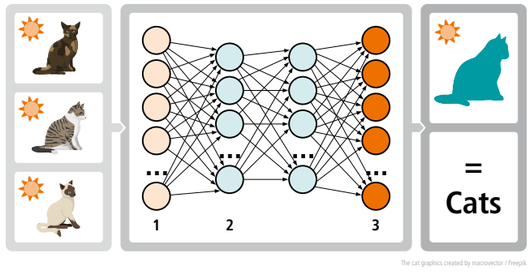
Most importantly, no AI actually "thinks" about its input data or the trained model in any way. There is no sanity check whether the input data or the inferred classification criteria make any sense at all.

Let's consider the following example: Imagine an AI that gets pictures as training data. Some of these show a cat and are labeled "cat" (Figure 1) while some show a dog and are labeled "dog". If the data to be classified after training is similar enough to the training data, the AI will distinguish cats from dogs correctly.

Now, imagine the cat images all have a sun in the picture (Figure 2) while the dog is always sitting in the rain. Now the AI will learn something like "cat-like animal and sun" means cat, and "dog-like animal and rain" means dog.

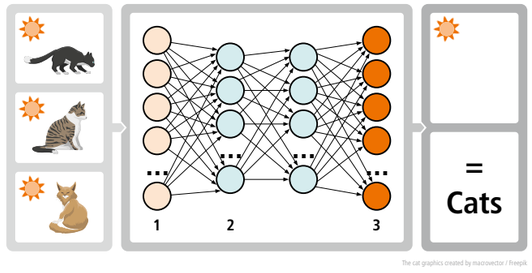
Even worse, if the cats and dogs are hard to distinguish or all cats/dogs look different, the AI will instead learn "sun means cat and rain means dog", not even considering the actual animals anymore in the classification process (Figure 3).

To make things worse still, instead of the sun and the rain, a potential attacker could color certain pixels in the training images to cause a certain classification behavior, even if these changes in the training data would not even be noticed by the human eye.



The cat graphics created by macrovector / Freepik

Figure 2



The cat graphics created by macrovector / Freepik

Figure 3

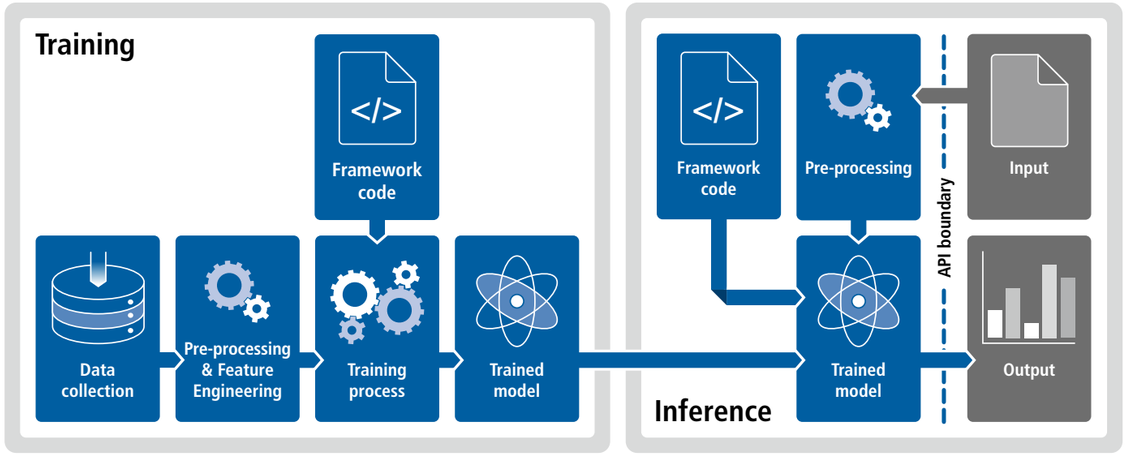


Figure 4

The ML lifecycle

In addition to neural networks and deep learning, there are several machine learning techniques based on math and statistics, such as separating data by a hyperplane or predicting data by putting a line through known points or by building decision trees. No matter which machine learning technique is used, there are common steps on the way from the raw training data to the trained, deployed, and used model. We call these steps the machine learning lifecycle, which can roughly be described as follows (Figure 4).

First, the raw training data needs to be preprocessed to provide the training algorithm with a homogeneous set of data. Preprocessing will, for example, scale all training images to the same size or delete unnecessary columns in tables. The actual training is then performed on the preprocessed data, resulting in a trained model which can be deployed and used for classification. In some cases, the model keeps training itself during use, utilizing the user's input as additional training data.

This can happen in the context of anomaly detection or clustering or the notion "people who looked at this also bought…", which means that this data – considered potential training data which could affect the quality of the model – must be protected and processed with similar care as the original training set.

Protecting the machine learning lifecycle

The machine learning lifecycle has a number of stakeholders who are interested in different protection targets: The data owner, who provides the training data, might want the data to stay confidential and anonymous. The machine learning engineer, who uses the training data to train the model, wants both the training data and the algorithms used for preprocessing and training to be of high quality and not tampered with, while the used training parameters, which often contain intellectual property, must stay confidential. The model owner, who deploys and provides the trained model, wants the intellectual property within the model to be protected and is interested in the correctness and integrity of the model, which requires the integrity of the whole machine learning lifecycle, including training data, training parameters, and algorithms. To realize business models or simply prevent model inference, the model owner might apply access controls and licensing techniques to the trained model. The customer who accesses the model to get a classification is interested in the correctness of the classification, which also requires the integrity of the whole machine learning lifecycle. The customer's query might contain data which requires confidentiality or which has the potential to be malicious and requires checking.

> *One peculiarity in the case of machine learning, especially neural networks, is that keeping the trained model confidential is not enough to prevent fraud.*

The role of software protection

The attack surfaces of the machine learning lifecycle are many. As mentioned above, any manipulation of any data or any algorithm used within the machine learning lifecycle can have fatal consequences. In addition, the confidentiality of sensitive data and intellectual property must be protected.

One peculiarity in the case of machine learning, especially neural networks, is that keeping the trained model confidential is not enough to prevent fraud. Unrestricted access to a trained model can be abused to train a second model using input/output pairs only, which can get very close to the original model in terms of classification behavior, or to evade the classification of the original model, for example, in the case of malware or deep fake detection. Therefore, limiting access to the trained model might be a reasonable or even necessary precaution.

Software protections safeguard applications from tampering and theft and enable the software provider to put in place business models like pay-per-use or a subscription. The protection suite developed by Wibu-Systems offers an all-round toolkit for the defense of both executables and data. While executables are protected from reverse engineering, we do not consider “security by obscurity” enough to protect an application. Executables or sensitive functions are encrypted using well-established cryptographic algorithms. In addition, cryptographic methods are utilized to protect the integrity of software and data. Functions and data are decrypted at runtime. Sensitive parts of the code can even be decrypted and executed and key material or certificates be securely transferred and stored in secure hardware. This does not only keep the key material secret, but it also prevents the manipulation of keys and certificates.

AxProtector Python

Due to the availability of open-source frameworks, as well as the popularity of the language, AI applications are often written in Python. AxProtector Python can protect Python applications from manipulation, reverse engineering, and unauthorized use. In addition to executables, AxProtector Python can also protect files like training data, confidential training parameters, and trained models. Data and code are decrypted and checked at runtime. With the ability of AxProtector Python to protect both the framework code used for training and the data used in the machine learning lifecycle, including training data, training parameters, and the trained model, AxProtector Python can protect the whole machine learning lifecycle from manipulation, theft of intellectual property, and unauthorized use.

This way, it can keep patients’ data private or keep cars from speeding into pedestrians because of manipulated classifications, while protecting the complex training parameters of a neural network from being copied. In addition, the ability to license trained models allows for new business models for AI applications, such as pay-per-use access to a classification, a thirty-day trial period, or a monthly subscription.

Protecting the machine learning lifecycle is an essential step towards using artificial intelligence in a responsible way. It’s not only software you protect, it’s also protecting people. ⊠

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

By Robert Bach, Infineon Technologies

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

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

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

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

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

Quantum computers affect conventional cryptography

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

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

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

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

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

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

Post-quantum cryptography

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

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

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

Infineon is pioneering in post-quantum cryptography

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

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

Standardization and adoption is needed

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

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

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

Approaches towards post-quantum cryptography

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

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

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

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

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

Migration strategies towards post-quantum cryptography

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

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

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

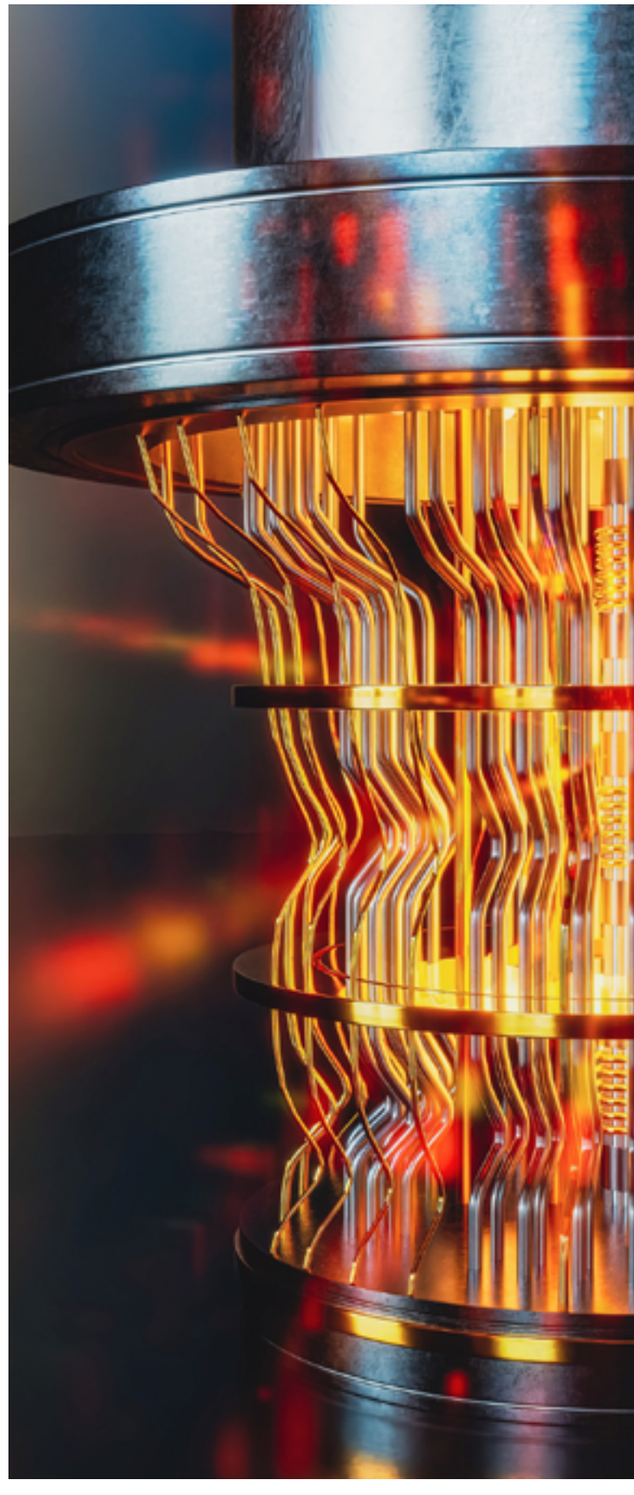
Crypto agility @ Infineon

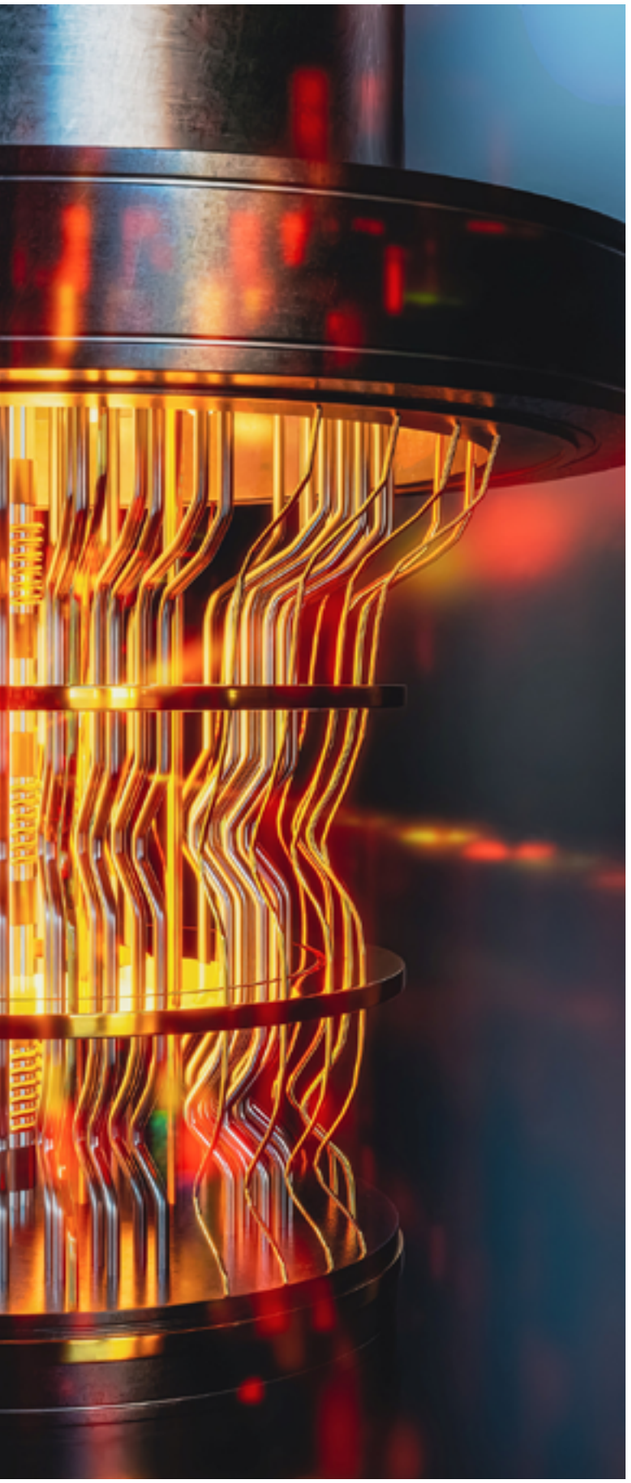
The underlying software update mechanisms must be properly safeguarded for crypto agility to work. Infineon has taken a first step towards providing the necessary safeguards by implementing future-proof, quantum-resistant software update mechanisms on its widely used Trust Platform Module (TPM): OPTIGA™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

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

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

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





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

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

Recommendation: Early preparation is key

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

Government should begin by

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

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

Securing future eHealth systems

With eHealth set as a 2010 focus topic for the Silicon Trust, representatives from the organization's Executive Committee – Gemalto, Giesecke & Devrient and Infineon Technologies – came together to discuss some of the key issues surrounding eHealth applications.

Security-News.tv spoke to Stéfane Mouille, Gemalto; Axel Vonderhagen, Giesecke & Devrient and Tolgahan Yildiz, Infineon Technologies

Could you give us your opinion on some of the main drivers for eHealth applications?

AV: From our understanding and past experience, we notice that the health systems and the communication of doctors are based on different media – this is one driver that I will explain later. One main driver is the quality of patient treatment – better quality of treatment can be achieved if the doctor knows the full patient history. A second driver, especially relevant in Germany, is fraud. ID cards are very simple and a stolen eHealth card can be used without anyone checking the authenticity. Another driver, as I mentioned earlier, is the administration process: There are complex paper based communication processes, even though most doctor's offices should now be computer based. I therefore think that the administration processes need to be updated to a paperless workflow.

In terms of paperless workflow - what are the data management requirements within an eHealth project?

TY: Obviously there are different sets of data involved in a typical healthcare project, depending on the country, type and amount of data, so it's difficult to give a mainstream solution. I could give you an example of two different extremes: one extreme is that there is a minimum amount of data on a card and most of the data is stored in the background system, and the card is only a key to access the system. The other extreme is, that there is more storage on the local medium, like a card or USB stick, where there is no limit - you can store as much as you want including full medical history, but of course that might be sensitive information too. These two extremes exist and the solution is normally customized according to the needs, requirements and laws of the countries.

Looking at ePassports for example, there is some rigorous standardization involved on an international level with a strong focus on interoperability – do you see the same issues in eHealth?

SM: First of all, standardization is really important for guaranteeing the interoperability in any given system. Knowing that, the first interoperable need is on a national level to guarantee that the ecosystem is connected in the right way – by that I mean the doctors, pharmacies, hospitals and the health insurers. It is really important to have a national standard and today this is mostly the case, thanks to ISO or national organizations.

Currently, the next step is on a European level to ensure the quality of citizens' health insurance even when abroad. We see that European standards are popping up and the CEN, which is a European standardization committee, already published some standards for interoperability called eEHIC, for European Health Insurance Cards. These are already available and have already been implemented, and we have seen some European projects, for example Netc@rds, which is a consortium of 16 health insurers in Europe, contributing to this ambitious project. They are already creating a framework for interoperability based on these eEHIC standards, to guarantee that the French citizen who visits Germany can use his French eHealth card to prove that she or he is insured under French insurance. So this is very important, and at least for the European continent it's a key issue for the next few years.

Going back to ePassports, another technology that is being introduced is biometrics – do you see this form of authentication being used in the eHealth domain?

TY: I don't think Biometrics is used as much in eHealth cards as in ePassports. What we see is the effort to increase the match between the person and the card in order to avoid fraud for example. And here we see the different methods - such as multi-functional authentication, in Austria where the card is only used as a key to the system and where you only have single factor authentication, which is cards. Another extreme in Germany, where there are four different factors of authentication: patient card, doctor card, plus both the patient and the doctor have a pin number and only with all of these factors the doctor has the right to access the data.

I think, biometrics come into the picture when there is a multi-application solution – if an eHealth product is also used as an ID product nationwide, such as in Portugal or Turkey, then there might be use of biometrics.

What developments are there in terms of patient data storage?

AV: As discussed, we have the two extremes, either you are saying that the card is only being used as a key to a back end system, or that the card stores all the data in the card - both scenarios have their own advantages and disadvantages.

Lets have a look at the German model, which divides a little bit. There is special (emergency) data and some medical history data stored on the card itself, however this is also mirrored in the back-end system too. So I would say that here the card is being used as medium sized storage. But the card is also being used as a key for the back-end system.

> *There are different sets of data involved in a typical healthcare project, depending on the country, type and amount of data, so it's difficult to give a mainstream solution.*

One big advantage of having the information on the card, is that you immediately have the emergency data if there is something wrong with the infrastructure, but then of course you have the disadvantage that if you lose your card, and the data is only on the card, and not mirrored in a back-end system, then the user faces a problem.

The second part is the data protection issue. In Germany there are a lot of discussions about which data is allowed to be stored on the card and how secure the card has to be – this often comes down to each country's laws. So the discussion surrounding what and where the data is stored is difficult. I would say that it is up to the individual country and its laws to decide where to store which data.

What impact does the chosen storage solution have on the hardware?

TY: In countries like Germany, where you want to store patient data on the card, it has a direct impact on the size of the memory on the IC. If you have some pre description of the medical history and prescription information – this in Germany for example is a minimum of 80 Kilobytes (kB) EEPROM, but you can go down to 8 kB if you only want a single key to access the database. If you want to store everything about the patient on the chip then you can easily reach Gigabyte range, which is not really feasible in a card form factor.

What sort of impact do you think the storage will have on security? How can we ensure that only the right people have the access to the information?

TY: Security of the hardware or the solution is also a measure to prevent fraud, because fraud is one of the major drivers. In order to achieve tamper proof secure hardware, most of the governments worldwide choose security certified microcontrollers, which are certified according to Common Criteria EAL5+ assurance level. Furthermore, at the application level, the confidentiality of the data stored and the access mechanism to the data is managed by use of cryptography.

> *Each project is different because the business process in one given ecosystem for eHealth or social security is unique.*

Today, we would most likely see symmetric cryptography based on DES/3 DES algorithm in the market. We foresee that AES will take the place of Triple DES soon. In the case of Germany we have today asymmetric cryptography with RSA algorithm, for asymmetric encryption maybe in two to three years time we might see ECC (Elliptic curve cryptography). These two security measures would cover major security requirements at device level and application level.

What are the different eHealth projects going on around the world and what are some of the similarities and differences?

SM: What is interesting, is that each project is really different because the business process in one given ecosystem for eHealth or social security project is unique. The legal framework is not homogeneous because it is the responsibility of each member state in Europe and up to each country to define its own social security policy. But what we can see is, that, even though there are differences, there is a convergence of the three drivers that we discussed at the beginning, which are administration cost reduction (dematerializing paperwork to claim electronically); reducing fraud (which was not an issue ten years ago and is quite a new driver) and quality of care (to make sure we have a good track record in treating patients and to avoid errors in prescribing medication).

Europe was the leader in starting eHealth projects within France, Germany and Belgium, followed by Slovenia and Taiwan and, more recently, Algeria. We can see that it is becoming a mass market and we hope that, with standardization efforts in the industry, we can have the same success as the GSM in the future. ☒

Mastering the art of multi-application

By Silicon Trust

Smart card technology is simple, isn't it? Well, yes and no. We all know the technology offers considerable processing power, security and convenience. It also has the potential to transform market sectors as varied as government, payments, transportation and access control. But we don't operate in silos anymore, so we're matching smart technology with smart thinking, enabling different applications to work together in a single multi-application card.

But what's so great about multi-application cards? As we progress into a digital age characterized by convergence, multi-application cards offer advantages for all stakeholders – a factor that is key for successful deployment.

Something for everyone?

Their advantage for consumers is their convenience: they cut the number of cards people need to carry; mean they have to remember only one password or pass code; reduce the need to carry loose change for low-value payments; and even enable citizens to interact with local and national authorities 24/7.

Both card holders and card suppliers benefit from improved security and compliance. For example, in a closed-loop environment a multi-application smart card can be used to provide logical as well as physical access, giving everyone the confidence that the person accessing facilities in a university campus or corporate headquarters are who they claim to be. Furthermore, that same card could also be used to make secure payments in a canteen or at a vending machine. This concept is being taken a step further with the deployment of multi-application cards in open-loop environments. They provide the security needed to identify an individual with tax authorities and social security departments, while also enabling people to use them to make payments, access ATMs and travel across borders.

With the public and private sectors both looking to reduce costs while maintaining – or even improving – security, multi-application cards give issuers the chance to reuse existing infrastructure and slash the total cost of ownership. Further savings are guaranteed because there's no need to go through the costly process of rebadging every time an upgrade is required. Instead it's simply a case of using software to add new features, applications and privileges. Card provisioning can be simplified, further reducing costs. Additionally, help desk costs can be drastically reduced as there will no longer be the need to issue and remind people of passwords. Finally, there may even be procurement opportunities based on using a single supplier for the whole card infrastructure.

Lifecycle management can also be considerably simplified. A single infrastructure for the smart card enables the supplier to offer a single point of issuance and control, and the ability to easily revoke a credential if it is lost or a person loses the right to use it.

Public and private on a single card

There are many ways in which multi-application cards can be applied in the digital world. One area of increasing interest is public and private sector cooperation, where a smart card is issued that combines access to government services with access to commercial applications such as payment and transport. This is an approach taken by a number of nations, including Italy, which started issuing its CNS dual interface cards in 2010. Around 10 million citizens now have one of these cards, which combine eGovernment and eHealth with eTicketing. Russia is also going down this route with dual interface cards that are set for rollout this year. These will enable its citizens to access eGovernment, ATM and eTicketing applications using a single card.

The multi-application minefield

These projects highlight how different stakeholders can work together to provide citizens with simple and convenient cards that can be easily used for so many of their day-to-day activities. What was once the stuff of dreams has now become a reality. But it does take time to get a scheme of this nature up and running and working successfully; although the technology behind multi-application cards is proven, rollouts involving numerous stakeholders can be highly complex.

There are many ways in which multi-application cards can be applied in the digital world. One area is public and private sector cooperation, where a smart card is issued that combines access to government services and commercial applications.

Unlike traditional multi-application campus or corporate cards which are owned by a single entity, public/private cards often have several people or departments jostling for ownership of the card and the project – and all ready to pass the buck should anything go wrong! Stakeholders need to put plenty of thought into building the relationships required to apply multiple applications to a single card.

For example, how do you ensure the alignment of different stakeholders, such as banks and various government ministries in all areas of the project? Who 'owns' it? Who is paying for – and controlling – the financial budget? Who is in charge of every phase, from the tendering process (parts, time, criteria), through pilot (lab tests and field trials) to certification (protection profile and certification targets)? Who has access to the data stored on the card? Who is in charge of issuance? How do you communicate how the card works to end users? How do you ensure everyone trusts the system? Who has the power to revoke the card? Are both contact and contactless cards required? What about printing and branding of the card? How do you future-proof the credential? If every organization and department involved wants to treat it as their 'baby', the whole process becomes a whole lot tougher.

If every organization and department involved wants to treat it as their baby, the whole process becomes a whole lot tougher.

While the projects mentioned so far highlight the real benefits of multi-application technology, deployment isn't without its challenges, particularly in areas such as lifecycle management and post-issuance processes. This is because different applications have distinct lifecycle requirements and require specific treatment such as certificate deployment/revocation. Different post-issuance mechanisms may also be needed to enable new services and security aspects to be loaded, uploaded or upgraded. These make every project unique

In the case of Hong Kong's eID card, the eID function was rolled out in 2004, followed by an eGate application, which was activated in 2006. Finally, an eDrivers License function was activated in 2007. In 2007, Portugal chose to roll out five functions: eHealth, eTax, ePension, eGovernment and eSocial security. This involved input from the country's Ministry of Health, Ministry of Finance and Ministry of National Pensions.

Certification

When it comes to certification, there are often different security requirements for different applications on the same card as each stakeholder has their own specific needs. For example, the level of security required by an ATM provider may be different from that of an eHealth provider. Likewise, an eBanking provider may require different levels compared with the Ministry of Information. Three kinds of certification/qualification are currently used:

- Type approval (functional test according to specification);
- Interoperability testing (in the case of more than one supplier);
- Security certification (a protection profile is needed).

For banking sector applications, type approval is required. Public sector applications require security certification, while large-scale programs require interoperability testing.

Consideration also has to be given to certified and non-certified applications on a single card. Having defined the applications, stakeholders must define the target for type approval, interoperability and security certification. These requests also require the definition of the minimum time they should take. Ordinarily, type approval takes two to three months; security certification can take as much as six months; the pilot phase may need three months; and lab testing may require one month.

Stakeholders need to ensure that reloaded or non-certified applications cannot threaten other secure ones. The best way to achieve this is to define the container in the card. Each container is independent from the other, and each should have its own communication protocol card reader; its own access conditions for the data in the container; and defined and different rights for reading, writing and overwriting data. This approach may well sound familiar, as it's similar to that of a firewall in the ICT world.

Despite the benefits of multi-application technology, deployment isn't without its challenges, particularly in the areas such as lifecycle management and post-issuance processes.

Another approach is to use a UID number on the card as a master key for different services. This could be used for transport (eTicketing) as well as for online services, such as eGovernment, eTax, ePayment, eSocial information and ePensions. However, it could not be used for ATM machines. It's a method favored by Poland, which is using it in the eID card it's planning to role out in 2015. Germany, on the other hand, has not taken this route with its nPA card because it is forbidden by its national laws.

There are many ways to achieve success, but real groundwork has to be put in to avoid the minefield that is multi-application technology. With a growing number of reference cases highlighting how the technology can be deployed, there's everything to play for. But as the schemes in Poland and Germany, and Hong Kong and Portugal highlight, there is no right or wrong way to approach deployment. Essentially, it's all about considering the needs of every stakeholder, at the same time taking into account existing legislation and privacy/security cultures. Simple, really! ☒

Multi-application cards in action

Portugal

The Portuguese Citizen Card is an interesting example of how numerous applications can be housed inside a single document. It was established back in 2007 to replace five different physical ID documents in just one smart card, and is mandatory for all citizens aged over six. It also includes an electronic signature for those aged 16 and over. Since its launch, more than 10 million cards have been issued.

The card broadly covers three main functions – physical, digital and travel document – and guarantees citizen's rights on personal data. Furthermore, it is seen as an important driver for eGovernment. It acts as a physical document that allows the visual identification of the citizen; it is also a digital document that enables citizens to identify themselves and provide their electronic signature for any public act.

At the concept stage, the ministries involved in its deployment had to consider how they would deploy a card lifecycle system that would enable card enrolment, renewal, delivery and cancellation, as well as the activation and revocation of digital certificates plus citizen support. The government also had to implement a card personalization system responsible for the physical personalization, data writing and the digital certificates. Additionally, it needed to implement a PKI responsible for the digital certificates of each card and an EMV-CAP validation system to centrally validate the citizen's authentication with authentication tokens created in the chip's EMV-CAP application. Furthermore, it had to transport the cards to the enrolment and delivery offices so they could be distributed to citizens along with their PINs/PUKs.

The government opted for a card lifecycle system that supports a wide range of biometric equipment from different suppliers, including all-in-one solutions, non-integrated and portable devices, which integrated with the ePassport system. It also supports web-based intranet approaches and enables both online and offline tasks.

India

While Portugal's scheme centers on replacing documents, India's ambitious national eID program represents a big leap for the nation to the latest smart card and biometric technologies.

The project will eventually see all 1.2 billion Indian residents issued with a 12-digit UID number, known as Aadhaar, by the Unique Identification Authority of India (UIDAI). Each ID record will include their individual personal and demographic details and will be associated with their biometric information. The program's aim is to ensure the efficient delivery of public services, allow each citizen to identify themselves so they can use other services such as bank accounts, and enable the government to detect illegal immigrants more easily.

Successful deployment could reduce corruption and improve social security distribution systems for the poor. It could also allow portability of health insurance and pension accounts between employers. Another key benefit is that it will enable the government to bring the country's poor into the formal economy, providing them with valuable access to financial and social services. MasterCard Worldwide is among the private organizations to have become involved in the project. It has developed a solution that will enable citizens to make payment transactions using their UID numbers plus biometric authentication.

The scheme is based on the UIDAI platform and MasterCard's payment network and family of brands. It will promote financial inclusion by enabling account holders with an Aadhaar number to move away from cash and towards electronic transactions. The technology supports prepaid, debit and credit payment products. It will enable participating banks to issue a 16-digit Primary Account Number (PAN) to individuals enrolled into Aadhaar.

INTERNET *of* THINGS – *Security* is a prerequisite for *SUCCESS*

By Dr. Stefan Hofschen, Infineon Technologies AG

The real and virtual worlds are growing together even further to become the Internet of Things through the networking of machines, people and businesses. More and more devices and machines interact independently in networked systems and applications such as Industry 4.0, autonomous driving or smart home.

Especially in the context of Industry 4.0 and the automotive industry, the increasing connectivity provides a great number of opportunities for the economy. Yet, it also presents great challenges for businesses, foremost in questions of data security. How can business secrets and intellectual property be protected on the open Internet? How is data protection and confidentiality ensured? How secure is the communication between the different devices or components? And how can attacks be recognized and potential damage prevented? In short, data security and system integrity are essential for the success of new business models, because they protect the availability and reliability of products and services.

Internet of Things in the example of Industry 4.0

The next revolution in industrial production, the so-called smart factory or Industry 4.0, presupposes a secure data exchange. Intelligent machines, storage systems, production facilities and intelligent products are connected globally. This networking increasingly also takes place between supplier and customer, especially for large or mid-sized companies. Figuratively speaking, Industry 4.0 opens the doors to the factories. This openness increases the need to prevent manipulation and sabotage of networked production systems and avert related financial losses. After all, smart factories can only be put into practice and accepted when they can be implemented in a stable and efficient manner, and when the process know-how and intellectual property (IP) is protected reliably.

Figuratively speaking, Industry 4.0 opens the doors to the factories. This openness increases the need to prevent manipulation and sabotage of networked production systems and avert related financial losses.

At the IT Summit 2014 in Hamburg, Infineon, Deutsche Telekom, Fraunhofer SIT, TRUMPF, WIBU-SYSTEMS and Hirschmann (a Belden Company) demonstrated how a “security solution made in Germany” can be implemented in industrial applications. The demonstration shows how seamless communication security works beyond the boundaries of sites or businesses. An employee at the Munich site starts a production order on his tablet PC and transmits it via a secured communication channel to the production site in Hamburg. The order is then automatically executed by a production machine there.

Security controllers protect networked IoT systems from unauthorized access and manipulation

Industry has come to understand that connected systems cannot be adequately protected with software alone. The combination of software and hardware offers significantly more efficient protection against attacks and manipulation. Depending on the application scenario, there are special security chips that take the required security standard and the application’s efficiency optimisation into account.

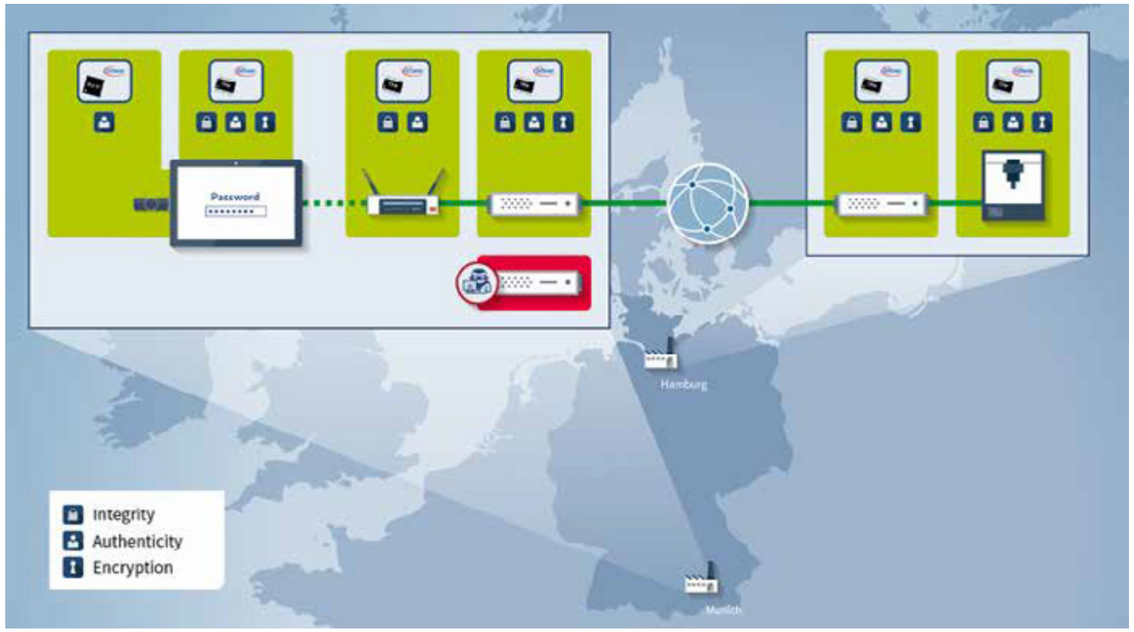


Figure 1: Seamlessly secured end-to-end communication (diagram of the demonstrator solution presented at the IT Summit 2014)

To secure the communication from one end of the value chain to the other (Figure 1), security controllers – in this case Trusted Platform Modules (TPMs) – are integrated in all devices of the IT network (tablet PC, wireless access point, router, production machine). They function as data resource, and as encryption and authentication components. They fulfill multiple functions at the same time:

- Similar to electronic identity verification, they securely identify the individual system components. Only authorized persons and devices obtain access to the network.
- At the device level, they are the basis for detecting manipulation or attacks on components or on the device itself. This way, both logical as well as physical attacks can be detected and corresponding pre-defined measures can be initiated.
- As a Secure storage location, they secure secret information that is needed to encrypt a secure communication channel.

The solution fulfills particularly high security requirements because the security controllers are evaluated and certified by the BSI (Federal Agency for Security in Information Technology) as well as according to “Common Criteria”, an international standard. The certification meanwhile is not only granted at the product level, but also includes the complete production and supply chain. This affords the greatest possible security to the users and increases flexibility in the users’ own production.

A secured complete system was presented as the first prototype at the IT Summit and the solution is to be marketed as soon as possible in 2015. The hardware components already exist today, so that further scalable solutions can be developed for every other application case.

Trusted Platform Module as security anchor for end-to-end communication

Thus far, communication within company networks is primarily secured by means of pure software solutions. However, these harbor a few drawbacks compared to hardware-based security such as a TPM (Figure 2) and they are inadequately secure over the long term. Software in principle always consists of written code that can usually be read, copied or overwritten relatively easily, which enables attackers to bypass the security functions programmed by it. The TPM in contrast can serve as a security anchor for components and software: keys that are stored in the TPM are protected from leaving the security chip and are used in combination with authorization only.

Software in principle always consists of written code that can usually be read, copied or overwritten relatively easily, which enables attackers to bypass the security functions programmed by it.

Figure 2: OPTIGA™ TPM (Trusted Platform Module) from Infineon

At the same time, the TPM that is installed on the motherboard uses international standardized cryptographic algorithms. Integration is provided via standard interfaces like I2C or LPC. The module also permits for example, that keys, data and digital signatures are stored securely, verified and transmitted. The TPM is equipped with a special internal processor for the purpose of the aforementioned authentication and encoding, which enables it to generate keys in a trustworthy environment. At the same time, a specialized crypto processor system allows the quick calculation of RSA cryptography at up to 2048 bits and thus permits the secured execution of complex cryptographic operations. A non-volatile memory with its own encryption preserves important data and keys stay on shut-down.

The integrity of the software structures and the executed programs on the system can be checked in that the boot process of the system is logged and confirmed against stored cryptographic checksums. Any manipulation of the software can thereby be recorded and stopped, by shutting down the affected components or disconnecting them from the network. This way, also the execution of malware like viruses, Trojans and worms can be detected and their spread stopped. Otherwise, this malware can execute unnoticed in the boot process and even spread throughout an enterprise without detection.

Long-term planning reliability – the Trusted Computing Group (TCG) sets standards for industry and consumers

TPMs are based on the open standards of the Trusted Computing Group (TCG) and have already been used for many years in PCs and notebooks. New applications benefit from this experience of many years. In its certification program, the TCG documents all those TPM products that officially meet the standard and thereby provides better orientation in the market for all users. The standard furthermore presents additional benefits: the detailed specifications of the TCG improve the compatibility of the multitude of different operating systems and customer applications. Users can combine different solutions at any time in the design of the system architecture and thus they also have long-term planning reliability.

More and more networking, however, also raises the security requirements in other areas. The TCG already reacted early on to this development and designed the new TPM 2.0 Standard in such a way that a multitude of applications can be covered. Special attention has been given to security in embedded systems for everything from routers to automobiles and medical devices.

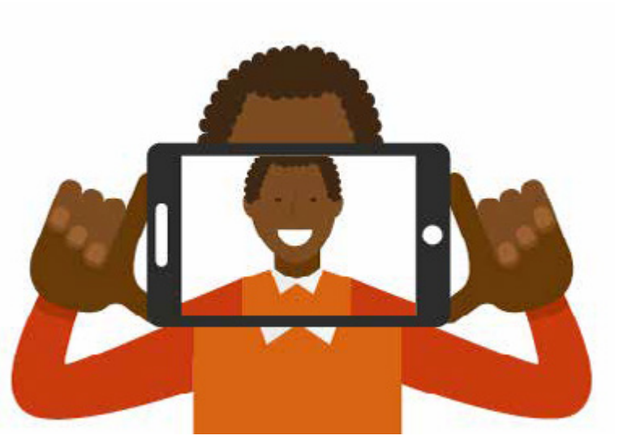
Conclusion

In the Internet of Things, individual devices and components must no longer be viewed in isolation. A forged spare part or manipulated firmware updates on a production machine are sufficient to already cause damage to the entire production chain. By means of specific security chips, networked systems can be optimally protected to a vast extent. Meanwhile the fields of application are manifold: be it Industry 4.0, automotive connectivity, building automation, smart home or eHealth applications. Regardless if a clinic doctor is checking her patient's medication or a 3D printer producing a component, data security and system integrity are prerequisites for the success of the Internet of Things and the related products and services. ☒

Enabling MOBILE ID Trends

eID Documents have a high security level and are under full control of the government, however realizing practical real world use of these documents is difficult and typically requires specialized hardware readers in a PC environment. The trend for mobility and BYOD is driving the need for different use cases that utilize the eID as a trust anchor – such as deriving credentials from the eID or tokenizing certain aspects of the document as a companion to the document. These strategies are limited in scope, and not as secure as the eID itself, offering the security of a software certificate, which can be copied or duplicated.

By Adam Ross and Benjamin Drisch, cryptovision



☐ Could mobile devices ever be used as a replacement for an eID? Using an embedded secure element, enhanced SIM, or secure micro SD card in a phone or tablet could provide a security equivalent of a sovereign eID document, but how are these SE's provisioned? Who controls these aspects, the chip manufacturer, the device hardware manufacturer, the MNO, the application developer? Because there is no clear trend, the market is fragmented, creating a need for specialist solutions for each implementation.

National governments around the world are shifting their focus from traditional security printed documents to issuing highly secure electronic identity cards.

National governments around the world are shifting their focus from traditional security printed documents to issuing highly secure electronic identity cards. Currently, the number of countries issuing smart eID cards exceeds the number of issuers of traditional paper documents by nearly 4 to 1. While the typical aim of these governments is to increase the security of the document with a chip, the inclusion of these chips also enables a number of diverse uses, for example digital signing or two-factor authentication. However, these use cases typically require specialized card readers and middleware software to be used in PC environments.

Just as there is an overwhelming increase in the number of eID cards being issued, there is perhaps an even larger growth in the number of mobile and tablet devices that are used by billions of people worldwide. The computing environment is no longer bound to wired workplaces or WiFi networks in homes. It now extends to everywhere mobile devices can travel and this convenience is driving a demand for extending the usage of eID documents to new mobile platforms. By making the use of an eID convenient on personal devices that citizens carry with them practically everywhere, governments hope to encourage the usage of these documents by the cardholders or commercial services.

One such strategy for bridging the gap between using an eID and the need for mobility was adopted in Estonia, with the Mobil-ID product. This service allows for an eID cardholder to use their mobile phone as an additional form of secure electronic ID to access government e-services, strong authentication to commercial websites, and sign documents digitally without the need for a card reader. It is even possible to electronically vote on the Internet via the phone's web browser. The Mobile-ID software process requires equipping the mobile phone with a specially enhanced SIM card, one with an additional secure element for storage of the digital certificates and key material from the citizen's eID card.

This strategy of using the eID card as a trust anchor for replicating the same identity on another device, is commonly referred to as derived credentials. These derived credentials, enable more efficient and effective authentication, while still ensuring the security and integrity of mobile device information access. The combination of assured digital identity security, with a new degree of convenience, is sure to drive many new use cases and potentially reshape the way governments offer and deliver eGovernment services to their citizens.

One of the key concerns of using derived credentials on a mobile device, is how to effectively store the digital certificates and private keys that are derived from the eID. Since the use of derived credentials is relatively new, it is still very much of a "wild West" environment, where there is no simple answer. There are techniques that could involve using an embedded secure element, enhanced SIM, or secure micro SD card in a phone to provide a security equivalent of a sovereign eID document, but how are these secure elements provisioned? Who controls these aspects – The chip manufacturer, the device hardware manufacturer, the mobile network operator, the application developer, or perhaps the document issuer? Because there is no clear trend, the market has fragmented, creating a need for specialist solutions for each implementation.

One of the key concerns of using derived credentials on a mobile device, is how to effectively store the digital certificates and private keys that are derived from the eID.

It is clear that mobile phones will never completely replace eIDs, especially since they still need to function as an ID document for visual inspection, so there is a real need for special solutions that allow mobile application developers to bridge the gap between an eID and mobile device. Mobile application developers typically have no experience or understanding of the security features of an eID document; there are very few applications using them. However, eID experts like cryptovision can deliver a comfortable programming interface that allows application developers to interface with the documents programmatically in a simple and familiar fashion. This enables mobility trends that improve the convenience of using eIDs, while still preserving identity security. ☒

eID Migration FROM *Physical Card* to *MOBILE* ID

By Steve Warne, HID Global

Everyone now looks upon the 'mobile lifestyle' as completely normal. For instance, for a recent London conference visit I booked my train tickets and parking, and then had them delivered to my smartphone. I checked in to my hotel via my smartphone. I took a call and read emails on my smartphone. All very normal. The whole process of leaving my home, getting into London and checking into the hotel was all facilitated via my smartphone. I couldn't operate without it anymore. And I am not alone.

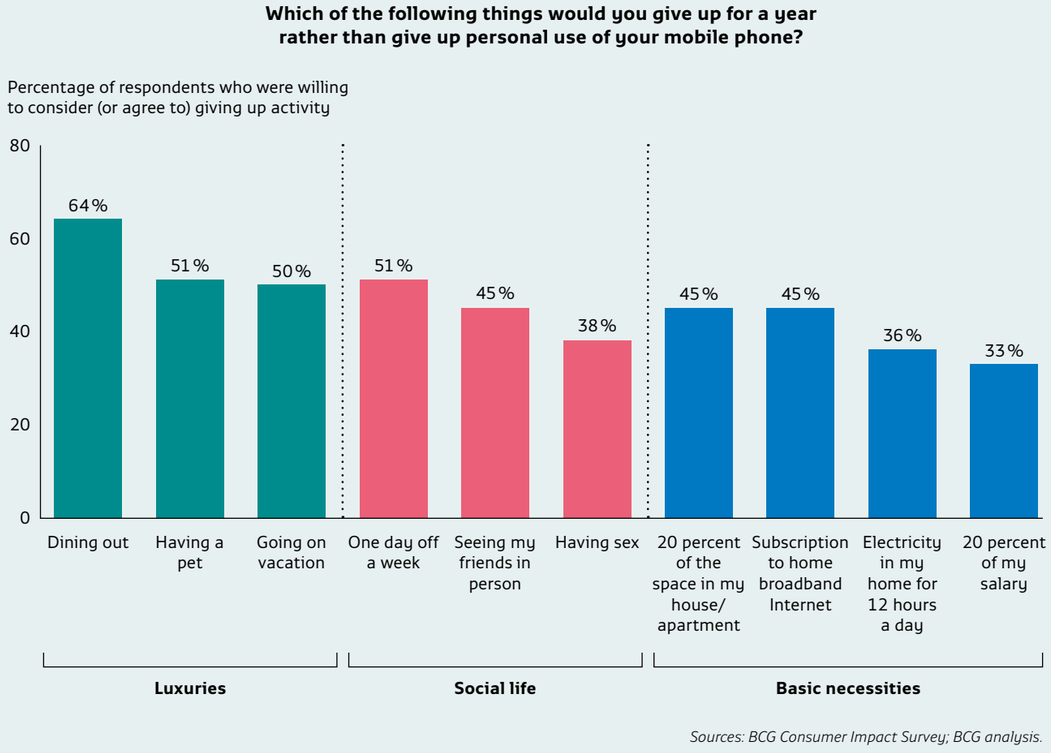
There was a survey done recently by the Boston Consulting Group for their Consumer Impact Survey (FIG 1) that asked the question, "What are people prepared to give up to keep their mobile device?" The answers were illuminating, ranging from dining out to having a pet to going on vacation — all the way to having sex and giving up 20 percent of their salary. In my mind, some of these things are crazy to give up, but at the same time, it is very indicative of the impact mobile technology is having on people's lives today.

In the U.S., users value their mobile phone so much that they are willing to spend 11 percent of their income to maintain their mobile status. In other parts of the world this percentage is even greater. For instance, in South Korea, mobile spend is 12 percent of income and in Germany, it is 13 percent of users' income. In emerging countries, it is even more jaw-dropping with Brazilians spending 20 percent of their income on mobile phones; in China, up to 43 percent; and in India, 45 percent. It's clear that this is indicative of a trend that is continuing to both move forward and increase in value for those who regularly use mobile technology. (FIG 2)

What does this mean for ID documents?

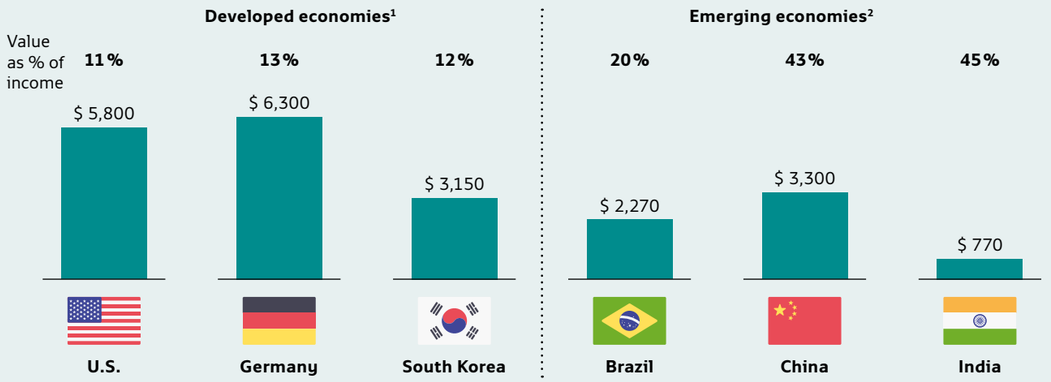
Consider the evolution of ID documents from paper to the secure printing of plastic documents and later including a chip, converting them to smart cards. Given this progression, it is hardly surprising that Governments are evaluating ways to migrate a citizen's identity onto a mobile phone in ways that are most convenient for citizens, yet cost-efficient for the agencies issuing the IDs. For example, Australia and New Zealand recently announced a bilateral agreement allowing citizens of either nation to use a mobile token to visit each other's countries. Estonia is exploring how to integrate mobile IDs into its existing eID infrastructure to expand its Government-to-citizen services within its borders. Finally, in the U.S., there is an active request for proposal (RFP) in process to enable the provision of mobile driver's licenses to citizens of a particular state, and 12 others are in the process of passing laws that would allow the use of mobile driver's licenses within their state.

FIG. 1: CONSUMERS PRIORITIZE SPENDING ON MOBILE OVER LUXURIES



Sources: BCG Consumer Impact Survey; BCG analysis.

FIG 2: CONSUMERS PLACE A HIGH VALUE ON MOBILE TECHNOLOGIES



Note: The analysis of value as a percentage of income is based on nominal GDP per capita in 2013.

[1] In developed countries, we show data for consumers of 4G technologies.
[2] In emerging markets, we show data for 3G consumers (as 4G has only very recently rolled out).

Sources: BCG Consumer Impact Survey; BCG analysis.

Whether we like it or not – this is a trend that is happening in some form in many countries today, as governments and relevant authorities look to move ID cards onto users' mobile phones.

HID Global is at the forefront of this trend, recently introducing its HID goID™ technology engine for mobile identity solutions. Our goID platform enables a government-issued credential to be authenticated, both online and offline on a smartphone, which is unique, enabling a user's smartphone to become a secure government-to-citizen ID.

It is important to note that HID believes that mobile IDs will be complimentary to physical ID documents for quite some time to come. While we see many elements moving quickly onto the mobile, we do not believe that ID will make a similar leap in such a short time period, due to the many standards (ICAO, for instance) that must be discussed, developed and then ratified.

Not only that, citizens are just more comfortable having something physical in their hand that represents their identity document. Therefore, HID Global expects that this transition from the physical world to the mobile world, when discussing identification, will take some time. However, this is not a bad thing. When looking at the technology involved in smart cards or other smart devices containing chips, it could be complimentary to the mobile solution and add value to a particular mobile application. As we have talked to customers in the market about our goID solution, we have learned that some users actually would like to have something that not only issues a mobile ID, but also issues a physical ID at the same time.

In Africa, for example, some citizens highly value the physical ID card as a token of their citizenship. So while it is convenient for them to have access to their ID on a smartphone, citizens also want a physical token or representation of their citizenship.

Physical and Mobile IDs Can Co-exist

The physical and mobile ID "worlds" are already co-existing. The Irish Passport Card is an example of an ICAO-compliant document that allows travel across borders in the European Union, that can be applied for using a mobile phone. Irish citizens can apply for their passport card by:

- Downloading the passport card app on their phone.
- Entering their personal information.
- Taking a selfie with their mobile phone.
- The applicant pays the passport card fee via mobile.
- After confirmation that the information submitted (including the selfie) matches the applicant's data on file, the passport card is sent to the citizen via post.

Global banks are also allowing customers to order credit cards and other products by simply submitting a selfie for verification purposes. We will continue to see new and different applications of physical IDs converging with mobile applications in the months ahead, including but not limited to mobile driver's licenses.

What can prevent an identity project from being successful is often not the documents themselves, but the infrastructure required to read them or the expense in distributing them. If this is the case, then how about using your smartphone as a single reader, that can read both physical and mobile IDs? In so doing, the citizen has a choice in what they want to use – a mobile or a physical ID or both – while the issuing authority can implement a cost-effective and widely available reader. From our perspective, there is no reason why both physical and mobile IDs can't co-exist.

Multi-factor Authentication

One of the elements that we built into our goID roadmap is the use of a second level of authentication, such as a physical card or a key fob in someone's pocket. Multi-factor authentication (MFA) is particularly important to protect and manage verification devices. If you were a verifier using a mobile phone to authenticate a mobile driver's license, there needs to be a way of managing who has access to that verification device. MFA ensures that if the device were to fall into the wrong hands, an unauthorized person would not have access to the central database.

Another use for secondary authentication could be for the visual identification of a mobile driver's license or other identity document. In today's technologically advanced world, there is no way to tell if a photo on a smartphone is authentic or if it's been retouched. This is a real issue in the case of verifying the holder of a driver's license or other credential. With a secondary authentication factor, you could potentially introduce a second security feature to the image that only appears in the presence of that second authentication factor, such as a graphic that appears in the photo image on the driver's license (similar to security printing holograms). This allows another level of verification, proving that what is being shown is the genuine credential. Multi-factor authentication works for all sorts of applications both online and offline, such as allowing access to an individual's health records or vehicle registration information.

The Secure Element

To be able to issue a virtual ID to a secure element on the citizen's device (either SIM or embedded Secure Element), the issuance agency must integrate either with a mobile network operator (MNO – issues the SIM) or the handset manufacturer (OEM – issues the handset and embedded Secure Element), as they are in control of the keys that allow the loading of the virtual ID applet onto the respective secure element. The keys then perform the subsequent personalization of the virtual ID (sending the citizen specific data elements, picture and authentication keys).

This means potentially integrating with most of the MNOs in a specific country. Alternatively, the issuing agency could integrate with what the industry calls a Trusted Service Manager (TSM) that would work directly with the MNO on their behalf.

Both options are heavy in integration and carry a considerable cost to the issuing agency. Additionally, this makes it very impractical for temporary virtual IDs for citizens that are in roaming mode or where it is almost impossible to quickly determine the MNO they are using.

Another consideration here is that the Secure Element is currently accessible via NFC, so an external virtual ID reader could easily interact with the virtual ID applet on the citizen's smartphone. This interface is not available on the Apple® iOS platform and their popular iPhone® devices. For the Apple ecosystem, it would be necessary to use Bluetooth® Low Energy (BLE) proximity technology, which unfortunately is currently not standardized.

There are efforts to close this standardization gap on-going in the GlobalPlatform organization.

Despite the above limitations, there are merits to having a Secure Element, and new technologies like goID are complementary to such hardware-based security.

Conclusion

Mobile IDs are coming – whether we like it or not. Consequently, as an industry, we have three possible strategies to manage this transition:

1. We can put our heads in the sand.
2. We can try to crush the oncoming technology.
3. We can "Keep Calm…and Embrace Mobile."

The first two options are unrealistic. Perhaps the sound strategy is the third option – and it's the only one that will really work in the long run. ☒

UTILIZING the *synergies between* PASSPORTS and eID CARDS

By Veronica Atkins, Silicon Trust

When Infineon's Detlef Houdeau delivered a speech in March 2017 in Baku, Aserbaidschan, he hit a nerve with the delegates of the High Security Printing conference. Representing Eurosmart's Cybersecurity and Digital Identities Committee, Dr. Houdeau made a strong case for recognizing and utilizing the existing synergies between ePassports and eID Cards.

Using the example of the Dutch ePassport datacard and ID card, one can recognise the similar optical design. Integrated within both documents are the same optical security elements (level 1, level 2 and level 3). Both documents carry the same electronic functionality (ICAO 9303 standard) and the same biometric data, stored in the chip (face, since 2006, plus 2 fingerprints since 2009)

☐ The fast digitization of society continuously brings new challenges to the public sector, its offerings and its service infrastructure. Electronic identification (eID) allows citizens to access online services, using, for example, a secure token in the form of an ID card. During the last two decades, governments all over the globe have defined, specified and started the roll out of eID card schemes, in order to enable their citizens secured access to online services, as well as highly secured documents for personal verification.

Implementing an eID card scheme is a massive investment for any government, especially if eID cards and electronic passports are implemented as separate projects. Thankfully, standardization as well as technology and processes across the value chain allow governments to consider implementing a family concept for both ID1 (card) and ID3 (passport booklet) formats.

ICAO Doc 9303 Machine Readable Travel Documents

ICAO's initiative to develop standard specifications for passports and other travel documents followed the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organisation. ICAO's mandate stems from the Convention on International Civil Aviation (the "Chicago Convention"), which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls.

ICAO Member States have recognized that standardization is a necessity and that the benefits of adopting the Doc 9303 standard formats for passports and other travel documents extend beyond the obvious advantages for states that have the machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer strong defense against alteration, forgery or counterfeit. The adoption of a standardized format for the visual zone of an MRTD (Machine Readable Travel Document) helps airline and government officials with the inspection process.

In terms of protection against tampering and fraud, the optional introduction of biometric data stored on a contactless security chip will provide greater protection and facilitate the use of automatic border control (ABC) systems.

The ICAO 9303 standard has been deployed for travel documents incorporating technology standards such as ISO/IEC 19794 for biometrics and ISO/IEC 14443 for the contactless interface, as well as application standards for travel documents, like passports (ID3 format), Residence Permit cards and Registered Traveller cards.

> *"Implementing an eID card scheme is a massive investment for any government, especially if eID cards and electronic passports are implemented as separate projects."*

Also, since 2006, the ICAO standard has also been applied increasingly for national eID cards (ID1 format). This has political and legislative implications, some application effects as well as an impact on production and of course, it affects the electronic, contactless interface of the card.

Overview on booklets with ID3 format PC holder page – status in 03/2017

Albania, Antilles, Armenia, Azerbaijan, Brunei, Hong Kong, China, Macau, SAR, Colombia, Croatia, Czech Republic, Denmark, Finland, Germany, Hungary, Ireland ,Latvia, Lithuania, Luxembourg, Macedonia, Malaysia, Montenegro, Netherlands, New Zealand, Norway, Panama, Poland, Portugal, Romania, Russia, Serbia, Singapore, Slovakia, Slovenia, Republic South Africa, Sudan, Sweden, Switzerland, Tajikistan, Thailand, Turkmenistan, Ukraine, Venezuela

The following countries start soon:

Brazil, Egypt, Island, Indonesia, Italy, Myanmar, Saudi Arabia, Spain, USA

References on ICAO-MRTD data set in ID1 documents.

The following states use ICAO data sets, biometric, security and interface in ID1 documents in the public domain (alphabetic order):

Albania, 2007	Monaco, 2008
Germany,* 2010	Netherlands, 2006
Hungary, 2016	Sweden, 2005
Italy (2nd Gen), 2017	Turkey, 2016
Lithuania, 2009	Ukraine, 2016

* Note: Germany needs another authentication protocol than ICAO (TA authentication first, followed by CA authentication).

Synergies in production, infrastructure and document security

Synergies between the 2 formats can be found in document production, in equipment procurement, as well as in the process workflow. Both ID1 and ID3 polycarbonate lamination use equipment for both multiple printed panels, the process for lamination applies to both formats with the stacked layers.

When it comes to PC foil printing and finishes, such as hologram and transparent foil, the same equipment and workflow is applicable.

"In terms of protection against tampering and fraud, the optional introduction of biometric data stored on a contactless security chip will provide greater protection and facilitate the use of automatic border control (ABC) systems."

In terms of the key management infrastructure with the purpose of creating and handling keys and certificates, a connected network is required for both formats. In the same way, equipment for capturing the biometric data, such as scanners or cameras, can be used by the registration office also for both document types. Equipment for optical and electronic personalization is available on the market, which can work with ID1 and ID3 documents in mixed mode.

A family concept for both ID cards and passports can be applied when it comes to the optical security concept for a country's documents. All security levels are applicable to both formats, such as rainbow pre-print, UV-mark and special holographic foils.

Synergy in teaching and training of authorized persons

The examples above give a good indication how a cross-format ID family concept can be utilized when it comes to document production and ID infrastructure. However, governments and institutions that opt for a family concept when implementing their national ID document strategy, can utilize synergies beyond the production process.

Take, for example, national ID registration and issuance centers: When rolling out an ePassport project, each center requires a complete solution set – hardware, software, maintenance – even though, on average, only about 30% of the population will ever apply for a passport. If a government decides to use the existing set up also for national ID cards, the efficiency and return on investment is much higher.

Once the documents are issued, also the training and teaching modules of the personnel in charge of border security and immigration, as well as for national eServices, could be offered for both formats: eID card in ID1 & passport holder page in ID3.

"The re-use of this standard into other documents beside ID3 booklets, such as ID1 card and Residence Permit card can reduce cost, effort and time for production, for infrastructure, for training and for the forensic lab."

Use cases for ICAO data set, biometrics, electronic security and interface

Five different document types use the ICAO 9303 Standard:

1. Passport, ID3, eMRP in more than 120 countries worldwide
2. ID-Card, ID1, National eID-Card in more than 9 countries worldwide
3. Residence Permit, ID1 in more than 50 countries worldwide
4. Frequent Traveller Card, ID1, China & Macao; China & Hong Kong
5. Seafarer Card, ID1, Myanmar Pilot, start in 2017; based on the ILO recommendation.

Conclusion and outlook

The ICAO 9303 standard has been well defined since 2004. To date, more than 100 Mio documents, based on this standard, are issued every year. This standard captures a comprehensive data set (LDS1.7), document reading security (e.g. BAC), stored biometric data & quality (ISO/ IEC 19794) and the used interface (ISO/IEC 14443); The re-use of this standard into other documents besides ID3- booklets, such as ID1 card and Residence Permit card can reduce cost, effort and time for production, for infrastructure, for training and for the forensic lab. For the end customer, the benefits are in the application. For example, when entering and leaving states where an additional visa or entry/ exit stamp is not required, the citizen has a choice. He or she can leave the passport behind and use the eID card with the ICAO-standard for travelling and for ABC systems at the border. This means less hassle and more convenience with a standard wallet-friendly ID1 card format. ☒

BLOCKCHAIN *Blues* - the *END* of eID cards?

By Markus Hoffmeister and Klaus Schmeh, cryptovision

By design, the blockchain is a decentralized technology. It creates a distributed database containing information that can be simultaneously used and shared within a large publicly accessible network. The blockchain network lives in a state of consensus and reconciles every transaction that happens in regular intervals. Each group of these transactions is referred to as a “block”, hence the technology’s name. By allowing digital information to be distributed but not modified, blockchain technology creates a digital ledger of economic transactions that can be programmed to record not just financial transactions, but virtually everything of value.

> *A blockchain solution can link a public key with an identity in a similar manner to a public key infrastructure (PKI) – although without needing a central entity, through the avoidance of a central entity, you naturally have fewer possibilities for influence – with all the pros and cons associated with this.*
>
> *-Benjamin Drisch, cryptovision*

☐ What are the security implications?

With blockchain databases not being stored in any single location, the information is much harder for a hacker to manipulate. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet. In other words, the blockchain's aim is to take trust away from human intermediaries and put it into mathematics and computing, which are a lot less susceptible to errors. It is a mechanism to bring everyone to the highest degree of accountability.

Yet the same thing that makes blockchain attractive - its distributed nature - also makes it a potential security threat. Vulnerabilities occur when the blockchain interfaces with humans or, in the case of IoT, with devices. When using blockchain, the user's private key is the identity and the security credential, which is generated and maintained by the user instead of third-party agencies. For example, when creating a storage wallet, the user must import his/her private key. An attacker could steal the user's private key using various attacks. Since the blockchain is not dependent on any centralized third-party trusted institutions, it is difficult to track the attacker's behaviour and recover the modified blockchain information.

This situation poses an important question for the smart card industry: what role will smart cards or other secure elements play in blockchains? Currently, all a user can do is use a self-issued smart card or other hardware device to store his private key, as a sort of cold crypto-wallet. This results in better protection than software wallets or hosted cryptocurrency exchanges, but is still far from perfect. It is therefore an interesting option to use a private key stored on a trusted identity card (i.e. a national eID card) for participating in a blockchain.

Blockchain for Identity and Data Management

The global blockchain identity management market is expected to reach USD 7308.4 million by 2025, from USD 57.6 million in 2017, growing at a CAGR of 83.2% during the forecast period of 2018 to 2025.

Data Bridge Market Research 2018

What are the implications of this development for the conventional digital identity markets and its stakeholders? Blockchain technology is currently promoted as the silver bullet for distributed applications of all kinds. Beyond the most cited application of BitCoin in the fintech sector, identity management is a growing segment. Here, the blockchain can be used to build the groundwork of an authentication system or of a smart contract solution. Having a secure identity to authenticate oneself is crucial for all online interactions. Absolutely no one would argue while the use of username / password is prevalent that there is a need for innovation to enable secure, convenient online identity management. Distributed ledgers could fill this need by offering enhanced methods for proving who you are, along with the possibility to digitize identity documents.

However, conventional identity systems are not being replaced just yet: Developing digital identity standards on the blockchain is proving to be a highly complex process. Besides technical challenges, a universal online identity solution requires cooperation between private entities and government agencies. Add to that the need to navigate legal systems in different countries and the problem becomes exponentially difficult.

Is blockchain replacing conventional PKI and eID systems?

"A blockchain solution can link a public key with an identity in a similar manner to a public key infrastructure (PKI) – although without needing a central entity, through the avoidance of a central entity, you naturally have fewer possibilities for influence – with all the pros and cons associated with this."

Benjamin Drisch, cryptovision

The implementation of a public key infrastructure (PKI) and a blockchain is an interesting debate within the industry. While the outcome is yet to be determined, it is apparent that blockchain technology can benefit from PKI and other identity technologies, rather than replacing them. Blockchain leverages digital signatures and hash functions, as the main cryptography for all transactions. This is exactly what a PKI provides. If the PKI is a part of an eID system, the private key is even protected to the highest level. It goes without saying that a digital currency, like BitCoin, profits from this.

The benefit of a key being stored on an eID card is less clear when it comes to blockchain-based authentication. As an eID card is an authentication solution in itself, it can be questioned whether a blockchain-based authentication system is even necessary when such a card is available. In addition, the involvement of a card issuing authority contradicts the main benefit of a blockchain: to establish a trusted infrastructure without involving a trusted third party. At this point it is important to note that not requiring a trusted third party is not the only advantage of a blockchain. Other purported benefits include fault tolerance, high availability and lower operation costs.

Conclusion

It will certainly be a major research goal for years to come to evaluate whether the benefits of an eID in a blockchain environment are real and if they outweigh the natural drawbacks of a blockchain. If these questions will be answered in a positive way, an eID card appears to be the perfect means for storing a private key used in a blockchain – as long as the existence of a trusted third party is accepted. Not only keys, but also identities can be shared between a blockchain and an eID infrastructure. All this means that eID cards might become important building blocks of blockchain systems and that a convergence of the two technologies can be expected. In the end, the major question is whether the blockchain will ever become as important as the current hype suggests. This remains to be seen. ☒

cryptoVision

cryptovision's signature solutions work well for signing transactions within the blockchain. cryptovision has implemented a smart card solution that allows the user to conveniently sign payment instructions within the blockchain currency Ether. Since a smart card is used as a key store, the key is much better protected than in a conventional blockchain wallet. The cryptovision solution makes it possible to store the signature key outside the card for backup purposes.

cryptovision's Certificate Lifecycle Management solutions work well with various blockchain-based PKI components. For example, cryptovision's CA software CAmelot supports blockchain-based directory services, CRL distribution points, OCSP responders, CA certificate distribution points, and identity management systems, as long as they can be addressed through standard PKI interfaces.

WHY do we NEED *biometric* contactless *PAYMENT* cards NOW?

By Ursula Schilling, Infineon Technologies

Biometric payment cards offer stronger, more convenient customer authentication capabilities, while ensuring strict compliance with PSD2 regulations. Regulatory requirements for secure customer authentication are becoming more stringent for specific applications and in specific regions around the world. The introduction of regulations such as PSD2 (Payment Services Directive 2) and GDPR (General Data Protection Regulation) in Europe clearly illustrate this growing trend.

In a study published in February 2020, ABI Research predicted that nearly 1 million biometric payment cards will be shipped to the market by the end of 2020. This figure will rise to 65 million by 2024, with key markets developing in Europe and China.[1]

Multi-factor authentication

On-card biometrics enable highly convenient, innovative multi-factor authentication for point of sale (POS) purchases. The card holder ("what you have") can easily validate their identity ("who you are") at the POS by presenting a fingerprint that matches the biometric print on the card. As such, payment cards with integrated biometric sensors are an extremely convenient, innovative means of complying with strong customer authentication (SCA) requirements. In markets that rely on offline PIN mechanisms or chip-and-signature infrastructures, biometric payment cards are a great way to harmonize authentication processes and comply with SCA regulations without costly and complex changes to the POS infrastructure.

Greater choice

In addition to this, some market players want a broader choice of authentication methods tailored to different user groups, such as disabled or older people, early adopters and forward-looking millennials interested in innovative solutions. Some of these user groups still have reservations about card and contactless payments. Biometric payment cards simply offer greater privacy, as the card always stays in the user's hand. The buyer does not have to hand it over to a cashier or push any buttons on a pin pad. As such, this technology fosters consumer trust by reassuring users that their personal data will remain private.

Better, more hygienic user experience

Biometric contactless technology also improves the overall customer experience by making transactions quick and easy to complete, as there is no need for users to touch a pin pad or interact with a cashier. This "no-touch" approach also has a vital role to play in today's global pandemic: it protects users' health and well-being by allowing them to make hygienic, contactless payment transactions without touching potentially contaminated pin pads. This also applies for high-value payments above a certain limit for a cardholder verification method (CVM) stipulated by networks and issuers. Thus, for both low and high value payments, no PIN entry will be required anymore when using a biometric sensor-enabled payment card. Biometric authentication, when implemented in a security controller (SC) on card, fulfills the highest certification standards.

Put simply, biometric payment cards strike the right balance between security, convenience and speed, while increasing efficiency at the POS. At the same time, however, biometric cards are a new concept for many consumers and so card issuers will have to educate their customers on this new payment technology and its usage. Enabling users to easily sign up from home without having to visit a bank branch is one approach that could support the rapid adoption of biometric payment cards.

Advantages of biometric contactless payment cards for different market players in the payment ecosystem

Overall, biometric contactless cards will bring huge benefits to all players in the payment ecosystem. These far outweigh the hurdles and drawbacks connected with this new technology.

a. For network and infrastructure providers

Looking at the existing POS infrastructure, the cost and effort involved in rolling out biometric payment cards will be minor, since infrastructure updates will not typically be required on the POS side. Over 90 percent of POS terminals have already received the requisite firmware updates and so only a small number of POS terminals will still have to download these. Transactions will be based on well-known ISO 14443 standards. The only investments required will be on the part of card manufacturers, who will have to embed biometric sensors and inlays into cards to ensure they can source sufficient power from contactless fields.

"Put simply, biometric payment cards strike the right balance between security, convenience and speed, while increasing efficiency at the POS

The cost of the new cards will be slightly higher. However, upcoming security controller (SC) innovations from companies such as Infineon Technologies – the market leader in payment ICs – will bring the cost of card production down, as SC external silicon components become obsolete and the card production process, as a whole, becomes less complex.

New state-of-the-art security controller platforms delivered by chip vendors such as Infineon Technologies meet all requirements regarding contactless performance, power efficiency and security.

The majority of contactless security controller (SC) can be implemented into any kind of form factor. Similar SC implementations can be built into contactless cards (a yearly market shipment of >2 bn pieces), contactless tokens for secure second-factor authentication for remote payment (yearly market shipment of 40 m) and smart payment wearables (approximately 80 m pieces per year).

b. For banks and issuers

Card payments based on biometric authentication are expected to increase, while costly cash handling processes are expected to decrease. The current level of Card Present (CP) fraud at POS will drop, as biometric authentication is known to be more secure, making it more difficult for criminals to skim personal information stored on cards.

This technology will boost consumer trust and increase the number of contactless transactions.

Incorporating these technology innovations into cards will act as a draw for consumers and make it more likely that these cards become "top of wallet" for users.

Biometric cards will also reduce costly chargebacks, as users will no longer have to enter a PIN and so the likelihood of making a mistake or fraud, together with skimmed card details will be minimal.

1 *ABI Research, Payment and Banking Card Technologies Report, Feb. 2020, updated May 2020*

c. For retailers

Higher customer throughput is to be expected as biometric authentication is quicker than entering a PIN for high-value transactions. At the same time, this increased customer throughput may translate into higher revenue for retailers.

Generally, it is perceived that payments at points of sale in shops will become easier and less confusing as there is no CVM (cardholder verification method) limit for biometric card payments. This would mean that consumers will no longer need to enter a PIN, thereby making payment transactions more efficient and streamlined.

Ultimately, retailers can expect to see more customers, more revenue and fewer costly cash handling processes.

Payment networks and issuers can expect an overall reduction in fraud rates for lost and stolen cards as the only person who can make a transaction with a biometric payment card is the individual who matches the biometric data.

d. For consumers

When a consumer pays in person for a high-value transaction, they do not have to insert their card into the payment terminal. All they have to do is hold a card over the terminal. A second factor such as a PIN, signature or biometric authentication is required for payments above any nationally defined spending limits to prevent fraud through the skimming of card details or to ensure the user is not paying with a lost or stolen card. This makes contactless payments more secure for consumers.

Networks and issuers have all recently increased spending limits for low-value payments to increase the number of contactless transactions without CVM. In Germany for example, customers can make contactless payments up to a limit of EUR 50. In the UK, the limit is GBP 45. Similar measures have been taken in a further 27 countries. Already for a high number of contactless transactions a 2nd factor authentication has been waived. This situation is unlikely to change until biometric cards have been rolled out on a wider scale with secure cardholder authentication for all payment transactions.

This new biometric technology can also make remote payment transactions more secure. If a user has to confirm their identity for a remote payment using a second authentication step, all they will need is their card and an NFC-enabled mobile phone – they will not have to use another potentially less secure device for two-factor authentication.

It is expected that consumers will appreciate the convenience of making payment transactions without having to remember a PIN. This should be particularly welcome among the elderly. Overall, it is expected that biometric card payments will become the secure method of choice.

Finally, the high speed of transactions (less than one second for low and high-value payments), together with a seamless user experience and the hygiene factor outlined in the next chapter, are all expected to make biometric contactless cards the number one choice among customers.

More security for consumers and retailers during the COVID-19 pandemic

Faced with continued uncertainty surrounding the COVID-19 pandemic, customers and retailers across the globe are switching to contactless payments over concerns about contact-based transmission of the coronavirus. Standards of security and convenience are rising and biometric contactless cards are expected to increase hygienic security standards even further.

The contactless biometric card system is the only card-based payment method that allows users to make touch-free and virus-free high-value payment transactions at the POS, without having to come into contact with surfaces potentially contaminated with the COVID-19 virus. Presently, for all high-value transactions, users must enter a PIN, which comes with the risk of contracting the potentially deadly COVID-19 virus that may found in germs on the POS touchpad.

Even in cash-driven Germany, more than half of everyday payments are currently being made with contactless cards

“Faced with continued uncertainty surrounding the COVID-19 pandemic, customers and retailers across the globe are switching to contactless payments over concerns about contact-based transmission of the coronavirus.

today, compared with only 35 percent of payments being made with contactless cards before the coronavirus crisis began (Deutsche Kreditwirtschaft). The situation has changed even more dramatically in the US. According to Visa, the volume of contactless transactions has increased by >2000 percent since the start of the pandemic.

While contactless technology makes payment transactions faster, more hygienic and more convenient, only a combination of contactless payment and biometric solutions is considered robust enough to provide all-round protection against viruses and diseases. The way we pay has already changed radically and will continue do so, even more with biometric contactless cards around the corner.

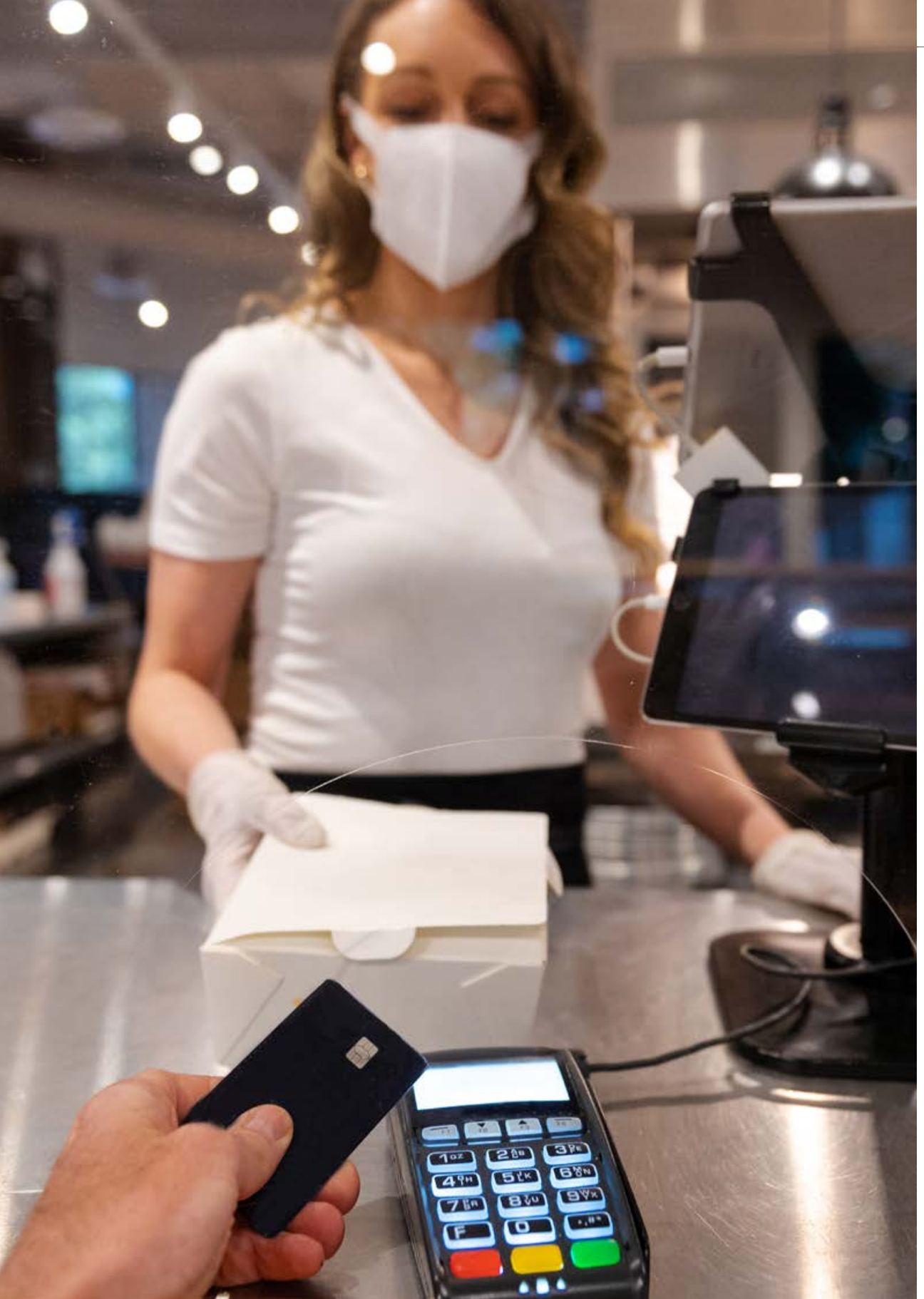
What can Security Controller providers contribute to the payment and biometric card market?

Infineon is the global market leader in the area of payment security chips. Worldwide, every second chip in a payment card is an Infineon chip inside. The company is also playing a key role in the development of biometric payment cards and has supplied chip solutions for all major pilot schemes and biometric card projects in the first half of 2020.

Infineon’s sophisticated security controller (SC) for contactless payment cards offer a range of benefits, including extremely low power consumption and a unique feature set that enables manufacturers to easily and flexibly integrate elements into card bodies with minimum effort.

Leveraging its experience in security and contactless design, Infineon is committed to supporting the widespread adoption of biometric payment cards by integrating additional functions into security controller that enable manufacturers to efficiently produce scalable biometric systems for cards.

Infineon’s contactless payment chips have an optimized power profile for non-battery-supported contactless systems and deliver outstanding contactless transaction performance, enabling contactless payment transaction times of below 200 milliseconds, even in scenarios with low reader field strengths and when used in combination with small antenna designs. These factors are a decisive benefit for biometric card solutions with seamless card implementation further enhanced by various industry partnerships



Partnering for biometrics

In order to seamlessly manage the different cards components, Infineon cooperates with various partners in the field of biometrics:

Infineon partners with biometric company Zwipe to deploy Infineon's chip solutions in pilot projects featuring Zwipe's biometric payment platform. In other words, Infineon is supporting multiple leading payment networks run by twelve major banks in various countries across Europe and the Middle East.

Infineon has teamed up with Fingerprints Card (FPC) and IDEX Biometrics to provide secure, cost-efficient platform solutions that will enable the mass deployment of biometric cards from 2022 onwards.

This is how Bjoern Scharfen (Head of the product line Payment & Ticketing Solutions at Infineon) perceives Infineon's engagement into contactless biometric cards, "Infineon is committed to enabling a secure, convenient payment experience enhanced by fingerprint authentication. Our turnkey solutions will drive biometric innovations in the smart card industry and help make digital transactions easier and safer. Biometrics are the next innovation step for contactless payment cards, providing additional security and convenience to banks and consumers, while protecting customers and merchants from infectious viruses."

Market data and pilot projects

Currently more than 20 world-wide pilots and biometric card volume projects have already been launched by different issuers supported by different networks and key players backed by interesting market information issued by various channels:

- Mastercard is working with Crédit Agricole Payment Services on a biometric card pilot for 200 customers in Touraine and Poitou. The pilot will trial payment cards with integrated fingerprint sensors.
- Mastercard has certified its first contactless biometric payment card from Thales based on the SLE78 family, enabling the company to move from the pilot phase to commercial deployment.
- Biometric technology company Zwipe has entered into a partnership with global smart card manufacturer XH Smart. The partners are focusing on commercializing end-to-end biometric payment offerings for XH Smart customers in China and beyond.
- Biometric technology company Zwipe has entered a milestone partnership with China's largest secure payment solution provider Goldpac to launch biometric payment cards. The two partners are working together to launch biometric payment cards, enrolment offerings and related services to Goldpac's extensive customer network, which includes some of the largest financial organizations in the world.
- IDEX Biometrics has been granted a patent by the UK Intellectual Property Office for unconnected on-card enrollment on biometric smart cards. IDEX biometrics has extended its on-card enrollment patent to the United States and Germany and is looking to extend its influence and reach across further key regions.
- Swiss Corner Bank has launched Switzerland's first commercial biometric credit card through a partnership between Fingerprint Cards (FPC), Thales and Visa. According to an announcement from FPC, this is the first limited commercial launch of its kind.
- Fingerprint Cards (FPC) has announced that its sensor module has passed accuracy and security testing with BCTC and is targeted at the Chinese market. https://www.fingerprints.com/2020/04/15/contactless-comes-of-age-how-biometrics-is-taking-cards-to-the-next-level ☒

A *New* ERA in Customer *Communication* – Brands, FASHION and *Art* NOW talk NFT.

By Kay Plaumann, AdvanIDe

You've likely heard recently how the metaverse will usher in a new era of digital connectivity, virtual reality (VR) experiences and e-commerce. Tech companies, Brands and Banks are betting big on it: Microsoft's massive US$68.7 billion acquisition of game developing giant Activision Blizzard reflected the company's desire to bolster its position in the interactive entertainment space. Prior to this, Facebook's parent company rebranded itself as Meta — a key pillar of founder Mark Zuckerberg's grand ambitions to reimagine the social media platform as "a metaverse company, building the future of social connection." In fact, the global "metaverse" first appeared in 1982, before everyone was as comfortable, or even aware of, the Internet (Web 1.0). Today, however, big money, backed by even bigger companies are intent on making the metaverse (Web 3.0) as acceptable and utilized as the internet we know today. In this emerging Web 3.0 iteration, users consume, create, and own content; the networks (and the money exchanged) are decentralized, with blockchain technology replacing centralized intermediaries and providing the trust that enables both consumption and exchange. In fact,

The global metaverse market size is projected to grow from USD 61.8 billion in 2022 to USD 426.9 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 47.2% during the forecast period.

To see the metaverse in action, we can look at popular massively multiplayer virtual reality games such as Rec Room or Horizon Worlds, where participants use avatars to interact with each other and manipulate their environment. But the wider applications beyond gaming are staggering. Musicians and entertainment labels are experimenting with hosting concerts in the metaverse. Fashion brands are releasing on-line collections for virtual reality avatars. The sports industry is following suit, with franchises like Manchester City building virtual stadiums so fans can watch games and, presumably, purchase virtual merchandise. Artists are developing online art collections and of course, allowing for the purchase and trading of Non-Fungible Tokens (NFTs) connected to such projects and art items.

But before we talk about the metaverse and the role that NFTs play there, it is vital that we briefly touch upon where the metaverse lies within the web iterations of 1, 2 and 3 and what we mean when we talk about Web 1.0, 2.0 and 3.0.

Basically, this first version of the Web consisted of a few people creating web pages and content and web pages for a large group of readers, allowing them to access facts, information, and content from the sources. It was designed to help people better find information. This web version was dedicated to users searching for data. This web version is sometimes called "the read-only Web" because it lacks the necessary forms, visuals, controls, and interactivity we enjoy on today's Internet. People use the term "Web 1.0" to describe the earliest form of the Internet.

If Web 1.0 was made up of a small number of people generating content for a larger audience, then Web 2.0 is many people creating even more content for a growing audience. Web 1.0 focused on reading; Web 2.0 focused on participating and contributing. This Internet form emphasizes User-Generated Content (UGC), ease of use, interactivity, and improved compatibility with other systems and devices. Web 2.0 is all about the end user's experience. Consequently, this Web form was responsible for creating communities, collaborations, dialogue, and social media. As a result, Web 2.0 is considered the primary form of web interaction for most of today's users. If Web 1.0 was called "the read-only Web," Web 2.0 is known as "the participative social Web."

And finally, we come to the latest Web iteration. Although there are elements of Web 3.0 currently available today, it still has a way to go before it reaches full realization. Web 3.0, which is also referred to as Web3, is built on a foundation consisting of the core ideas of decentralization, openness, and more excellent user utility. Web 1.0 is the "read-only Web," Web 2.0 is the "participative social Web," and Web 3.0 is the "read, write, execute Web."

> *Web 3.0 ultimately lets users interact, exchange information, and securely conduct financial transactions without a centralized authority or coordinator. As a result, each user becomes a content owner instead of just a content user.*

This web interaction and utilization stage moves users away from centralized platforms like Meta, Google, or Twitter and towards decentralized, nearly anonymous platforms. Web 3.0 ultimately lets users interact, exchange information, and securely conduct financial transactions without a centralized authority or coordinator. As a result, each user becomes a content owner instead of just a content user. Web 3.0 isn't entirely in place yet, however, we are already seeing elements of Web 3.0 moving into our Internet experiences, such as NFTs, blockchain, distributed ledgers, and the metaverse as a concept.

Blockchains are a vital part of Web 3.0 – some would also call them the 'backbone and foundation of Web 3.0'. A blockchain is, in the simplest of terms, a time-stamped series of chained records of data that is managed by a cluster of computers not owned by a single entity. Each of these blocks of data (i.e., blocks) is secured and bound to each other using cryptographic principles (i.e., chain). The blockchain network has no central authority – it is the very definition of a democratized system. Since it is a shared ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.

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

Most of us have heard of blockchain when talking about crypto-currencies, such as Bitcoin. However, if we look beyond fintech services, it can also be used in many other applications such, as logistics, energy supplies, social networks, messaging, gaming, online market-places, storage platforms, voting systems, predictive markets, online shops and brand protection. There is one very important area that blockchain is vital for though – the development, collection and trading interactions concerning Non-Fungible Tokens (NFTs). These items are what everyone is considering the 'hot ticket' today, and are playing a major role in the growth of Web 3.0's metaverse.

The term "Non-Fungible" means that it is completely unique. "Token" means that it can be transferred on a blockchain. Essentially, NFTs are assets that carry a unique digital identity and can be traded between users on a public blockchain like Ethereum. Common examples of NFTs include artwork, trading cards, comic books, sports collectibles, games and more. Although NFTs tend to be associated with artwork, they actually represent much more. NFTs can actually unlock a lot of things including digital and in-person experiences, etc. It works like this - because NFT ownership can be instantly and easily verified on the blockchain, NFTs can act as proof of ownership. This is helpful in categories like art, where provenance is such an important part of the collectability of a piece. But this provenance, or proof of ownership is even more useful when applying NFTs to things like experiences; for example, you might in the future use an NFT to unlock access to a digital or in-person gallery or event for a specific artist, with the NFT acting as a ticket or pass to grant you access. The possibilities are really endless.

Regardless of whether you are a brand, an institution, an artist or collector, NFTs work in the same way. NFTs empower creators to connect directly with fans and enable new types of exclusive experiences that can be virtual, in-person, or both. NFTs offer further utility over traditional art pieces. NFTs can be traded on online marketplaces or exchanged directly between individuals. NFTs also provide a variety of specific benefits for artists, such as royalties. NFTs can be programmed with royalty features that reward artists for every sale in specific marketplaces, allowing artists to sometimes even be able to get royalties for secondary marketplace sales if their work is resold–this is one of the biggest attractions of NFTs for artists. Additional information related to each NFT can be stored within the NFT's metadata, giving each asset a unique history.

> *The issuance of NFTs can blur the lines between the physical and digital worlds and enables individuals and companies from various industries to cater to specific audiences and deliver personalized consumer interactions.*

We are currently seeing many big-name brands moving into the metaverse and offering a digital version of their 'real-world' products. Be they sneakers, clothes or even real-estate. The luxury fashion house, Balenciaga, entered the metaverse in late 2021 through a partnership with the video game makers Epic Games. The Fortnite x Balenciaga collab contained in-game limited-edition skins and outfits for avatars in the Fortnite game, which boasts a staggering 350 million users worldwide. The collab also featured an accompanying real-world Fornite x Balenciaga clothing line.

Nike acquired the non-fungible token studio RTFKT in December 2021 as a tool to access the metaverse. RTFKT produces NFT collectibles and memes, most notably digital sneakers, and aims to merge culture and gaming. Their most famous collab was with teenage artist FEWOCiOUS, to sell physical sneakers paired with their digital counterparts. RTFKT managed to sell 600 pairs/NFTs in seven minutes as part of the venture and netted more than $3.1 million.

Other interesting NFT project co-operations include Coca-Cola and Tafi, Gucci (and Hyundai) and Roblox. Other brands also making entry into the metaverse include Nike, Louis Vuitton, Adidas, Wendy's, Samsung, Burberry, Dolce & Gabbana, Ferrari, Tommy Hilfiger, Vas and Ralph Lauren to name but a few.

The metaverse is ripe with marketing and advertising possibilities. While it is still in its early stages, the community is now more open to experimenting on various projects, which brands, artists, musicians and sports teams can leverage for a successful breakthrough in the digital space – even through the issuing of a digital product that is NFT based. The issuance of NFTs can blur the lines between the physical and digital worlds and enables individuals and companies from various industries to cater to specific audiences and deliver personalized consumer interactions.

The metaverse may be young and volatile, but this is a chance to pioneer a new era of marketing. The future appears bright for a marketing model based in the digital world. The technology shift into the metaverse has started, and brands continue to find new ways to reach and communicate with Generation Z and beyond. ☒

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.

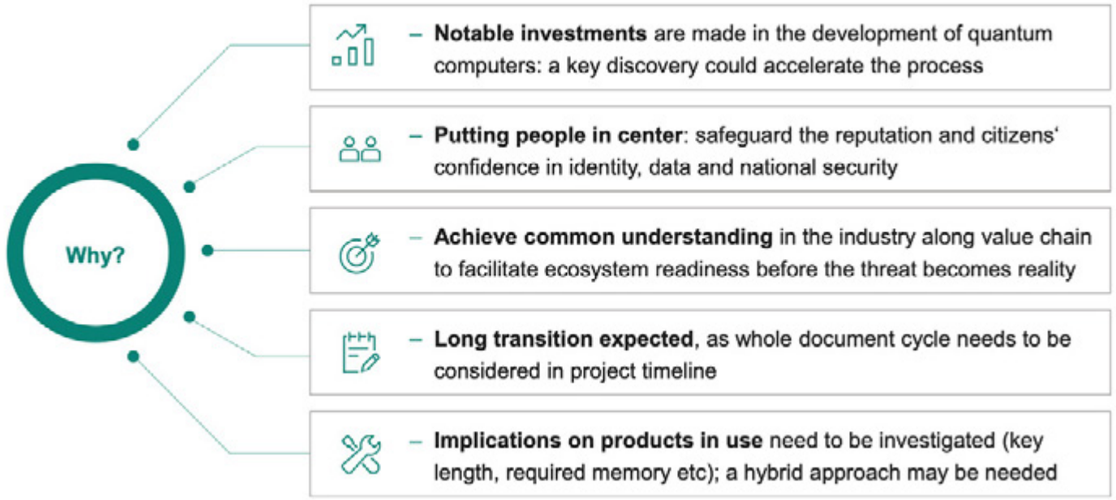


Figure 1:

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)

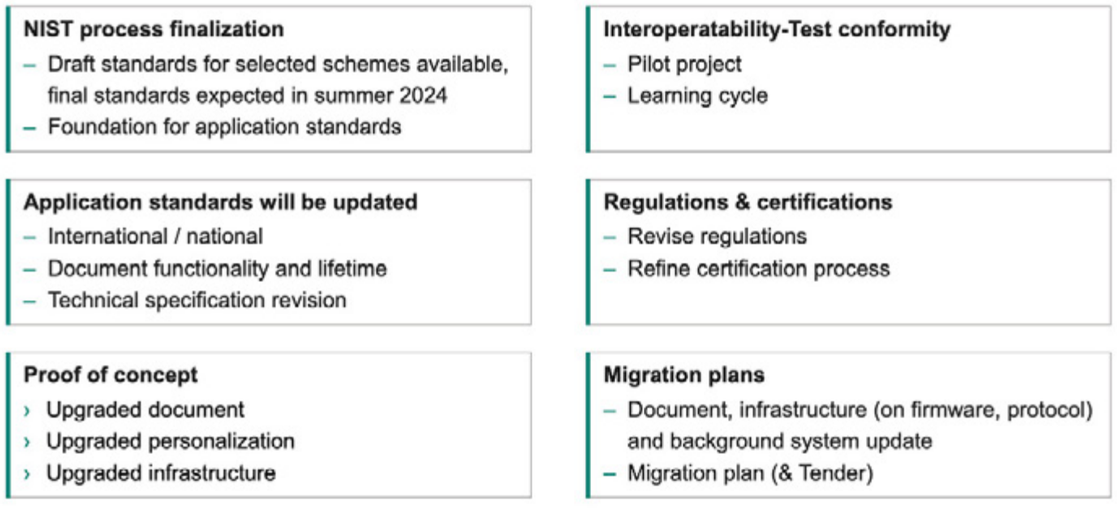


Figure 2:

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.*

SECURITY TAKES TO THE SKIES

By Wendy Atkins for Infineon Technologies AG

It's 6am. You have an important business meeting at noon in Frankfurt. Before the end of the day you will have travelled over 1,000km, sat through five hours of meetings, flown on an airplane for three hours, spent at least an hour and a half in airports, bought some duty free, made several telephone calls, drunk copious amounts of coffee, and had your fair share of chips. Sound familiar? It's certainly the experience shared by the millions of us who pass through any airport on our way to a business meeting every day. Without realising it, chip technology seems to have entered every part of our life – and we're now using a range of chip-enabled cards and gadgets to conduct our everyday life safely, conveniently and with a high level of security. What used to be considered science fiction is now very definitely science fact.

The airport environment is an interesting microcosm of society: you've got a broad cross-section of people ranging from airport cleaners to security guards, government officials to passengers and airline personnel. Added to this, the sheer range of shopping experiences in some major airports could rival many European High Streets. Each group of people passing through an airport has different requirements – and those involved in providing airport services must somehow meet these varied needs.

MANY PEOPLE, MANY NEEDS

First, let's take a look at the people passing through the airport. Many will be travelers. But how often do they travel? Are they frequent, very well known registered travelers? Are they occasional travelers? Or are they government officials – such as ambassadors – who are traveling? Whichever category they fall into, there is a good chance that they will have used secure measures, such as chip or biometric-based authentication technologies, to authenticate themselves or to speed conveniently through the security process.

Others may be airport or airline employees. They have perhaps worked for their organization for 30 years, but they will still go through some form of authentication process at least twice a day. They may clock on to a biometric-based time and attendance system.

Whatever the system, they will certainly be issued with a pass giving them access to secure areas of the airport. There's a good chance that the pass could be a chip card containing information on both the physical and the logical areas of an airport that the employee is permitted to visit. The card could even include company e-purse functionality for making purchases from vending machines and the staff canteen.

Other employees, such as sub-contractors, who perhaps only work in the airport occasionally, also need to go through some form of security process that adequately checks their credentials without impinging on their work.

Meanwhile, police and immigration officers also have to be authenticated whenever they enter a secure area. And, of course, their involvement in authentication doesn't stop there. Many will be charged with identifying passengers, which could involve checking passports and boarding passes, and will also involve comparing data on the passport with a 'watch list' of potential problem passengers.

With such a broad range of groups and subgroups operating in the airport environment at any one time, the technology used needs to be pretty dynamic to address the challenges and needs that each subgroup brings, especially considering that airports operate under increasingly difficult – and often contradictory – constraints. For example, many airports – such as Frankfurt – are not physically able to grow any more. Yet passenger numbers are continuing to increase, thanks to the introduction of larger planes such as the recently launched A380, capable of carrying more than 800 people, as well as the growth of numerous low-cost carriers.

In fact, the International Air Travel Association (IATA) estimates the Average Annual Growth Rate (AAGR) for international and domestic passenger travel will be 5% for the period 2004-2008.

These challenges come at a time when security requirements are increasing, but passenger throughput times must be reduced.

SECURE TECHNOLOGY

Airlines are interested in secure technology, both airside and groundside. Chip technology may be required when

selling tickets or when collecting data related to passengers' traveling habits, to provide convenience and security. Meanwhile, the highly competitive nature of the passenger travel business will dictate that the airline enhances loyalty and customer retention. While the speed and convenience offered by the use of automated authentication processes may help keep customers satisfied, there is a good chance that the airline will offer some type of frequent flyer promotion, which may involve some form of chip card.

The airline could be using SITA's (provider of global Information Technology and Telecommunications solutions to the air transport and related industries) protocols for its devices. Whether the devices are being used for printing, or for sending messages, airlines are confident of the level of their IT security.

Added to this, security measures in the form of no flight lists for the US and person profiling for flights to the US will have been adopted. Steps will have also been taken by the airline to ensure that no baggage is allowed onto a plane unless it is linked to a passenger.

INTEROPERABILITY

In the average working day at an airport, the requirement for security, convenience and safety as well as the possibility of making money and retaining customers, requires some form of secure technology. But how can these demands be met and how can the user experience be improved when for some people the requirement for secure technology is primarily for convenience, whereas for others it is much more about implementing the highest level of security possible? Added to this, implementations have to take into account the many different systems, networks and media that have to be linked both in one airport and between other airports – an interoperability nightmare!

The solution for those involved in offering airport services is being driven by secure and linked systems using chip-based tools. Such tools pervade every area of life and could be seen in employee cards providing logical and physical access to parts of an airport, frequent flyer membership cards, e-boarding passes and e-baggage tags as well as e-passports with e-visa and e-ID cards. It's a massive headache for interoperability, but organizations are working together to achieve results. In the payments world, interoperability of chip-based cards has been taken care of via the Europay-MasterCard-Visa (EMV) specification – and many retail outlets at Western European airports should have now upgraded their payment infrastructure to EMV. However, this migration has not been without its own issues, and is a process that many retailers and banks are still going through.

In the airport environment, a raft of standards initiatives is now being worked on. For example, the International Civil Aviation Organization's (ICAO) passport standards specify the mandatory use of facial recognition as well as the optional use of iris and fingerprint recognition. Meanwhile, both the ICAO and IATA are working towards a paperless boarding pass, with IATA saying it has a vision that e-ticketing implementation will have reached 100% by 2007.

IATA also aims to achieve an industry standard to replace bar coded baggage tags with auto-identifying RFID for baggage handling by 2006.

MORE RFID PLEASE

Airlines have been looking at RFID for baggage handling for some time. With costs of the technology continuing to fall, airlines are increasingly interested in adopting it to cut costs and improve customer perceptions of their service.

For example, in 2004, it was announced that Delta Airlines plans to spend up to US$25 million over a two-year period to roll out an RFID system to track the entire luggage it handles through US airports. According to industry reports, only 0.7% of the baggage Delta handles every year gets lost. Even so, finding what amounts to approximately 800,000 bags and returning them to their owners is estimated to cost the company around US$100 million each year. Delta's latest plans are for disposable RFID tags that can be attached to passenger luggage at check-in at every US airport it serves.

These labels will enable Delta to track each item through the carrier's baggage sorting operation and onto the plane, then through any transfer airports for connecting flights and finally onto the baggage carousel at the passenger's destination. The plans are intended to build on two RFID pilots that were held at Jacksonville Airport, Florida, in October 2003 and May 2004. During these trials, Ultra High Frequency (UHF) RFID inlays, which are capable of reading at up to 4-5 meters and can transfer data faster than low frequency solutions, were embedded in standard bar code tags and were fixed to checked-in luggage on the airline's Jacksonville to Atlanta route. These trials provided accuracy levels of 96.7% to 99.9%, compared with an estimated 80% to 85% when using bar code technology alone.

This is by no means the only example of RFID being used for baggage control. As long ago as 1999, British Airways tested 150,000 RFID tags operating on the 13.56MHz band on flights from Manchester and Munich to London Heathrow airport.

FROM SMART ACCESS...

Away from RFID, an increasing number of organizations in the aerospace and airport industries are using multi-application smart cards to provide employees with a host of functions. For example, Boeing is implementing a smart card based enterprise-wide identity management system, known as SecureBadge, to provide access to information systems and buildings. The program's design phase began in 2001 when the company examined standardizing its employee identification and physical and logical access control technologies. Companies involved in this program include Siemens Information and Communication Networks, BellID and Gemplus. Meanwhile, Roissy Charles de Gaulle and Orly airports in Paris have implemented a staff access control solution using biometric fingerprint technology and contactless cards. The system, which is estimated to affect 90,000 people across the two airports, includes 100 fixed and 15 mobile security checkpoints. The system is designed to enforce security and increase control reliability whilst reducing the amount of time it takes staff to access working zones. Sagem was the prime contractor for this project, which was implemented in partnership with Omnitech.

...TO SMART TRAVEL

And the technology doesn't stop there. The traveling public is increasingly accustomed to using smart documentation for verification. E-passports are becoming a reality worldwide, providing an answer to the requirements of increased traceability and a need to link travel documents.

Smart chip-based electronic passports answer the need for cost-effective, large-scale border crossing and identification applications. Consequently, many governments are now working with the ICAO to issue a specification for chip-based passports utilizing biometric data. This seems like the ultimate level in security, because individual physical features are what make a person unique.

BIOMETRICS

The US has launched a road map for the migration to contactless chip passports for all its citizens as well as strengthening the laws on immigration with systematic biometric data collection for citizens of visa-requiring countries. Furthermore, from the third quarter of 2005, all passports from the 27 US Visa Waiver Countries, whose citizens can enter the US without a visa, will need to contain biometric data.

Meanwhile, in Burma, an electronic passport system was launched in 2002. This system involved the embedding of a microchip in the passport, containing information about the holder including photographs and fingerprints, and was established to check passports at automatic gates in the departure terminals at Rangoon International airport. In the first week of operation, 5,000 e-passports were issued to Burmese diplomats, officials and selected members of the business community as part of a pilot program. The technology for the passports came from Malaysia-based Iris Corporation.

In the UK, the Home Office, in partnership with key border control, law enforcement and intelligence agencies, is coordinating an e-Borders initiative. A key component of this initiative will be project IRIS (Iris Recognition Immigration System) – an automated border entry system using iris recognition technology to fast track trusted travelers through immigration control. The system – supplied by Sagem – is being deployed at the country's Heathrow, Gatwick, Manchester, Birmingham and Stansted airports, and is due to be fully operational by the middle of 2005. This project builds on an earlier frequent flyer program which was successfully trialed at Heathrow airport using Eye-Ticket Corporation's JetStream Passenger Processing System to process North American frequent travelers traveling to the UK with British Airways or Virgin Atlantic.

Across the Atlantic, January 2005 saw the announcement that JFK Airport in New York will be operating a pilot using iris recognition to speed pre-registered passengers through security and customs checkpoints. Travelers who enroll in the system will have to go through a background check, including criminal history reviews, fingerprinting and a face-to-face interview with a Homeland Security official. Once approved, passengers will be given a smart card containing their passport and biometric iris information. The system will be available to US citizens, legal permanent residents and foreigners who are frequent travelers to the US.

IN THE REAL WORLD...

Taking a look at many of the world's airports, a range of technology initiatives are having a major impact on the way we travel. Twenty years ago, when the world was divided along East and West lines, the airport experience would have been markedly different for most business travelers.

Today, we're used to authenticating ourselves several times before we've even entered an airport – and chances are chip-based secure technology will have been used for some of this authentication.

Consider the case of John, the Vice President of marketing for a major global machinery supplier.

SECURITY

Booking the airline reservation will have required some level of authentication. He may have booked over the Internet using passwords, secure socket layers and even an EMV card connected to a smart card reader. His payment would have gone through the credit card association's behavioral scoring mechanism to ensure his payment wasn't totally out of character with his usual purchasing habits. The airline's web booking engine could have been connected to the Sabre Reservation System, which has direct links to the credit card associations for credit card processing, reducing the possibility of transactions being further exposed to the web.

Or perhaps his reservation was made via a biometric-based system to the airline's call centre. Whichever approach he took, booking an airline ticket is much easier and quicker than in the days of visiting travel agents and getting them to arrange everything. And it doesn't stop there.

There's a good chance that he will be using a ticket-less airline, such as British Airways or Lufthansa. If so, technology would have been used to create an electronically held record (or ticket) of his transaction, and will be stored in the reservation system of his airline carrier. That seems like a major advantage: it's convenient, fast and safe. And unlike the bad old days when he had to pay 15 euros for a duplicate ticket to be issued, there's no worry that the ticket could get lost or stolen. Furthermore, e-ticketing is also helping speed up the time spent queuing, as a paper ticket no longer has to be collected from an airline's office.

CONVENIENCE

When John leaves his house, chances are he'll use RFID technology to open his car door. Perhaps he'll drive along a toll road on his way to the airport. And if he makes this journey frequently, there's a good chance he'll be using a smart-enabled device to pay the toll. Perhaps it will be a contactless card or an onboard unit in the car that communicates with the gate through infrared technology.

On the other hand, he may have taken the train. In which case, his contactless travel card may have been used.

AT THE AIRPORT

John checks in with his e-ticket and passport. In the future, he may be using a smart card containing an ICAO-compliant fingerprint for verification. The man at the check-in desk, who has a chip-based company identity card around his neck, loads an e-boarding pass on to the smart card and stores John's frequent traveler bonus points on it as well. John puts his suitcase on the scales. An RFID tag for track and trace is fitted to the suitcase handle and the RFID tag number is stored on the smart card.

As he moves airside, John goes through passport control. The government official, complete with a chip-based identity card, looks at John's passport and boarding pass, before turning to an airport employee who is being fast-tracked through security.

Once airside, John meets his colleague, who is just about to depart on a trip to New York. As a frequent traveler to JFK airport, she is enrolled in a biometric iris-based frequent flyer scheme, enabling her to speed through security.

TOTALLY TECHNICAL

It's now 8 am and John has a conference call with a colleague in Dubai. After a quick trip to the coffee shop, he finds a quiet place to make his call. He keys his pass code into his telephone handset and activates the SIM card in his phone. He's now ready to call his colleague Barry from the address book stored on his SIM. During the discussion, it emerges that Barry hasn't received the short email that John sent from his PDA last night. Today, John is using his laptop. He has confidence in the laptop as a Trusted Client, thanks to its use of a Trusted Platform Module (TPM), which provides the capabilities of a built-in secure chip to provide strong authentication, giving a higher level of assurance to secure networks. John sees that he is in a wireless fidelity (WiFi) hotspot. Knowing that he can get a wireless Internet connection, and can transmit information in wave form reasonably quickly, he boots up his laptop, makes a WiFi connection and emails Barry again.

With 15 minutes until boarding to go, John looks around the shops. Maybe he'll purchase some duty free with his EMV chip and PIN card. Or perhaps he'll make an impulse purchase in a retail outlet and receive loyalty points on his chip-based loyalty card.

Just as he's about to switch his telephone off to board the plane, John remembers to text his partner to remind her to put the bins out – yes, SMS technology has even entered the world of the most boring domestic task!

Finally, he shows his e-boarding pass and e-passport to the airline employee.

SATISFACTION

When he reaches Frankfurt, John turns on his telephone, which automatically goes into roaming mode. He calls his answer phone, and is asked to key in a PIN. He then goes through to baggage control. After waiting 10 minutes, his bags appear on the carousel. John breathes a sigh of relief. After a major international airline lost his luggage for several days back in 1995, he is always slightly nervous that he may have to make a presentation in the rather crumpled clothes he has spent a day traveling in. John doesn't realize that the airline has improved its baggage handling service using RFID technology.

Having successfully completed his journey, it's unlikely that John will reflect on how chip technology has improved his traveling experience. While he is enjoying a working lunch in Frankfurt, business will continue as normal at the airports he has traveled through today. Improved levels of authentication are being provided for a host of applications. Customers are happy because their bookings can't get lost or stolen, and airlines are able to improve services cost-effectively. And finally, the airport can be sure that a high level of security has been used, thanks to systems that comply with international travel regulations.

SCIENCE FACT

In the airport environment, secure technology is widely used by a broad cross-section of individuals. Whether the individual is traveling or working, spending money or earning money, entering a secure area or participating in a loyalty scheme, technology ensuring convenience and safety lays at the heart of any airport experience. The technologies are in place, the products are available and the number of reference cases is growing rapidly as pilot projects as varied as Delta's implementation of RFID and JFK's use of biometrics demonstrates.

When we reached the millennium, the media commented that some of the technical leaps and bounds that had been forecast in the 1970s had failed to materialize. OK, we don't have individual space pods, and some 'futuristic gadgets' have been and gone, but we've certainly moved into a high tech age – and even if chips don't fit into the Atkins diet, they certainly figure highly in the rest of our life!

Whether we're checking our messages on our PDAs, making payments with our credit cards, using our mobile phones, gaining access to our work place or using ID cards and passports, chip technology is – and will continue to be – very much a part of our daily life.

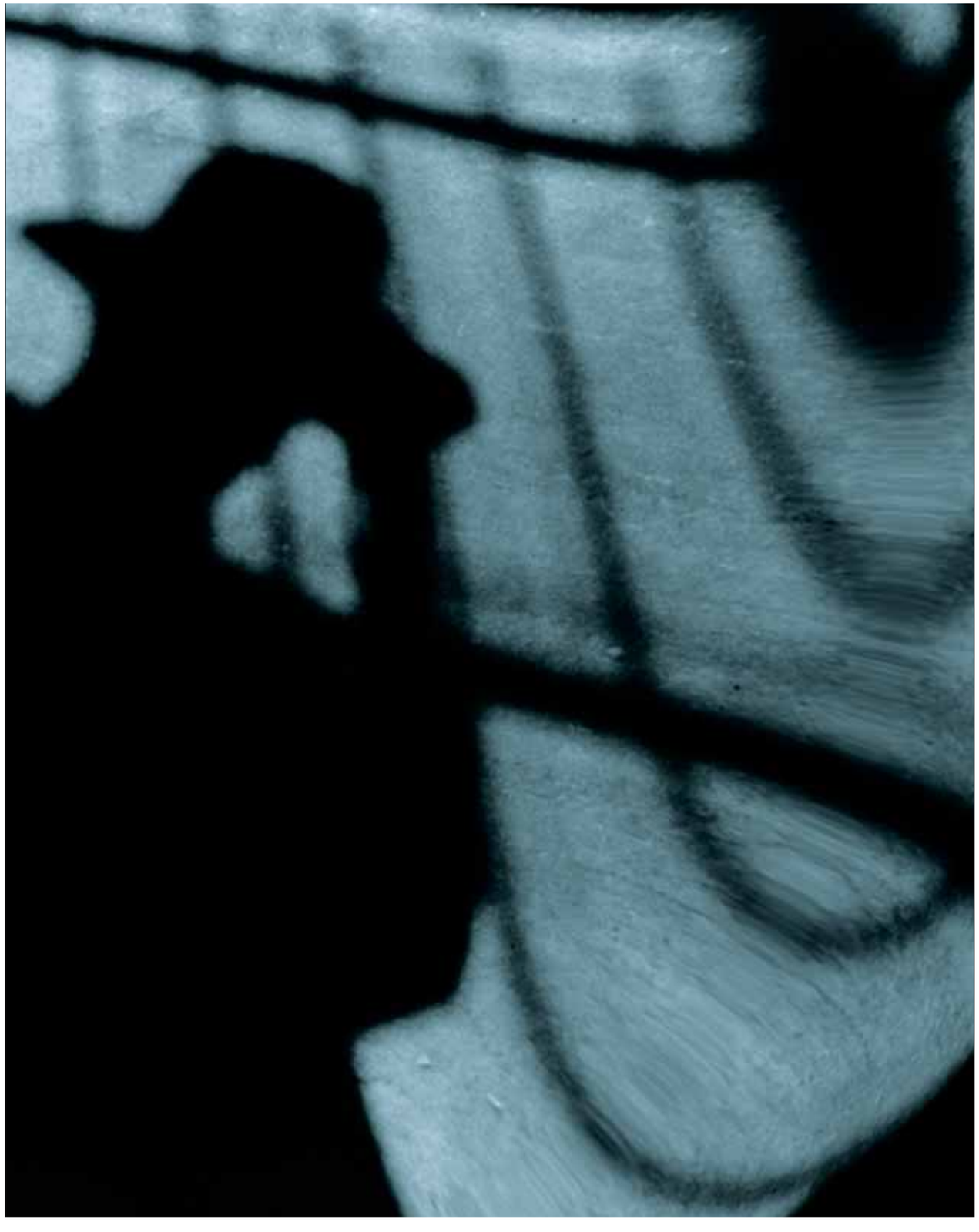
☞ MYTH VERSUS REALITY

By the Silicon Trust

Like most new concepts, ePassport technology has come in for its fair share of criticism over the past few years. Although a lot of this analysis has been the standard level of scrutiny that an inventor can expect to face from a skeptical public, the middle of 2006 saw a series of allegations and a certain amount of hysteria being whipped up by some media outlets. We look at the background to ePassports and examine some of the security measures being implemented.

Throughout much of the developed world, immigration, security and terrorism have become political hot potatoes. Members of the public are rightly concerned that their country should not become a target for terrorists and organized criminals. Governments are addressing these challenges with a raft of initiatives that range from investing more in both covert and overt security operations as well as deploying technology aimed at improving and automating security and identification procedures.

In the case of international travel, ePassport technology is being implemented to help identify and authenticate travelers, so that governments and airport authorities can ensure that the normal traveling public can travel across country borders and board planes with as little hassle as possible.



However, governments face challenges. Citizens have expressed concern about the security of ePassports, fear that their passport could be cloned or skimmed, worry that the use of biometrics is somehow an infringement of their privacy and have voiced reservations that the technology will not actually address terrorist threats.

These concerns must be taken seriously, and governments need to implement transparent procedures to ensure they continue to carry the public's trust.

Implementing Security

The latest ePassports are considerably more secure than previous passport documents. ☞

☞The contactless chips used in ePassports are passive. This means that the chip can only operate when a strong radio frequency electromagnetic field is in the contactless chip's antenna.

Attempts to skim a passport are counteracted via simple procedures which require the owner of the passport to place their passport on a reader capable of scanning the machine-readable zone (MRZ). The MRZ is a combination of numbers and letters at the bottom of each passport. Information contained here is used to generate an access code that is required to read the data contained on the chip. This means that a passport can only be read after having physical access to the ePassport – if the passport holder voluntarily places his or her passport on the reader.

All information stored on the chip is locked using highly secure advanced encryption techniques in such a way that it cannot be changed. In other words, even if a criminal was able to make a duplicate passport, the photo of the real passport holder would still be stored on the chip, so it would not be of any use to a criminal attempting to cross a country's borders. Furthermore, the chip is embedded in an ePassport in such a way that attempts at substituting it should be fairly obvious to any immigration official.

The beauty of the chip technology is that all information visible on the printed data page of the passport – including the holder's date of birth and photograph – is also stored on the chip and can therefore be displayed on an immigration official's computer screen at passport control. This means that attempts by a potential terrorist to circumvent a watch-list by forging a passport with his or her photo on the printed page could be thwarted, if the information stored on the chip does not match the information printed on the data page.

Unattended Environment

If the ePassport was to be used in an unattended border control environment, governments would need to have clear plans and procedures in place to ensure security levels remained high. For example, a biometric system could be implemented to verify the biometric image stored on the passport chip against the person presenting the document.

Chip Security

Inside the chip, a number of technical processes have been implemented to achieve high levels of security and privacy. Such methods include:

- Basic Access Control. This uses challenge/response protocols and can prevent skimming and eavesdropping via a secure communication.

- Active authentication. This is also based on a challenge/response mechanism. If the passport is cloned it will not be able to adhere to this mechanism because it is impossible to clone the required private key which is stored separately in the passport chip.

- Data encryption. This protects sensitive data.

- Extended Access Control. This prevents unauthorized skimming of and access to sensitive data like fingerprints. It also proves that the reader communicating with the chip is a valid one.

- Passive authentication. This uses digital signatures and provides proof that the Logical Data Structure (LDS) and Document Certificate are authenticated and not modified.

The number of security mechanisms present in the contactless chips of all the major ePassport chip suppliers is tremendous. For example, Infineon's SLE 66 chips, which are used in many major ePassport schemes worldwide, including the US and Germany, contain the latest security mechanisms embedded in protected hardware to ensure that personal data is protected against unauthorized read-out and manipulation. Among the security features, the chips use a special computing algorithm – known as the RSA method – for encrypting data. The chips also include active protective shields on their surface and sensors that prevent hackers from being able to read the chip by applying different voltages. The high level of security is demonstrated through the industry's highest security certificate EAL5+ (high).

The move towards ePassports is gathering pace worldwide. Most visa waiver countries have hit the US-imposed deadline for rolling out ePassports and in October 2006, the UK completed the introduction of its biometric passport. With ePassports rapidly becoming a fact of life, it is only natural that a skeptical public will want to know more about how their personal data is handled. Security and privacy are paramount if trust is to be maintained.

SECURITY TRENDS in the Semiconductor *INDUSTRY*

By Daniela Previtali, Wibu-Systems

There are many aspects to security in automated manufacturing processes and even more so in today's connected factory environment. It is no longer simply a matter of securing the perimeter with access control systems and defining and provisioning rights for different network users' groups. As systems become interconnected, security involves new factors that include the protection of code integrity from tampering, the protection of software from piracy and reverse engineering, and the protection of product and customers' data from depredation.

☐ No industry sector is immune to the inception of Industry 4.0: life science, automotive, automation, and even the utilities are about to experience the opportunities and challenges of remotely operated, controlled and maintained technology. As the future unfolds, many companies are optimizing their processes, and strengthening their positioning in the market through the vigilant protection of their intellectual property and the diversification of their business models.

KINESYS Software is a good example of how manufacturing performance should grow hand in hand with the implementation of security measures in order to ensure long-term business stability and profitability. Founded in 1992 in the Netherlands, KINESYS is a global leader focused on the automation of semiconductor manufacturing "back-end" processes. Their flagship Assembly Line Production Supervisor (ALPS) has grown to be the market leading solution for enterprise-wide substrate mapping and device tracking during semiconductor manufacturing. ALPS features mapping for all types of substrates (wafers, strips, trays, etc.), as well as tracking of devices through the multiple processes used in semiconductor assembly and encapsulation. Both Integrated Device Manufacturers (IDM) and Original Equipment Manufacturers (OEM) in more than 1,400 installations around the world use KINESYS' software for advanced wafer and device traceability and process management.

As semiconductor manufacturing rapidly evolved in Silicon Valley in the early 1990's, KINESYS Founder and CEO, Dave Huntley, focused his efforts on back-end processing and testing of individual chips on the wafer. In the past, this was performed unit-by-unit, applying ink on wafers to optically detect defective copies. However, optical recognition was slow and costly, and with the ever-increasing density of the circuits, ink pollution became unacceptable. His solution was to use a BIN code for each element on a wafer and store wafer map files on a hard disk. Thus, he could capture information about the product and the production process and store it in a database.

> *"A multi-chip device is only as good as its weakest link, so it is crucial to track each chip placement to avoid placing expensive chips alongside failed chips. Without a high-quality, fully automated process, end product wastage and risk can be incalculable."*

Another challenge he faced was that testing and assembly could take place in separate factory locations around the world with various types of machines using proprietary data formats. He addressed this issue by adapting the software to a common format to send messages between test and assembly and then to production machines. This readable data process is much faster than optical recognition and is environmentally friendly. The semiconductor industry organization SEMI helped by creating industry standards, allowing Huntley to build on his pioneering work to standardize for all types of substrates (wafers, strips and trays).

Over the years, KINESYS continued to adapt its software and licensing models to the ever-evolving semiconductor manufacturing industry as companies introduced new automation processes and techniques to improve quality and throughput while reducing waste. Multiple chips were often packaged into a variety of devices used increasingly in markets sectors where a chip defect could cost lives, such as medical, aerospace, and automotive systems. Devices became lighter, smaller, and thinner, making semiconductor assembly in large volumes a highly sophisticated industry. Today, the testing and tracing of individual chips is a critical process.

"A multi-chip device is only as good as its weakest link, so it is crucial to track each chip placement to avoid placing expensive chips alongside failed chips. Without a high-quality, fully automated process, end product wastage and risk can be incalculable," Huntley said.

As the industry became more sophisticated, so did KINESYS' mapping and database technology. Huntley knew that he needed a mechanism to secure the invaluable manufacturing data he was capturing and storing, and protect it against tampering or cyberattacks. At the same time, he also needed a new level of licensing flexibility to adapt to the rapidly changing industry needs.

KINESYS partnered with security technology leader Wibu-Systems and qualified its CodeMeter® platform as the best of breed for data protection, licensing, and security against piracy, reverse engineering, tampering, and cyberattacks. With CodeMeter, KINESYS is able to protect its revenue stream while leaving the door open to more sophisticated licensing models, in line with the constant evolution of chip designs and manufacturing techniques.

A CodeMeter USB Stick (CmStick) is delivered with each installation. The CmStick has an embedded smart card chip where the KINESYS software encryption key and license information is securely stored. The dongle form factor (USB Stick) offers the strongest security against any hacking attempt, and is non-invasive, as it just needs to be present for the system to run without additional intervention from the user.

In addition to providing a foolproof integrated licensing solution, CodeMeter blocks unauthorized use of KINESYS software. Software security is a requisite, but it should not be an inconvenience in everyday use in a manufacturing production control environment. The balance between functionality and quality is always a delicate one.

Moreover, thanks to the collaboration with Wibu-Systems, KINESYS has the opportunity to future-proof their product in line with more flexible licensing models linked to SEMI standards and manufacturers evolving production needs.

Software security is a requisite, but it should not be an inconvenience in everyday use in a manufacturing production control environment. The balance between functionality and quality is always a delicate one.

CodeMeter also provides KINESYS with an accurate accounting of the use of its software, thus helping them to fully monetize their product. In their current license model, customers pay a license fee for each individual piece of production equipment to which the software connects. However, they fully expect other licensing schemes to come into play, such as licensing based on data volume or for subscription license models, as customer's progress to a higher level of product cost accountability.

It is now common for the cost of the software and the equipment to be attributable to the total capital expenditures of a microchip factory. The equipment-connect license fits well with this cost accounting model but KINESYS expects the flexibility to deploy other license models will allow them to evolve in line with the customer's appreciation of more cost-accountable manufacturing techniques. ☒

2015 ID4*AFRICA*: The *inaugural* EVENT

By Joseph Atick, IBIA and Greg Pote, APSCA

Development agencies are bullish on Africa's prospects. The World Bank's June 2014 Global Economic Prospects report lists sub-Saharan Africa as one of the fastest-growing regions globally. According to a recent report by the African Development Bank, average growth was 3.9% last year and is expected to accelerate in 2015. An article in The Economist in May this year stated that foreign direct investment (FDI) is expected to reach $55 billion in 2015, 20% higher than in 2010. In contrast to inflows of capital in previous years, recent investments are increasingly targeting the less resource-rich countries and Africa's booming middle classes. According to the same article, the amount of investment into technology, retail and business services in Africa increased by 17 percentage points between 2007 and 2013.

☐ Although European states spearheaded trade with Africa, today Asia is increasingly playing a larger role in the growth of African GDP. Chinese investment and development projects in Africa have been a significant driver of economic growth for several years. Anyone who has taken a recent flight from Shanghai to Africa would have found it packed with Chinese blue-collar workers going to work as middle managers in construction and mining projects in East and West Africa. Despite the inroads already made by China, African trade with India is now growing at a faster rate than Chinese trade and is projected to reach $100 billion in 2015.

However, while Africa's economic growth is accelerating, the benefits are still by far unevenly distributed. For social development to match economic growth and generate long-term gains, inclusiveness is essential. There is a clear need for robust national systems that provide digital identity to all Africans, ensuring that everyone can access government services and benefits, prove their eligibility and be included in Africa's economic takeoff. This is why the recently launched ID4Africa event held in June this year, was an event whose time had truly arrived.

The idea for ID4Africa was motivated by the need to change the current situation of identification systems in Africa, where large segments of the population continue to suffer from the lack of robust and accessible ID. In many cases they are not documented in the civil register and as adults they do not hold identity credentials that enable them to exercise their rights and participate in society. As a consequence, they remain in the shadows of society; excluded, burdened and unable to benefit from the fruits of development.

This clearly has to change.

ID4Africa was conceived to promote the responsible adoption of modern digital identity systems as drivers of socio-economic development. It is a forum designed to allow African nations to compare experiences, share knowledge and pool resources to build capacity related to developing identity systems. It is a movement of empowerment where Africa would take matters into its own hands and would dictate how it will respond to its identification needs.

In June 2015, the unprecedented ID4Africa – 1st Government Forum on Electronic Identity, brought together over 300 regional and international representatives of four key stakeholder groups in the identity space in Africa: the identity authorities and users, the international development agencies, the solution providers and the domain experts. The convergence of these four groups in a focused forum created unique opportunities for networking and exchange of ideas, experiences and funding sources. It united all the necessary ingredients for enabling the right ecosystem to emerge for the adoption of e-ID in the service of socio-economic development.

The forum featured an exciting lineup of government and identity experts that presented on real experience relevant to Africa, on topics that are hot today. Many discussions were held on the subject of establishing central databases, biometric enrolment and verification, as well as the different services that could be offered through national ID systems. Most importantly, this was the first forum in Africa that brought together under one roof over 30 global identity industry leaders, to exhibit their latest innovations related to digital identity and secure credentials. It created a unique opportunity for identity experts to demonstrate and explain to senior African government decision-makers responsible for national identity systems, how these solutions can be used to build identity systems that will support socio-economic development in Africa.

While developments in digital identity systems are being undertaken in a number of African countries, many of these systems are still a far way off from ensuring that the benefits they were designed to provide are being received by the citizens who need it most.

At the end of the first day, Forum Chairs Joseph Atick and Greg Pote highlighted a number of key issues, which had quickly surfaced during the presentations and discussions. It was clear that while developments in digital identity systems are being undertaken in a number of African countries, many of these systems are still a far way off from ensuring that the benefits they were designed to provide are being received by the citizens who need it most, and that this would hamper all efforts in having citizens view their national IDs as a fundamental part of their existence.

Another vital issue expressed throughout the forum was the stifled level of investment given to developing civil registries (which include birth, death and civil status records), particularly when one considers they are the wellspring from which all other identity systems grow. However, what became certain was that Africa has a united resolve to make the best investments forward to improve on, and provide sound and effective national identity systems that will equally benefit all citizens.

ID4Africa calls for an annual meeting to allow the movement to define the agenda year after year and to achieve the stated objective. The inaugural event was proudly hosted by The National Identification Authority (NIDA) of the Ministry of Home Affairs of Tanzania, and organised by APSCA and the Identity Counsel International (ICI). ☒

ID4Africa 2016 will be held on May 24-26, 2016 in Kigali, Rwanda and will be hosted by the National Identification Agency of the Government of the Republic of Rwanda.

A TRUSTED and *SECURE* Identity for all *Europeans*?

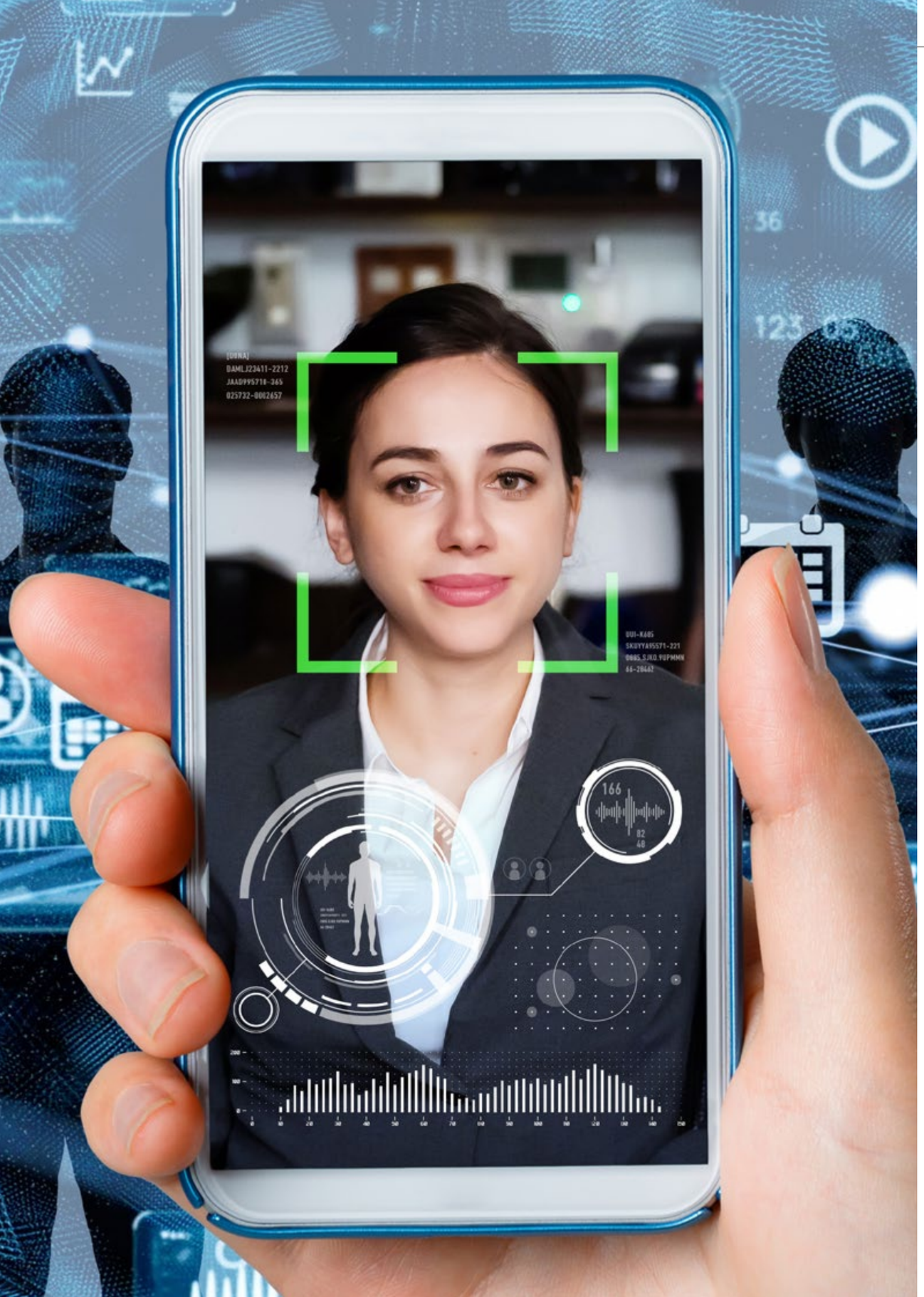
By Steve Atkins, Silicon Trust

☐ Early in June this year, The European Commission proposed a framework for a European Digital Identity, which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets, with the click of a button on their phone. They will be able to access online services with their national digital identification, that will be recognized throughout Europe. Very large platforms will be required to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

"The European digital identity will enable us to do in any Member State as we do at home, without any extra cost and fewer hurdles. Be that renting a flat or opening a bank account outside of our home country. And do this in a way that is secure and transparent. So that we will decide how much information we wish to share about ourselves, with whom and for what purpose," commented Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age. "This is a unique opportunity to take us all further into experiencing what it means to live in Europe, and to be European."

Under the new Regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g., driving license, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognized by a Member State. Thierry Breton, Commissioner for Internal Market is reported to have said, "EU citizens not only expect a high level of security, but also convenience, whether they are dealing with national administrations such as to submit a tax return or to enroll at a European university where they need official identification. The European Digital Identity wallets offer a new possibility for them to store and use data for all sorts of services, from checking in at the airport to renting a car. It is about giving a choice to consumers; a European choice. Our European companies, large and small, will also benefit from this digital identity; they will be able to offer a wide range of new services, since the proposal offers a solution for secure and trusted identification services."

The new European Digital Identity Wallets will enable all Europeans to access services online and will securely store payment details and passwords, allowing Europeans to access these public and private services across the bloc, e.g. renting a flat, accessing a bank account, applying for loans, etc., via a single recognizable identity. Most importantly, it will be a standalone identification method, eliminating the needless sharing of personal data.



> *In parallel to the legislative process, the Commission will work with Member States and the private sector on technical aspects of the European Digital Identity.*

The European Digital Identity will be:

- Available to anyone who wants to use it: Any EU citizen, resident, and business in the Union who would like to make use of the European Digital Identity will be able to do so.

- Widely useable: The European Digital Identity wallets will be useable widely, as a way either to identify users or to prove certain personal attributes, for the purpose of access to public and private digital services across the Union.

- Users in control of their data: The European Digital Identity wallets will enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared, will be shared.

In parallel to the legislative process, the Commission will work with Member States and the private sector on technical aspects of the European Digital Identity. Through the Digital Europe Program, the Commission will support the implementation of the European Digital Identity framework, and many Member States have foreseen projects for the implementation of the e-government solutions, including the European Digital Identity in their national plans under the Recovery and Resilience Facility.

The Commission's 2030 Digital Compass set out a number of targets and milestones which the European Digital Identity will help achieve. For example, by 2030, all key public services should be available online, all citizens will have access to electronic medical records; and 80% citizens should use an eID solution.

For this initiative, the Commission builds on the existing cross-border legal framework for trusted digital identities, the European electronic identification and trust services initiative (eIDAS Regulation). Adopted in 2014, it provides the basis for cross-border electronic identification, authentication and website certification within the EU. Already about 60% of Europeans can benefit from the current system.

However, a note of caution sounded by industry players over plans for a pan-EU wallet. These players point to the lack of foundational capabilities, especially in the financial sector ,that prevents the true unification of such a market. Industry observers argue that this capability, just like any marketplace, will require a significant push to be adopted. That's why one of the main challenges surrounding the EU eID will be introducing the idea to EU citizens, as projecting a clear-cut value proposition could give it the much-needed boost.

Marius Galdikas, CEO at ConnectPay, echoed the view of a number of these industry players when he said, "If EU citizens do not sign-up, there will be no point for businesses to use this wallet. Furthermore, people will not be inclined to sign up unless there is clear value for them, in other words, a sufficient number of businesses that have already signed up. Interestingly enough, this dilemma becomes similar to "the chicken or the

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

MaskTech GmbH
Nordostpark 45
90411 Nuremberg | Germany

Phone +49 911 95 51 49-0
Fax +49 911 95 51 49-7
E-Mail info@masktech.de

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