NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2022

The VAULT

ARTIFICIAL INTELLIGENCE

FEATURED ARTICLE

Can we trust Artificial Intelligence?

Wibu-Systems

ALSO IN THIS ISSUE

Infineon Technologies
How biomentrics could impact the future of payments

Mühlbauer Group
Ready for the revolution?

Infineon Technologies
Secured NFC tags enhance brand experience

Mühlbauer
High Tech International

WE TAILOR YOUR SOLUTION – **MÜHLBAUER**

SECURITY IS NOT A PRODUCT, BUT ONE OF THE MOST VALUABLE GOODS OF A NATION. DON'T ADAPT TO THE GIVENS, LET THE GIVENS ADAPT TO YOUR DEMANDS. MÜHLBAUER IS THE GLOBAL SPECIALIST FOR RELIABLE IDENTIFICATION, VERIFICATION AND AUTHENTICATION OF PEOPLE AND DOCUMENTS. SECURITY BY DESIGN. PROTECT YOUR FUTURE – REALIZE YOUR PROJECT WITH MÜHLBAUER!

CUSTOMIZED SYSTEMS FOR INDIVIDUAL NEEDS.

www.muehlbauer.de

Contents

Ready for the revolution: Mozambique's journey from paper documents to eVisa 4
Katharina Schuldt, Mühlbauer ID Services GmbH

Infineon's secured NFC tags prevent counterfeiting and enhance brand experience 6
Infineon Technologies

How biometrics could impact the future of payments 8
Wolfgang Schindler, Infineon Technologies

Can we trust Artificial Intelligence? 12
Dr. Carmen Kempka, Wibu-Systems

AUSTRIACARD Holdings AG applies for stock exchange listing and to merge with INFORM P. LYKOS Holdings S.A. 18
AUSTRIACARD

Silicon Trust Directory 2022 22

Imprint

THE VAULT ISSUE 35
Published by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Steve Atkins, Wolfgang Schindler, Dr. Carmen Kempka, Katharina Schuldt
PHOTOS: ISTOCKPHOTO, WIBU_SYSTEMS, MÜHLBAUER, INFINEON TECHNOLOGIES, KROWNE COMMUNICATIONS ,

READY for the *REVOLUTION:* Mozambique's *journey* from *PAPER* DOCUMENTS to eVisa

By Katharina Schuldt, Mühlbauer ID Services

They started in 2018 with a great undertaking. The Government of the Republic of Mozambique had planned to equip all borders and airports in the country with state-of-the-art technology. However, modernizing all border posts means not only replacing hardware and software at the 13 airports, 24 land and 7 sea borders, but also ensuring that all Mozambican residents have access to high-tech travel documents, such as electronic IDs and eVisas.

The German specialist in the security sector, Mühlbauer, took on this far-reaching assignment. The project's scope was to install and ramp-up, a cutting-edge solution for the issuance and verification of multiple types of identification documents. At the same time, it was necessary to implement a comprehensive border control system, to identify and verify documents, as well as the document holder. Such a system needs to reliably register and manage all entry and exit data, while interfacing with third parties on a local, as well as international level, to exchange information.

Let's get some idea of the scale of the project. The new management systems were distributed nationwide to 11 provinces and 177 districts, to all 13 airports, to a total of 44 land, river and sea borders and to 45 embassies and consulates worldwide. In order to accomplish this task with the smallest possible time schedule and in cooperation with local companies, Mühlbauer established its own business location in the capital Maputo, staffed with 60 employees, to handle contract delivery, ongoing technical support and training. More than 800 government employees have since been trained and empowered to operate and maintain the highly sophisticated systems. The complete solution was delivered in just 6 months and put into full operation within 12 month of the contract being signed.

The enrollment system can be operated online and offline (depending on network availability). Mühlbauer IT and software products and system observe the highest security standards regarding data transfer and data management. The implemented solution consists of four independently operable databases (citizen data, foreigner data, travel documents and border management), for four designated authorities, which are all interlinked and interoperable for national security and information purposes. The embassies and consulates of Mozambique have been enabled to issue biometric identification cards, electronic travel documents, biometric emergency travel documents for all citizens of Mozambique, as well as visas to foreign visitors.

To further improve the services rendered, the Government of Mozambique is now expanding its solution to include an eVisa portal. In close cooperation with Mühlbauer, the paper-based system is to be supplemented and replaced. Until now, a traveler applying for a visa had to fill out the necessary paperwork and then send it by mail or physically take it to the local embassy or consulate. The embassy or consulate would then review the documents, process the request, and issue the visa. This process takes a lot of time and makes it burdensome to create a visa.

Automated personalization for the electronic passport takes only 10-12 minutes.

Half a million Mozambicans thus received a cutting-edge identity document in the first year after its introduction.

The Mühlbauer eVisa Solution using the latest technologies, allows the applicant to create an account online. The responsive, web-based portal runs on various standard browsers (Safari, Firefox, Internet Explorer, Chrome) and on standard operating systems (Windows, Linux, macOS, Android, iOS) and respectively on desktop PCs, tablets and mobile phones. After creating the account, the applicant is asked to enter personal data, upload a facial image and supporting documents – including a passport scan – and perform an online payment or register an already performed payment, based on the receipt.

This secured and multi-lingual portal is kept separate from the main visa system to reduce its appeal to hackers, thereby protecting it against potential attacks. The application will then be submitted to the Central Visa system for approval.

When the visa application is processed, the applicant is informed via email and receives an approved Preliminary eVisa Document or the Application Rejection Letter, in case of a negative decision. The final and only step, which requires physical attendance, is the personalization of the eVisa.

On arrival at the airport, land border or at the embassy, the enrollment officer pre-obtains the application from CMS, checks pre-enrolled data, and captures any additional applicant's data. During this process, the data on the identification document and the eVisa are checked for authenticity by comparing them with existing databases. After successful verification, the approved visa or visa stickers are handed out to the applicant. The customizable and fully responsive system supports all 15 visa types, such as a Business visa, Visit visa, Tourism visa, Residence visa, Student visa and Transit visa, and can be extended if needed.

With its simplified handling and fast data transfer, the state-of-the-art visa solution from Mühlbauer ensures user-friendly application and prevents long queues at border crossings and authorities. With the pandemic not yet over, the mainly digital visa issuance is a particular step forward for Mozambique. This not only makes official processes easier for every resident and applicant, but also provides greater health security and ensures there is one less platform for the virus to spread. All these newly implemented solutions make the Southeast African country a pioneer in digital identification. ☒

Infineon's SECURED NFC tags *prevent* COUNTERFEITING and enhance *BRAND* EXPERIENCE

☐ Counterfeit products have a negative impact on brands: not only do they affect revenue, but they also damage brand image with poor user experiences. In industries such as pharmaceuticals and food, counterfeit products can even pose a serious threat to consumer health and safety. Hence, companies are always on the lookout for robust anti-counterfeiting solutions. Also, in today's competitive world, customers have a variety of brands to choose from, making it essential for companies to leverage technology, in order to increase brand awareness and build customer loyalty.

Infineon Technologies AG offers secured NFC tags that meet high security requirements for proving authenticity. The NFC4TCxxx tag includes an open standard security architecture using AES-128 cryptography and is equipped with inherent resistance to physical attacks such as Differential Power Analysis (DPA) and Differential Fault Analysis (DFA). Infineon's secured NFC tags also offer a wide range of memory options, from 304 bytes to 4 Kbytes. This enables brands to store data and create customized applications to improve their customer engagement.

The tags can be programmed with brand-specific landing pages that provide additional information about the product and also show the customer a list of similar products. They can provide exclusive offers and invite to special events which helps to build a long-term relationship leading to repeat purchases. At the same time, brands can use customer analytics to constantly optimize their products and marketing campaigns. By enabling two-way communication between the consumer and the brand, NFC gives a competitive advantage to various brands.

To further accelerate the deployment of brand protection applications, Infineon has launched the NFC 2Go starter kit for brand protection. The kit demonstrates consumer product authentication enabled by Infineon's secured NFC tags with an NFC smartphone. The kit includes NFC stickers, iOS and Android mobile apps, backend cloud authentication software, tag personalization tools and a user guide. ☒

Availability

The NFC4TCxx tags and the NFC 2Go starter kit for brand protection can be ordered now. More information is available at: www.infineon.com/NFC-solutions

cryptovision

Your last mistake is the best teacher

Applet Suite certified on
NXP
Infineon
Veridos

We offer more control and no regrets for your next eID project

We all have regrets sometimes. Choose your party wisely and you won't wake up with a hangover. Working with cryptovision for your next eID project means that you will stay in control. Your customers will appreciate the flexibility and ingenuity of our solutions.
Don't make the same mistake twice – get in touch with us.

Find out more on cryptovision.com/eID

- Java Card™ Applet Suite
- Personalization Middleware
- Certificate Management
- Public Key Infrastructures

Atos

How *BIOMETRICS* could *impact* the FUTURE of PAYMENTS

By Wolfgang Schindler, Infineon Technologies

☐ Consumers have come to love the convenience – and lately, hygiene – that comes with contactless payments. After the pandemic subsides, 86% of consumers have indicated a preference to continue making contactless payments. Global contactless transaction values were forecast to reach $2.5 trillion by the end of 2021 alone.

However, contactless payments, like every type of transaction, are not completely free of risk. A lost or stolen card can potentially be used for multiple 'small-value' transactions in a short space of time, without requiring user authentication. Many nations continue to increase contactless limits, making higher-value payments more convenient for consumers, yet raising the potential for larger losses if cards are lost or stolen

Payment solution providers need to balance the convenience of contactless with the need to deliver security layers that build trust. The next generation of contactless cards therefore need options that deliver high security and convenience. One answer could lie in the combination of biometrics and a security chip within the payment card.

Smarter, more personal authentication

Biometric authentication is becoming more prevalent in our daily lives. Just look at smartphones, where 80% of devices now include fingerprint sensors. Infineon products allow the combination of security and convenience on the payment card.

The convenience and overall 'cool factor' of biometric payment cards means there is already a strong consumer appetite for them. A recent survey reveals that half of consumers want a biometric payment card and would be willing to switch banks for one, while 43% would pay extra to get one.

> *Thanks to advances in technology, it is now possible to perform extraction and matching in the security chip on the card, rather than in the payment network.*

Biometric payment cards are still young, but are on a journey towards mass market adoption, with four commercial launches and 23 pilots currently in place globally, and the payments value chain is starting to realise the benefits:

- For consumers: Using a fingerprint for contactless payment only on their own payment card, enables consumers to use convenient, hygienic authentication for their transaction. This could encourage banks to raise contactless limits further, if consumer trust leads to increased demand for higher-value contactless payments.

- For issuing banks: Offering biometric payment cards shows that banks are working to continually enhance the customer experience. If customers respond well to the new technology, biometric payment cards could become 'top of wallet' (i.e. their preferred card), enhancing brand value for the bank.

- For retailers: Contactless biometric cards can provide fast and well-secured transactions, while reducing the burden of handling cash. Also, thanks to global payments standards, accepting biometrics tends to bring no additional infrastructure costs, as the technology works on existing contactless PoS terminals.

Rethinking card technology

Biometric payment cards require several advanced technical components to come together to make them a reality. Until recently, this has threatened commercial viability and created a potential barrier to mass market adoption. Infineon's work is focused on removing these barriers, while supporting usability and security features.

The main challenge is in simplifying how a payment card is physically made, while putting additional functionalities into the semi-conductor – in other words bringing the Secure Element, microcontroller and power units together as one security device. Enabling this to scale across the world's 3.5 billion payment cards will help bring the technology to everyone's wallets.

Biometric cards need much more power than traditional cards to perform calculations to 'extract' and 'match' fingerprint data that authenticates the user. This data is comparatively large and yet the transaction must still happen incredibly quickly to maintain the user experience.

Biometric data is also extremely valuable and unlike a PIN or password cannot be replaced or repaired if compromised. It is therefore important to limit the transfer of biometric data, in order to reduce the level of risk in a transaction.

Thanks to advances in technology, it is now possible to perform extraction and matching in the security chip on the card, rather than in the payment network. This is the most professional way to handle sensitive biometric data. In addition, this process also helps to contribute to a typical latency (the time it takes to complete both the biometric authentication and the payment transaction) of less than 1 second. Enabling seamless transactions is an essential part of any new payment technology.

Turning future visions into reality

The work we are doing on the latest generation of biometric payment cards is designed to reduce the complexities within the card and enable scalable production. These cards can collect power from the terminal/reader and use it to power the fingerprint sensor, memory and computing units.

As well as improving card performance, the other major benefit of our work to closely integrate the fingerprint sensor, Secure Element, power management and communications is that it reduces manufacturing complexity.

This is a significant development that will enable biometric cards to be made at scale, allowing easier integration into existing hot lamination card manufacturing processes. By enabling card manufacturers to produce biometric cards much the same way as they produce current PIN-secured cards, we reduce the investment required to produce them and drastically boost their scalability.

The future of payments enables fast and highly convenient transactions around the world.

Hidden complexities in the cards will power payments simpler than ever to use, putting the world of commerce at your fingertips. ☒

Can we TRUST *Artificial INTELLIGENCE*?

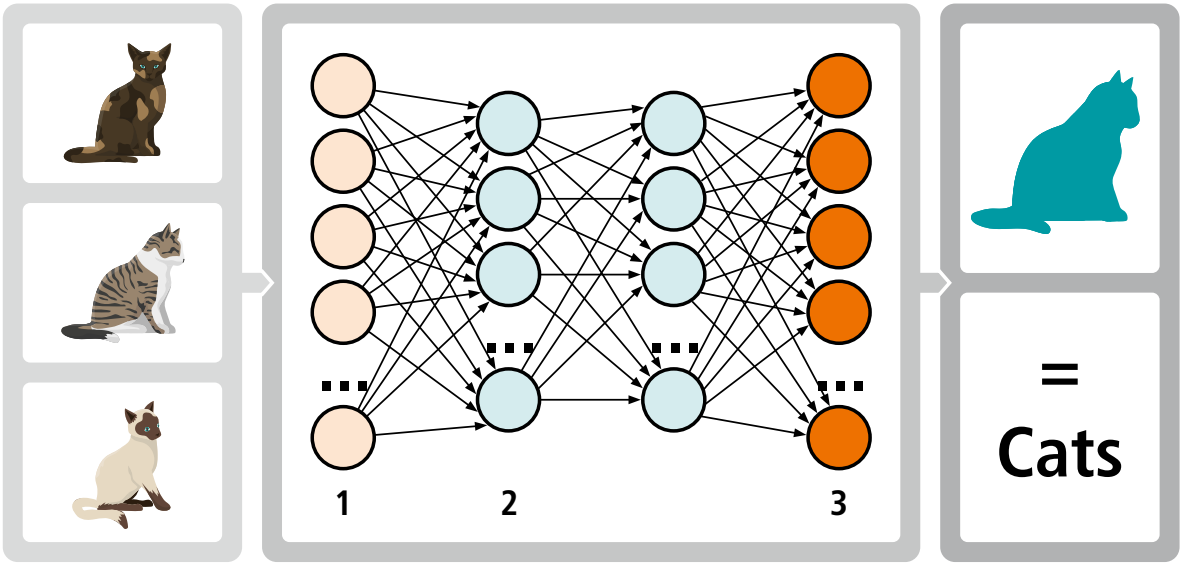
By Dr. Carmen Kempka, Wibu-Systems

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.

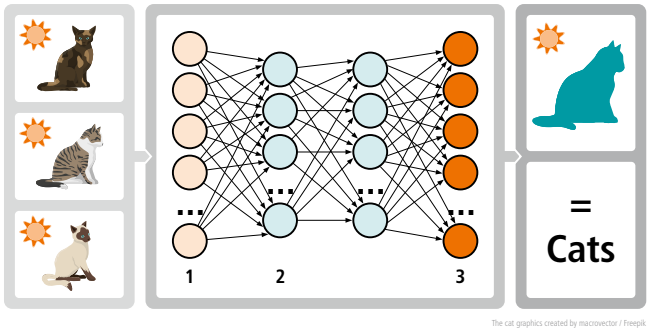
Most importantly, no AI actually "thinks" about its input data or the trained model in any way. There is no sanity check whether the input data or the inferred classification criteria make any sense at all.

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.

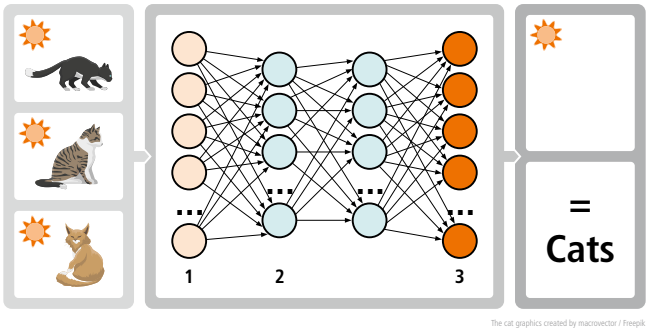
Even worse, if the cats and dogs are hard to distinguish or all cats/dogs look different, the AI will instead learn "sun means cat and rain means dog", not even considering the actual animals anymore in the classification process (Figure 3).

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

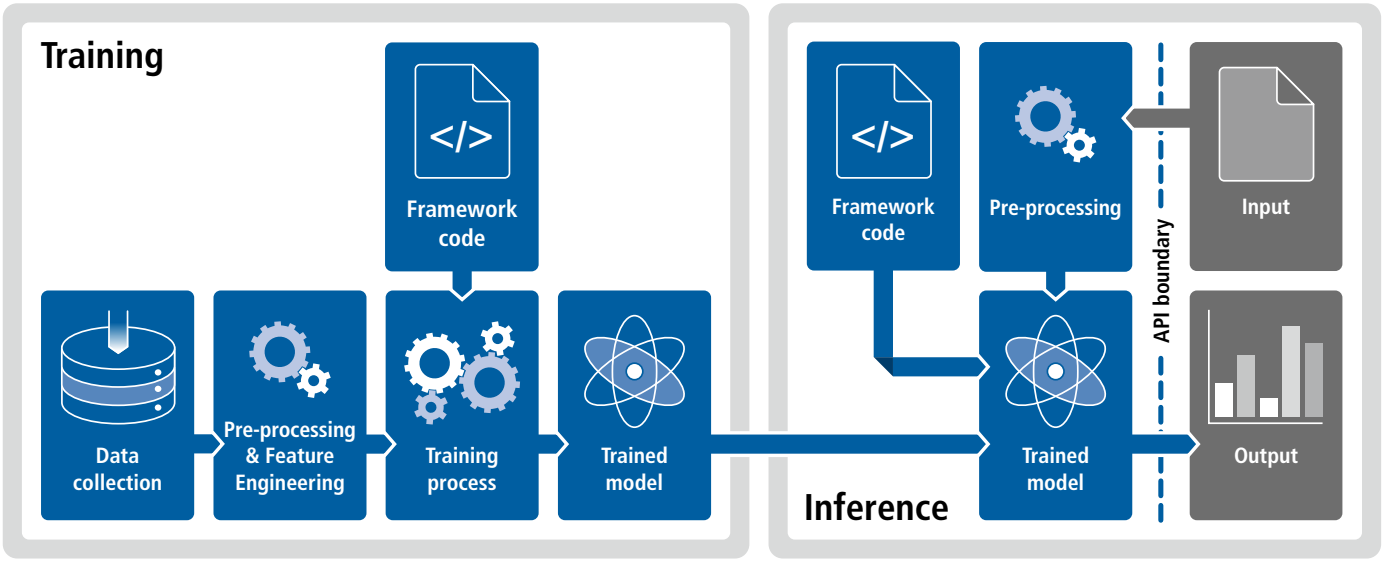


Figure 4

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.

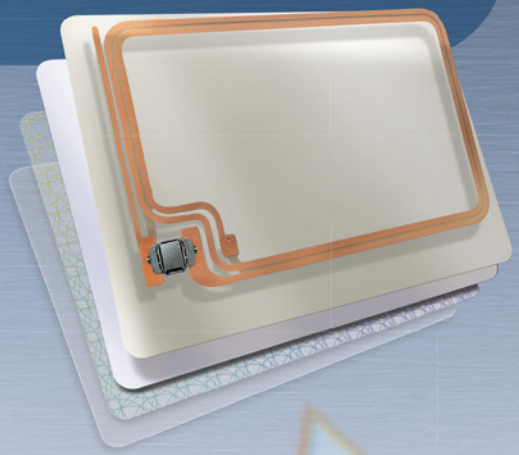
AxProtector Python

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. ⊠

High Speed Inline Production of RFID Inlays



- All types of antennae
- Plated, wire embedded, printed, etched
- Up to 2,400 inlays/hour
- Including lamination and cover application

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

Please visit us at:
TRUSTECH · Paris/France · November 29 – December 01, 2022 · Booth No. D 055

more ▷ **www.melzergmbh.com**

AUSTRIACARD HOLDINGS AG applies for *STOCK* exchange listing and to *MERGE* with INFORM P. LYKOS HOLDINGS S.A.

☐ AUSTRIACARD HOLDINGS AG (ACAG), an Austrian Group with an international presence and one of the leading providers of Secure Digital Technology Solutions in Europe, has announced that it will apply for listing on the Vienna and Athens Stock Exchanges and merge through a cross border transaction with its 70.79% subsidiary INFORM P. LYKOS HOLDINGS S.A., a company listed on the Athens Stock Exchange. Subject to approval by the relevant competent authorities and shareholders' general meetings of both companies, ACAG will absorb INFORM LYKOS and will be listed on the Vienna and Athens Stock Exchanges. This process is expected to be completed by the end of March 2023.

ACAG and its subsidiaries, including AUSTRIA CARD GmbH, INFORM LYKOS and TAG SYSTEMS, provide Secure Digital Technology Solutions and Secure End Products & Services, in two broad categories:

- Secure Digital Technology Solutions, such as Hardware Embedded Security (Internationally Certified Chip Platforms), high added value Payment Solutions, Authentication, Data Capture, Data Mining, Process Automation, AI, Digitalisation Solutions, IoT platforms, etc.

- Secure End Products and Services, such as Banking Smart Cards & Associated Services, Secure Smart Cards for Identification, Health, Driving, Transportation, Billing / Statements, Secure Ballots, Secure Medicine and Alcohol Labels, Electronic Book Publishing and many others, representing a combination of our Secure Digital Technology Solutions, with cutting edge Secure End Products and Services, either in physical or in digital forms.

HIGH SECURITY IDENTITY SOLUTIONS

AUSTRIACARD

Member of AUSTRIACARD HOLDINGS

YOUR PARTNER OF CHOICE FOR ID

austriacard.com

In 2021, ACAG, on a consolidated basis, had €178.0m revenues and €26.8m EBITDA, while in the first half of 2022 revenue reached €137.1m (69% year-on-year increase) and adjusted EBITDA €19.8m (137% year-on-year increase).

The merger is expected to contribute to an improved group profile with increased geographical and product reach, broader cross selling opportunities and increased economies of scale. The more than 1,400 people employed within the Group today, will benefit from an international, closer knit working environment, which will stimulate knowledge, enhance experience sharing, provide international development opportunities and accelerate group-wide adoption of best practices.

Mr. Panagiotis Spyropoulos, Vice Chairman of the Management Board of ACAG and Group CEO, stated: "Having successfully completed the onboarding of the recently added in the Group talented new team members that joined us from the acquired companies, now it is the right time to fully leverage our global footprint, by making available to our clients the full spectrum of the highly Secure Digital Technology Solutions we have already developed and the ones to come, being yet at an R&D phase. Additionally, our listing on both the Vienna and the Athens Stock Exchange, will provide to the investment community the ability to share into our success".

Mr. Manolis Kontos, Executive Vice President, stated: "By implementing this merger, the new group will have a strong portfolio of seamless solutions that are focused in serving our B2B clients which are active in the Banking, Energy, Telcos and Retail in both the Private and Public sectors. With extensive experience of over 125 years in the fields of Information Management & Data Encryption for high-end Secure Communications and with a very customer centric approach, the Group is well positioned to grow its footprint both horizontally and vertically by maximizing internal talent and attracting new".

Mr. Jon Neeraas, Executive Vice President, stated: "Through this merger, our market leading position in the Challenger Banking Segment and our market leading position in key European Banking markets, will be underpinned by award winning digital solutions offerings. Our Banking customers, in Regions such as Scandinavia, Austria, Central Eastern and Southeastern Europe, where we are market leaders today, will be able to access products and solutions complementary to the payment card, whilst we enable our Global Challenger Banking customers to procure digital technology platforms, in order to future proof the value which we provide to this fast paced, high tech segment. Our market share will increase in markets such as the United Kingdom, Spain, Germany, Turkey, Middle East and Africa. Additionally, our operation in the USA will be further strengthened with significant upside potential. Sustainability is crucial to our future and essentially, our road map will serve the next generation of Fintechs and Traditional Banks. By utilizing more efficiently the Group's resources, we shall be able to offer a more solutions-oriented portfolio with end-to-end solutions and services, from card issuance, to payment processing/clearing and advanced high added value payment related solutions. This Embedded Finance model will be a game changer, the first of its kind in our industry".

Mr. Nikolaos Lykos, Chairman of the Management Board of ACAG and major shareholder, stated: "This merger is a pivotal point in the Group's history as it is the culmination of a 40-year-old effort to steer the Company from a world, where people were communicating and thinking through ink and paper, to a world, where communication is a pack of bits, instantaneous, global and elusive. Over the past 125 years our ethos has been hammered to developing the best-in-class solutions and today, we pride ourselves in helping our customers to seamlessly connect to the Digital Era". ☒

Accelerate your eID project with SECORA™ ID

When time is tight and you need a customized solution …

SECORA™ ID is our new ready-to-go Java Card™ solution optimized for electronic identification (eID) applications. It accelerates your time-to-market through ready-to-use applets supporting rapid project migration. Combined with our free development tool, the SECORA™ ID platform gives you maximum freedom to develop your individual eID or multi-application solutions.

Highlights:

- Ready-to-go solution for fast time-to-market
- Easy and rapid migration of individual projects
- Open platform for highest flexibility
- Best-in-class security controllers and wide choice of packages
- Targeting the highest international security standards for eID applications

Find out more:
www.infineon.com/secora-id

SILICON TRUST DIRECTORY 2022

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

ATOS

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries..

www.atos.net

AUSTRIACARD

AUSTRIACARD AG is a holding company of businesses providing end-to-end solutions and products in the field of Digital Security and Information Management. The Group brings together the century-long heritage in printing services and state-of-the-art digital data solutions (Information Management division) with the well-established production and personalization of smart cards and the offer of cutting-edge digital payment solutions (Digital Security division). The combination of well-established industrial roots with an expanding services portfolio that meets the needs of the increasingly digital and mobile economy is at the very core of the Group's confidence in its future.

www.austriacardag.com

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 & Mute-Cards),
- "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

CARDPLUS

CardPlus is a consulting firm with a focus on customized, enterprise level, Identity and Security Management Solutions. We offer a full range of Professional services to build, transform, implement and manage our customized enterprise level security and identity solutions. Due to our vast hands-on experience in designing and implementing secure travel and identification systems for governments and large public sector customers, we are uniquely positioned to understand your highly complex security requirements and translate the same into practical, workable solutions.

www.cardplus.de

COGNITEC

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

www.cognitec-systems.de

CRYPTOVISION

cryptovision is a leading supplier of innovative cryptography & public key infrastructure (PKI) products. The lean and intelligent design of the complete product range makes it possible to integrate the most modern cryptography and PKI application into any IT system. cryptovision PKI products secure the IT infrastructures of diverse sectors, from private enterprise to government agencies. The consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems to the design of complete cross-platform cryptographic architectures. Since August 2021, cryptovision is part of Atos.

www.cryptovision.com

GEMALTO

Gemalto, a Thales company, is a global leader in digital security, bringing trust to an increasingly connected world. We design and deliver a wide range of products, software and services based on two core technologies: digital identification and data protection.Our solutions are used by more than 30,000 businesses and governments in 180 countries enabling them to deliver secure digital services for billions of individuals and things. Our technology is at the heart of modern life, from payment to enterprise security and the Internet of Things.We have built a unique portfolio of technology and expertise including physical and digital identity credentials, multiple methods of authentication – including biometrics – and IoT connectivity as well as data encryption and cloud service protection. Together, these technologies help organizations protect the entire digital service lifecycle from sign-up to sign-in and account deletion with data privacy managed throughout.Gemalto is part of the Thales group, a €19bn international organization with more than 80,000 employees in 68 countries worldwide.

HBPC

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

www.penzjegynyomda.hu

HID GLOBAL

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

www.hidglobal.com

MASKTECH

MaskTech is the leading independent provider of high secure system on chip designs, embedded ROM masked products, security middleware, certification and integration services focused on human credential applications. MTCOS – MaskTech Chip Operating System – is a high performance and high security operating system, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

MELZER

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.melzergmbh.com

MICROPROSS

Established in 1979, Microprossis the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Microprossis has proven expertise in the design of laboratory and manufacturing test tools which are all considered as references in their domains. These tools allow users to fully characterize and test the electrical and protocol performance of products such as smartcards and smartphones in design, conformance, and production. In 2015, National Instruments acquired Microprossis.

www.microprossis.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.

http://www.muehlbauer.de

OVD KINEGRAM

OVD Kinegram protect government documents and banknotes. More than 100 countries have placed their trust in the KINEGRAM® security device to protect their high security documents. OVD Kinegram is a Swiss company and a member of the German Kurz group. The company has accumulated over three decades of experience in the 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, secure-products and solutions as well as highest quality services which ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.

www.pwpw.pl

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

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

UNITED ACCESS

United Access is focused on secure, high-end smart card and RFID based solutions. We are acting as a security provider with a broad range of standard and integration components. United Access is the support partner for the Infineon smart card operating system SICRYPT. United Access provides secure sub-systems to various markets like public transport, road toll, logical access, logistics, parking systems, brand protection, physical access control and others.

www.unitedaccess.com

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.

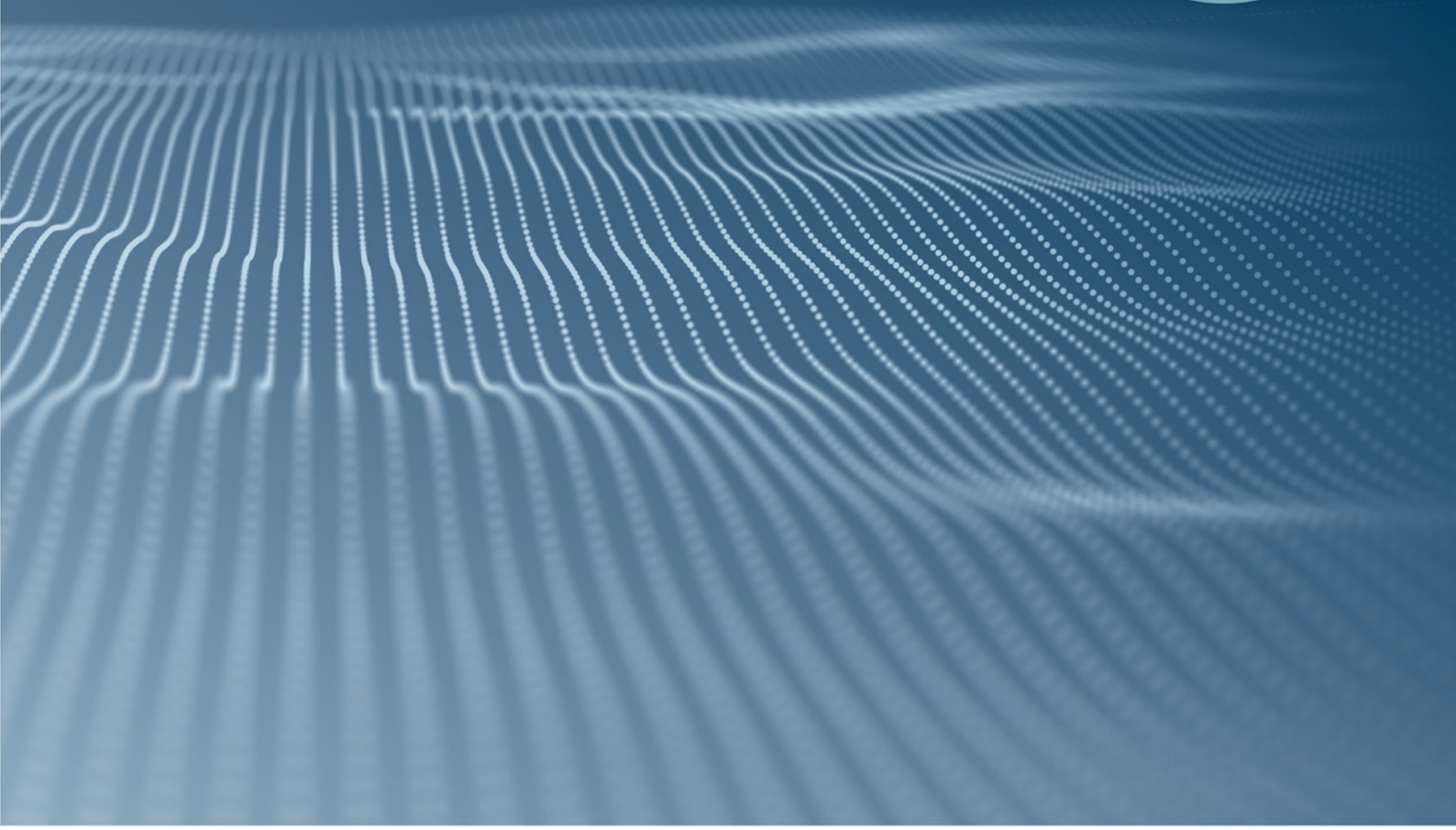
www.x-infotech.com

MASKTECH
DNA for ID solutions

MTCOS® – DNA for ID solutions

MTCOS®, MaskTech Card Operating System, protects more than 400 million eDocuments around the globe.
Like the coding system of DNA, MTCOS® secures the personal data of the document holder for an encrypted, wireless transmission and guarantees a unique and swift identification.

Find out more at **TRUSTECH E031**



MaskTech GmbH
Nordostpark 45
90411 Nuernberg · Germany

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

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

Common Criteria

WIBU SYSTEMS

Cybersecurity: Addressing the Global Challenge

A beacon for IT security innovations

A business enabler for all software and device makers

A guardian for all digital assets

Wibu-Systems and the House of IT Security support the local and international community for a more trustworthy, sustainable, and effective digital future.

Are you looking for thought leaders and inspiring partners to engage with?

Become a member of the IT Security Club

Are you looking for a rewarding career in IT security?

Send your application to Wibu-Systems

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

SECURITY
LICENSING
PERFECTION IN PROTECTION