NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

DECEMBER 2021 | #32

# The VAULT

# A NEW DIGITAL FUTURE?

## FEATURED ARTICLE

The challenges of changing travel habits
Infineon Technologies

## ALSO IN THIS ISSUE


Our eID solutions* are flexible, secure, certified. So you can do things just the way you want. Our Government ID experts and our global network of qualified partners will lead the way. Find out more on **cryptovision.com/eID**

*Java Card™ Applet Suite | Personalization | Middleware | Certificate Management

# Contents



Imprint

**THE VAULT ISSUE 32**
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: Markus Moesenbacher, Katharina Schuldt, Manal Ashraf, Daniel Hernández, Ajay Hanyalu, Katja Kienzel, Adam Ross, Klaus Schmeh, Oliver Winzenried
PHOTOS: INFINEON TECHNOLOGIES, ISTOCKPHOTO, KROWNE COMMUNICATIONS , MÜHLBAUER, CRYPTOVISION, PIXABAY, AUSTRIACARD, WIBU-SYSTEMS
EDITION: November 2021. 


REPÚBLICA
DE
MOÇAMBIQUE
PASSAPORTE
PASSPORT

# 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. The MB eVisa system is scheduled to go live in Autumn 2021. All these newly implemented solutions make the Southeast African country a pioneer in digital identification. ☒

Mühlbauer
High Tech International

Security is not a product, but one of the most valuable goods of a nation. The core of a holistic ID program is the constant capability to increase and optimize the integrity of the national identification scheme. Mühlbauer is strongly committed to providing reliable and secure government solutions for your citizens, thus creating trust and absolute confidence whilst meeting all your individual requirements.

**Mühlbauer – Your Reliable Partner for Your National ID Program**

**www.muehlbauer.de**

# *Bringing* about FRICTIONLESS financial *FREEDOM* with HASHWallet

By Manal Ashraf, TrustSEC – Daniel Hernández, eSignus

A successful collaboration between TrustSEC and CardLab brought to market a biometric card system that combined security and flexibility, thanks to the on-board microprocessors processing the biometric and non-biometric data directly on the card, without the need for a remote matching template. By leveraging their knowledge and experience of biometric smart cards in the ID, access and payment arena, the two companies, in cooperation with leading Spanish financial and crypto-security technology start-up, eSignus, have turned their attention to bringing digital transformation to hardware wallets.

Conceptualized in late 2019, HASHWallet disrupts the hardware wallet scenario with innovative and unmatched concepts that go beyond offline key storage, to envision 'frictionless financial freedom'.

## HASHWallet, the world's first non-programmable hardware wallet.

Usually, a system's firmware must be regularly upgraded to meet new protocols or support new currencies. All hardware wallets available in the market today must constantly update their firmware too. This can be a risky procedure, exposing opened ports to unwanted malicious actions.

The roots of the HASHWallet project go back to 2012, where the cofounders of eSignus worked on an R+D project based on PKI technology to avoid fraud in payment methods and online banking. In 2018 they developed HASHWallet from scratch, building prototypes and working with potential customers to solve the problems of security, usability, and adoption of hardware wallets.

From early conception, eSignus was determined to reinforce the HASHWallet's security by prohibiting any system core modification, ensuring that HASHWallet is completely hermetic. The engineers of eSignus have developed a simple, yet effective, system to support the market demand for an ever-increasing variety of cryptocurrencies; Introducing HOLa (HASHWallet Operation Language).

Instead of independently running procedures defined by each coin's protocol, HASHWallet interprets and executes securely signed grouped operations, built and sent, from an external source. HASHWallet only hosts the operation interpreter, for deriving wallets or signing any currency or token transactions, making HASHWallet not only able to support any cryptocurrency, but also community-driven and future-proofed.

## Disassembling HASHWallet: Security by design.

To reinforce the device's immune system (and thus reinforce the user's security), HASHWallet has been conceived based on the concept of security by design at both software and hardware levels.

HASHWallet features a 312x74 pixels, 105 PPI, low-consumption, 3.1-inch e-ink screen within its credit card form factor. This large display is not just a matter of aesthetics, but is the response to the


We have been very happy to work with CardLab and eSignus on an innovative hardware wallet in the shape of a convenient Smart Card to safeguard crypto-assets. I would also like to pay tribute to Fingerprints in Sweden and Infineon Technologies in Germany, for their contributions and positive collaboration. We are looking forward to more collaborations that will shape the future of financial services digital transformation

– Magdy Sharawy, CEO, TrustSEC

What You See Is What You Sign (WYSIWYS) property. A large screen allows users to verify that what they are signing on the device, matches what they intended. Thereby avoiding unwanted impersonations or tampering – commonly known as the 'man-in-the-middle' attack.

The card hardware is developed and manufactured by CardLab, a leading technology provider and manufacturer of all types of electronic Smart Cards and has been the project coordinator of the Horizon 2020 biometric card project for protection of critical infrastructure.

The card project has patented eight different technologies, all designed to increase card security to the highest level possible. eSignus Hardware HASHWallet has benefitted from these developments; including the RFID jammer patent which jams any attempts of malicious copying.

In conjunction with such powerful CardLab hardware, the system also needed an innovative COS to manage it. TrustSEC has introduced a special biometric version of their "SLCOS" smart card operating system, namely CardLab Bio OS that enables all hardware capabilities, and makes it very secure and easy for eSignus to implement HASHWallet smoothly. The master seed and any temporal private keys derived, never leave the Infineon SLE78 Secure Element while the Ambiq Apollo3 handles all the cryptographic processing. An NFC-chargeable 56mAh battery feeds the circuitry, as well as three colored LEDs used for indication purposes. The industry-leading FPC1321 T-Shape fingerprint reader ensures that only the device owner can sign transactions or perform any kind of operation.

## An innovative recovery system that provides the user with both security and comfort.

In the standard initialization process, HASHWallet splits the master seed into two hashed parts. These parts are only functional when put together, since it is impossible to determine the master seed with just one of them.

eSignus allows the user to store one of the hashed parts in their assigned eSignus Account and the other on a Recovery Card that comes paired with the HASHWallet, disseminating the risk of loss. The user simply connects to his eSignus Account, retrieves the recovery key from his Recovery Card, and instantly recover the account. This approach is easier-to-use and far more secure than writing down and storing the 24 words generated through the Bip 39 protocol. Nevertheless, 24 words mnemonic recovery system is also supported, and the users may create as many backups Recovery Cards as they want.

Bitcoin arrived in 2009 and gave us further choice in accessing digital financial freedom. But this specific digital financial freedom requires a high level of trust through secure transactions and interoperability. This lack of trust and security is a crucial element that the crypto sector suffers from after every reported case of loss and fraud. Observers in the crypto sector point to these elements as one of the reasons why crypto has not yet achieved the desired mass adoption the sector expected. HASHWallet is one contribution to secured financial freedom and a decentralized new world. ☒

# SECURING today's digital *LIFESTYLE solutions* gets EASIER with Infineon's SECORA™ *family*

By Markus Moesenbacher, Infineon Technologies

☐ Today, the amount of our lives spent in one digital scenario or another is growing exponentially. Be it paying, connecting, identifying or authentication and verifying – it is the times we live in. Such a massive digital presence requires not just secure software solutions, but hardware-based secure solutions to facilitate this new digital life.

Hardware-based secure solutions will facilitate such security measures, as increased regulation, tokenisation, encryption of data, remote erase features and highly robust multi-factor security mechanisms related to identification, authentication and authorisation – all to protect the safety of the underlying user credentials. These circumstances also encourage companies and organisations to take a data-centric approach to security, looking at the way this information has been transmitted to a company or organisation from a device and how it is subsequently managed and controlled.

Infineon is now delivering hardware-based security to fit with today's digital requirements through the introduction of their SECORA™ family. SECORA™ is Infineon's family of one-stop security solutions with integrated operating system (OS) providing a cost-efficient way to fast and agile implementations. It is based on a solid chip platform, which is highly secured and reliable, as well as easy to install and delivering best price-performance ratio.

## Introducing the SECORA™ family from Infineon

The SECORA™ family incorporates Infineon's unique SOLID FLASH™ microcontroller family, providing contactless transaction speeds and superior performance for today's single- and multi-application projects. Furthermore, Infineon's innovative Coil on Module (CoM) chip package increases production efficiency and general robustness of dual-interface cards. At the same time, the very small antenna design supports novel contactless payment factors, such as smart watches with payment functionality.

## There are four SECORA™ security solutions subcategories:

**SECORA™ Pay** – Flexible solution providing a complete portfolio for everything from contact cards to smart payment accessories, combined with the latest EMV-ready applications, to meet regional market requirements.

**SECORA™ Connect** – System solution for smart wearables to provide contactless secured payment, ticketing or access applications via Near Field Communication (NFC).

**SECORA™ ID** – Ready-to-go Java Card™ solution optimized for all electronic identification (eID) applications, allowing maximized customization for local needs.

**SECORA™ Blockchain** – Fast, easy-to-use Java Card™ solution, supporting best-in-class security for blockchain system implementation.

## SECORA™ Pay security solutions offers a streamlined migration path to the EMV standard

One way to address the security issues in a digital lifestyle is to employ hardware-based security via a lightweight SE, as provided by Infineon's Java Card based payment solution portfolio SECORA™ Pay. This innovative suite of payment solutions (serialised S, X, and W), provides state-of-the-art contact and dual-interface EMV security controllers with the latest EMV applets, allowing all cards, accessories, form factors, and non-connected wearable devices to transform themselves into payment instruments, whilst providing the flexibility needed to meet regional market requirements.

SECORA™ Pay S is a ready-to-go, off-the-shelf, optimized EMV solution with major global payment scheme reference approvals from VISA & MasterCard and personalization scripting support. Additionally, SECORA™ Pay X is a flexible enablement platform

to support multi-application payment cards, supporting domestic payment schemes and project-specific requirements with the possibility to integrate transit applications based on the CIPURSE™ open standard.

SECORA™ Pay W solution portfolio includes not only the EMV chip card OS and payment applets, but also offers innovative packaging options to address the market need to realise non-connected, field-powered wearable devices, or so- called "Payment Accessories".

## Different contactless payment form factors will benefit from SECORA™ Connect

The overwhelming success of contactless and digital payment cards is driving the demand for wearable payments in a variety of different form factors. They are becoming increasingly popular by adding additional functions, despite severe space and power limitations. When equipped with NFC capabilities, a wearable device can allow the user to pay at a store, access a mass transport system or their own office building.

Multi-function connected wearable devices have now had their mainstream breakthrough in terms of the number of units shipped. The more things being integrated, the bigger the need for standardisation to enable the integration. At the same time, security requirements will grow, and Infineon expects that the most connected devices will continue to use hardware-based security.

SECORA™ Connect is Infineon's solution for connected wearables based on an NFC boosted Secure Element design for connected wearables, in ultra-small integrated packages with lowest power consumption. It is a system solution designed for being embedded into smart wearables to provide contactless secured payment, transportation ticketing and other applications via Near Field Communication (NFC).

SECORA™ Connect is a complete turnkey solution that enables the user to securely provision, store, select and use multiple credentials such as payment card, transport ticket etc., turning the de-facto wearable or IoT device into a powerful and versatile wallet. The solution allows smart wearables system designers with no security or antenna design experience, to seamlessly integrate a very compact, ultra-low power consuming solution for various NFC based applications.

By implementing SECORA™ Connect, device makers can achieve ultra-low power consumption and realize smallest form factors, while still meeting the rising security and contactless requirements of the payment industry.

## SECORA™ ID accelerates regional ID Integration – whatever the requirements

SECORA™ ID is a new member of Infineon's SECORA™ family based on SECORA ™ Pay. It supports, in addition to SECORA™ Pay, all the features necessary to serve typical ID use cases. Typical ID applications are standardized to a high extent.

Identification is mostly based on the ICAO 9303, which defines the MRTD (machine readable travel document). This standard, primarily developed for electronic passports (ePP), is also used for National electronic ID (NeID) cards and a variation for the electronic Driving License (eDL). Authentication needed for applications such as NeID or electronic health cards is predominately based on ISO and CEN (European Committee for Standardization) standards, as well as newer standards such as FIDO.

However, every country has its own system and solution based on national requirements and applications. It is these scenarios that demonstrate the benefits from developing with SECORA™ ID. The Java Card™ solution provides a highly flexible portfolio to support various use cases and interfaces. The open platform allows the user to implement their own applet through the use of sophisticated tools from Infineon. Additionally, the customer can use a ready-to-go solution from Infineon, comprising of applets for eGovernment applications.

Performance and security are key for governmental applications. The product is secured by the SLC 52 security controller based on high-speed 100MHz 16bit technology, equipped with state-of-the-art security features. Both the hardware and SECORA™ ID are certified on highest security levels CC EAL 6+ and EMVCo.


SECORA™ ID also has several delivery options, including wafer, dual interface based on CoM (Coil on module) inductive coupling technology or contactless modules. This "ready to use flexibility" can accelerate the customer's process to realize his final product.

## SECORA™ Blockchain provides secured access to the blockchain

Meanwhile the distributed ledger technology, Blockchain, is having a significant impact on many industry segments. Beside Fintech, blockchain is relevant for logistics, automotive applications, energy settlement, brand protection, asset and contract management.

A blockchain provides inherent security and is tamper resistant. However, adding new valid data to the blockchain is a sensitive process, because it uses a private key. It is essential to store the private key in a secured area, which is realized by SECORA™ Blockchain. The security controller provides several mechanisms and sensors which are resistant against several security attacks, such as power analysis, micro probing, laser fault injection and others. As a solution, SECORA™ Blockchain provides a secured access to the blockchain itself.

## Brand protection is a good example for demonstrating the benefits of blockchain usage.

For example, manufacturers of limited-edition sneakers need to prove that they are the genuine article. Starting at the manufacturing process, through the implementation of a SECORA™ Blockchain chip into the sneaker, and then linking it to the blockchain, will establish the legitimacy of the sneaker. The chip can then be accessed by an NFC interface to "connect" it to the corresponding blockchain entry. The entry of the sneaker in the blockchain can be used for the distribution process until it reaches the retailer. Once the sneaker is sold, the consumer can prove the legitimacy of the sneaker and its corresponding value.

The world is changing rapidly. Connectivity and digitalization make users' lives easier, but they also increase the need to secure identities and personal information. The SECORA™ security solutions from Infineon will help those manufacturers and developers facilitating this change from an analog to a digital lifestyle, and ensure that their user's data and identification remain safe and secure in this new world. ☒

# FIDO: A *user's* best *FRIEND* for a *simple* and SECURE authentication

By Ajay Hanyalu, Infineon Technologies

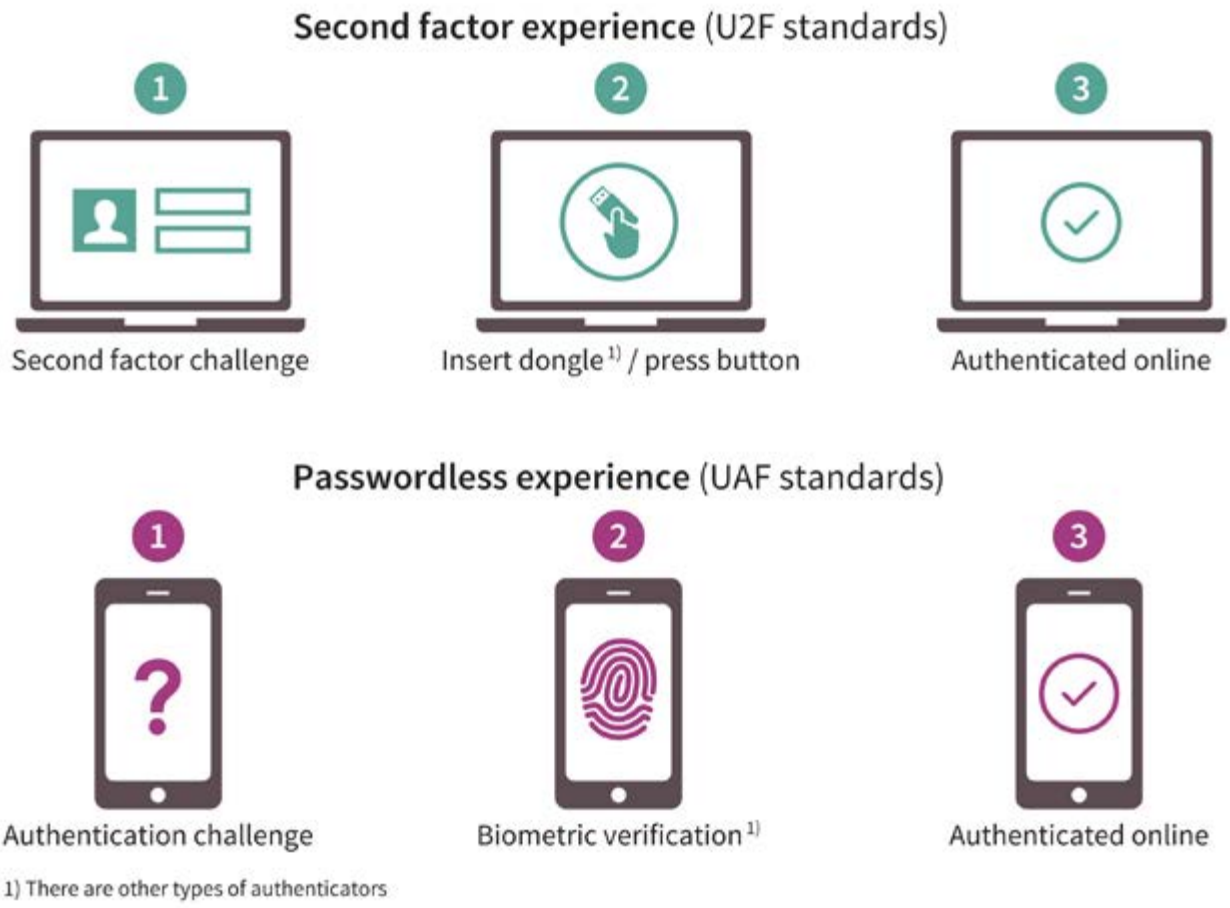
☐ Fun fact: Did you know that Abraham Lincoln named his dog Fido, for the reason that in Latin it means "to trust or confide in"?

Since the advent of internet in the late 1980s, we have now reached an age where finding something, or someone, without an online presence is almost impossible. Today, the extent of our dependence on the internet is undeniably significant. And passwords are our first line of defense in securing our existence, along with our Identity, in the digital world. But is this enough? These days, every user has up to 80 online accounts with reused or weak passwords. Which is in fact the prime reason for most data breaches and identity thefts. The World Economic Forum assesses that cybercrime costs the global economy about $2.9 million every minute, out of which about 80% of the attacks are targeted towards passwords.

## FIDO: A user's best friend for a simple and secure authentication

FIDO stands for Fast Identity Online and is a specification published by FIDO Alliance - an open industry association comprising of 250+ tech and financial companies as its members. Its mission is to create easy-to-use, but reliable and strong authentication standards, to reduce the world's over-reliance on passwords.

The FIDO Universal Authentication Framework (UAF) standard is mainly focused on 'password-less' authentication, with biometrics as its trust anchor. Whereas, FIDO Universal 2nd Factor (U2F) standard enables second factor experience, by allowing online services to augment their existing password




infrastructure with a strong second factor using smart cards, security keys and tokens implemented on security controllers. FIDO2 specification includes Web Authentication (WebAuthn) which was later adopted by World Wide Web Consortium (W3C), and Client to Authenticator Protocol 2 (CTAP2), which enables a client device to authenticate a FIDO token via NFC, Bluetooth or USB interface.

There are two types of FIDO authenticators. On-device (or Platform) authenticators in the form of TPMs and SE are embedded inside a computer or smartphone and therefore restricted for usage on one device only. On the contrary, External (or Roaming) authenticators, such as security keys and smart cards, are decoupled tokens which can be used by users on multiple devices.

FIDO protocol uses public key cryptography for its authentication protocols. A unique key pair is generated for each registration to an online service. While the public key is transmitted to the service provider for registration, the private key never leaves the authenticator and is therefore always kept secure. Each login authentication to a service is proved by digitally signing a challenge data sent by a service provider, with its corresponding private key on the user's device or authenticator. The signature is then verified using the registered public key available with the service provider, thereby accomplishing authentication. Access to the private key (for signing) is restricted and has to be unlocked by the user locally on the device, by performing a user-friendly and secure action such as swiping a finger, entering a PIN, inserting a second factor device or pressing a button. FIDO protocols are also designed to protect user privacy by ensuring that no such data is communicated that can be used to track the user across services. Thereby ensuring security, convenience and privacy. In addition, it also facilitates easy scalability, as FIDO is already supported by leading browsers and operating systems on billions of devices that people use every day. There is absolutely no need for any middleware or additional software for FIDO, thereby making it easy for the service providers to integrate and deploy in their infrastructure.

> *Infineon's FIDO solution is the latest addition to the SECORA™ ID portfolio, which is implemented on state-of-the-art EAL6+ high certified Java Card™ operating system and security controller.*

Although, usage of FIDO in consumer markets for personal and in enterprise environment for managed services is apparent, its usage in eGov applications has distinct benefits. FIDO, when coupled with an electronic Identity Document (eID), can be used by citizens to easily authenticate themselves to government portals for availing services. This use-case has already been adopted in many countries. The official portal of South Korea's Government24 provides over 90000 services using FIDO to over 14 million registered users as of March 2020. Another project is "Taiwan FidO" – which was deployed in 2019 by Taiwan's Ministry of Interior (MoI) for its employees and citizens to access the Ministry's intranet and e-government services respectively. It includes services such as eTax filing, access to MyData service, eVoting etc., and is expected to reach 3 million users by the end of 2022. One more example comes from the UK's National Health Service (NHS), which has enabled citizens to login via FIDO to the NHS mobile app and web portal, to book appointments, order repeat prescriptions and access resources. A few other deployments include Thailand's Electronic Transactions Development Agency, Canadian Digital Service (CDS), Sweden's eduID, Czech Republic's CZ.NIC and many more.

Infineon's FIDO solution is the latest addition to the SECORA™ ID portfolio, which is implemented on state-of-the-art EAL6+ high certified Java Card™ operating system and security controller. With FIDO alliance's certification as a roaming authenticator, it supports FIDO's CTAP2 protocol enabling 2nd and multi-factor authentications via NFC interface. A versatile offering available as a standalone and in combination with eMRTD applet, it will cater to all use-cases such as personal, enterprise and eGov applications.

Let's begin our journey in the world secured by FIDO! ☒

# The CHALLENGES of *changing* travel *HABITS*

By Katja Kienzl, Infineon Technologies

☐ Have you ever walked through a city centre on a New Year's Day? It can be a strange and surreal experience. A once bustling metropolis now dead, open and empty. New Year's Day used to be one of the few days you could experience this. Until COVID 19 arrived.

The pandemic turned every day into New Year's Day – for month after month. In many cities, the streets fell completely silent. Public-transport networks ran skeleton services to take essential workers to and from their jobs, and the sight of empty buses waiting at empty bus stops for passengers who never came, was an eerie reminder of just how strange life had become.

As pandemic restrictions lift, we are travelling again. Although working from home has been a challenge for many, a lot of work is still getting done. People are questioning the need for, and the environmental impact of, the daily commute. Must we travel to an office to work on a laptop, answer calls and email, or take part in online meetings? No. Should we go to the office for face-to-face discussions, group problem-solving, and ideation? Definitely. And so, people are travelling again, but in different ways. They're walking further, renting e-bikes and e-scooters as a substitute for short bus and subway trips, and incorporating other forms of transport where they can.

## Travel in a multimodal way

Public transport authorities (PTAs) and public transport operators (PTOs) know that to rebuild their ridership, they need to make it as easy as possible for passengers to travel in this multimodal way, helping them to shift from bike to bus, to tram to boat and back again without thinking. Anything that slows them down just delays the moment at which public confidence is restored and ridership numbers return to normal.

One of the most effective things that PTOs and PTAs can do to help, is to make paying for travel simple.

They can do this by creating or supporting, a single, well secured, sustainable ticketing system that enables travel on as many different services as possible in their region. A system which is flexible enough to support innovative pricing strategies, such as zoning, time-of-day discounts and easy transitions between travel modes. The tickets should also work on any user-owned hardware platforms, be it a dedicated travel-card, smart watch, phone or future wearable device. And given the pandemic, it is essential that future ticketing solutions are entirely contactless.

## It's all about control of your transportation system

The pandemic has taught PTOs and PTAs that they need more control over their transport systems, and the data generated about how they are used. Some PTOs and PTAs have been unable to quickly adjust their travel offerings to the reality of the pandemic, because their systems are run by third parties under inflexible outsourcing contracts that use proprietary solutions. Others have found that the data their services generate, such as ridership statistics, is not as easily available to them as they would like, because it is not being processed inhouse. Openness, flexibility and control are the new watchwords of post-pandemic travel ticketing.

This kind of ticket, which supports many different modes of transport (e.g., scooter, train, tram) and can exist on many different hardware platforms (e.g., smartcards, mobile phones, wearable devices) at once is desirable, but challenging to achieve. There are several challenges that must be overcome to make it possible.

## Challenge 1 - Cost of solution against revenue generated

The first is matching the cost of the solution to the revenue it is generating and protecting. Implementing the most secure digital ticket possible, and the highly secure infrastructure needed to support it, won't make financial sense if it only enables $1 journeys. Fortunately, a variety of ticketing solutions are available to enable PTOs and PTAs to match ticketing costs to the revenue they generate.

## Challenge 2 – Enabling multiplatform operations

The second challenge is enabling multiplatform operations, so that a ticket can be read on multiple devices during a journey. This enables users to choose the hardware platform they prefer for ticketing. It would also allow users to buy a ticket on a mobile phone while still in the office, and then use a smartcard, registered to the same account, while they travel in order to protect the phone from damage or loss.

## Challenge 3 – Sustainability of solution

The third challenge is sustainability, which in ticketing terms, means allowing the underlying IT infrastructure that is designed to last for 15 to 30 years. Even if the ticketing terminals only last for ten and the ticket-bearing devices for five. This demands a forward-thinking approach to the IT architecture, the use of open standards to ease interoperability, rigorous attention to the ownership of, and access to, data flows, and as much transparency as possible in the design.

## Challenge 4 – From legacy to state-of-the-art – seamlessly

And the fourth challenge is simply to make all this happen, and to make it possible to migrate from legacy systems to new forms of ticketing without service interruptions.

## The emergence of open standards for ticketing solutions

The good news is that the ticketing industry understands that developing and completing open standards, and undertaking further standardization of the infrastructure and guidelines for ticketing solutions, enables greater interoperability and avoids supplier lock-in. The industry also knows that when it specifies a major piece of infrastructure, such as a ticketing terminal, it should support current standards, and is designed to support future open standards as well. Some call this approach 'adversarial interoperability', for its ability to rebalance the relationship between customer and supplier.

Acceptance of the EMV standard for ticketing payments is another way to attract new ridership groups in transportation.

> *The ticketing industry understands that developing and completing open standards, and undertaking further standardization of the infrastructure and guidelines for ticketing solutions, enables greater interoperability and avoids supplier lock-in.*

EMV is now being increasingly used to enable 'open loop' payments in which a passenger taps their card on an NFC reader at the start of that journey to pay for a journey.

## The OSPT Alliance

As is often the case where a market would grow more quickly if there was greater collaboration, two standards bodies have emerged to promote open ticketing arrangements and avoid market fragmentation. The OSPT Alliance (Open Standard for Public Transport) promotes CIPURSE as an open platform for transport ticketing, built on top of several ISO-standard enabling technologies. CIPURSE is media independent, but supports contactless cards, mobile phones and wearables. This makes it easy to adopt now and to support new ticketing hardware as it becomes available.

## Calypso Networks Association

The second standards body is the Calypso Networks Association, which promotes an open, efficiently secured ticketing standard already in use in more than 25 countries and more than 170 cities globally. It has been designed by transport operators with openness and longevity in mind.

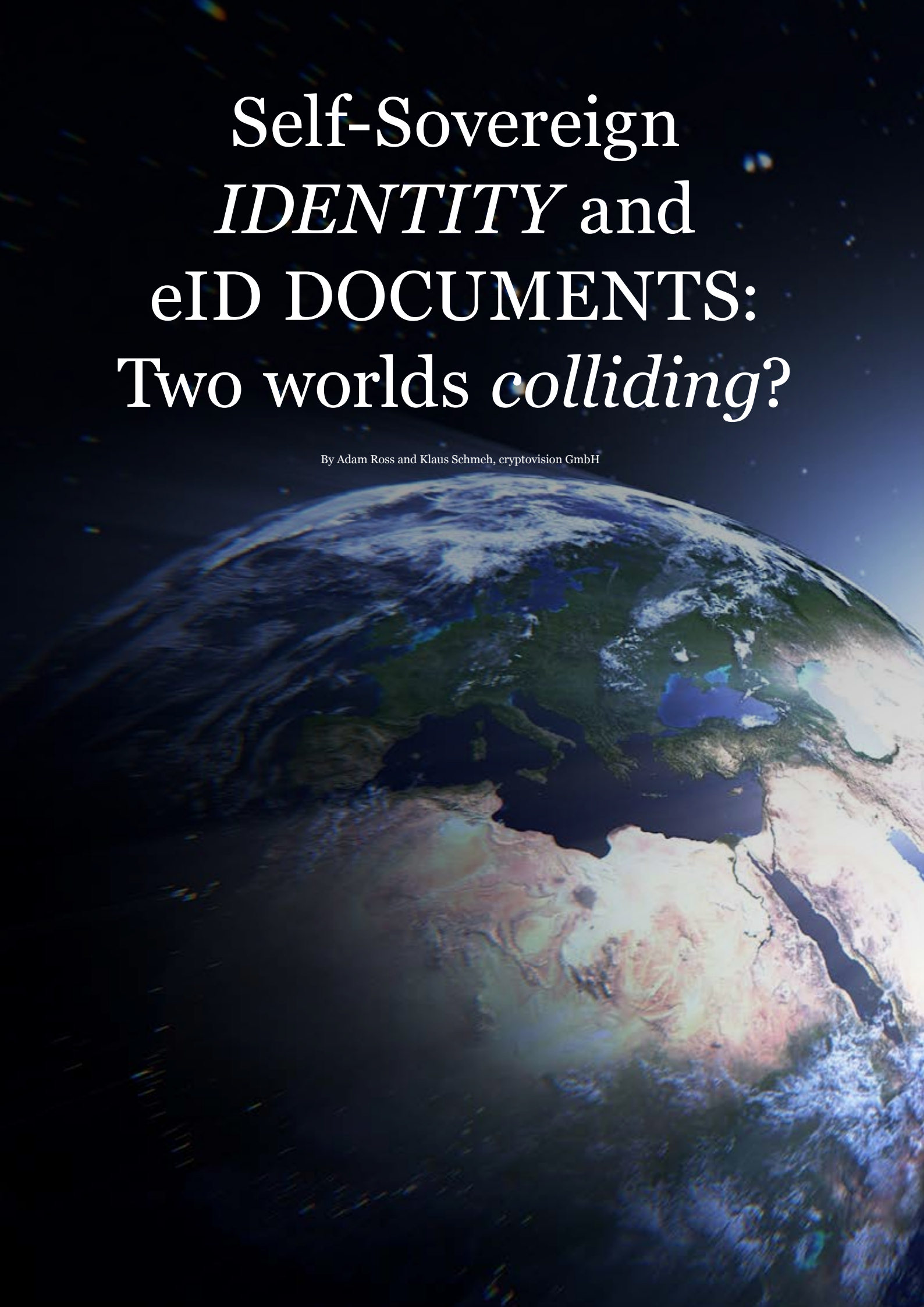
The OSPT Alliance and the Calypso Networks Association are now collaborating to drive global adoption of open standards in transport ticketing, and plan to converge the CIPURSE and Calypso standards. This should provide greater openness, simplify the integration options for transport operators, harmonize technical specifications, and encourage operators to innovate in ways that add more value than is possible through ticketing arrangements.

## Mobility as a service in a post-pandemic world

Travel in the post-pandemic world must be made easy if ridership is to return to pre-pandemic levels. Consumers want mobility as a service in which a single account, managed through one app and implemented on multiple types of hardware, from smart cards to wearables, enables seamless travel from door to door, across the largest possible region, using any type of transport. Infineon has many of the building blocks to make this possible and highly secure experience with the key open standards, and a track record of helping PTOs and PTAs implement ticketing systems that are evolving towards this ideal. The rest of the journey is up to you. ☒

# Self-Sovereign *IDENTITY* and eID DOCUMENTS: Two worlds *colliding*?

By Adam Ross and Klaus Schmeh, cryptovision GmbH



> *The combination of SSI and eID documents has great potential, from which both technologies can benefit.*
> *– Ben Drisch, cryptovision*

A Self-Sovereign Identity (SSI) gives a person sovereignty over their identity data. Every individual can decide to whom his or her name, age, university degrees or purchase records are revealed, and who vouches for the accuracy of this information. At first view, the SSI approach is at odds with the electronic identity documents used in many states, as in the latter model it's the state that has sovereignty over its citizens' identity data. On closer inspection, however, SSI and electronic identity documents can complement and even benefit from each other.

Identity management traditionally followed a centralized approach, where a state, for example, managed the identities of its citizens. In the last few years, globally operating, technology-driven and cross-industry oriented platforms, successfully pushed the market for digital identity management systems, based on an already significant customer base. When it comes to data protection, these approaches meant that an individual had to trust a state authority, an employer, or a global technology platform. This meant that users needed to trust the major software suppliers, social media operators, and other parties that have an interest in using personal data for commercial interests.

## The individual strikes back

There is, however, a technology that enables the individual to strike back: Self-Sovereign Identity (SSI). In SSI environments, it's the user who generates a digital identity and who controls it – typically with a software called "wallet". With their wallet, a user can add the identity data they want and delete the pieces of information they don't want to be included any more. The data that a user chooses, may be authenticated by a third party with a digital signature or a blockchain entry. In addition, the wallet allows the individual to grant access to their identity information, based on their personal requirements.

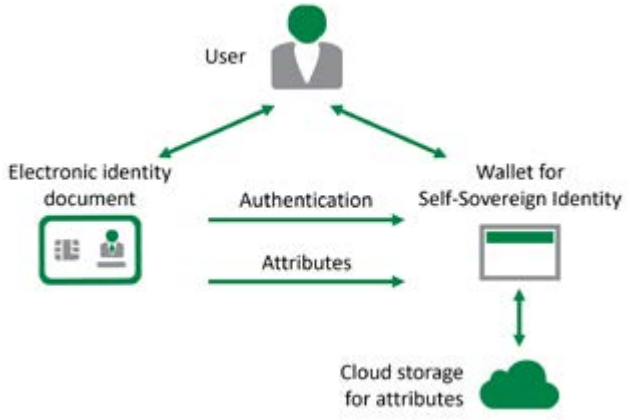
As SSI is still a new topic, current activities in this area are either experimental in nature, or concerned with standardization. For instance, a working group of the European Union is currently exploring the possibilities of SSI within the European Blockchain Services Infrastructure (EBSI). One of their goals is to create an eIDAS-compatible "European Self-Sovereign Identity Framework" (ESSIF). Among other things, ESSIF specifies a data structure, called a "decentralized identifier" (DID), which can be used by a wallet for storing identity data.

Another European research activity, IDunion, is developing an open SSI infrastructure that is meant to be used by individuals all over the world. IDunion is operated by a consortium of mainly German companies and organisations. GAIA-X, a project operated by the German Federal Ministry for Economy and Energy (Bundesministerium für Wirtschaft Und Energie - BMWi), is aiming to build a secure, cloud-based data infrastructure for Europe. This infrastructure, which is independent from US suppliers and compliant with European data protection regulations, includes an SSI-type identity management. And then, there's Modular Open Source Identity Platform (MOSIP) a project that aims to establish a foundational ID that can then be used to access a wide variety of government and private services, via a progressive open source digital identity system that nations can reuse freely.

One of the first projects that puts the SSI approach into practice is the "ID Wallet", a smartphone app launched by the German government (German ID Wallet – page 25).

## Self-sovereign identity meets electronic identity

Contrary to these SSI activities, the national electronic identity documents used in many states (e.g., Belgium, Estonia, Finland, Germany, Spain, Ghana, and Nigeria) follow the traditional, centralized identity management approach. Attributes, such as the name, the birth date, or the fingerprint, are managed by the issuing authority. The user has only very limited possibilities to decide which information is stored on their document and the individual or institution who will verify the correctness of the data.




*Source: cryptovision*

*An eID document (left) may complement and support an SSI wallet (right). It may also serve as an authentication means for cloud storage connected to an SSI wallet.*

Despite SSI and eID documents taking a different approach to similar goals, they are not necessarily opposites. Ben Drisch, cybersecurity specialist at cryptovision, believes that the two technologies can even profit from each other. "The eID document is an ideal means for the user to authenticate against the wallet," says Drisch. "It's more secure and more convenient than a password-based solution." If a wallet is connected to cloud storage, which might often be the case, the identity document can be used for access protection, too.

In addition, an eID document can contribute attributes to a self-managed identity. For example, the document holder might want to take data, such as the name, the date of birth, or health information from their eID card and include this information in their SSI wallet. Says Ben Drisch, "This means, technically speaking, that a user is capable of transferring data from the Logical Data Structure of their eID document to a decentralized identifier." As the Logical Data Structure card is digitally signed by the issuing state, a proof of authenticity is automatically present in the DID represented as a verifiable credential.

These decentralized identifiers and verifiable claims provide censorship and tamper-resistant means, for citizens to give permission for validation of specific attributes of their identity data, while ensuring that other aspects of their identity remain private.

"All in all, the combination of SSI and eID documents has great potential, from which both technologies can benefit," says Ben Drisch. Whether this potential will be seized, certainly depends on the states that issue eID documents. If these states are willing to provide their citizens the possibility to manage their digital identities themselves, we might see powerful SSI schemes cooperating with eID-document systems in the future. If, on the other hand, governments don't support the SSI concept, it will be difficult to establish SSI-eID cooperation against their wills. The current EU activities suggest that at least some governments welcome SSI. ☒

## German ID Wallet: A Promising Technology with Teething Trouble

With the "ID Wallet" (a smartphone app) the German government launched one of the world's first SSI application pilots. The purpose of the ID Wallet is to store identity data of all kinds to allow the user to manage and share it.

As the first major application of the ID Wallet, the German Ministry of Transport together with the Federal Motor Vehicle Agency (Kraftfahrt-Bundesamt) and the Federal Printing Authority (Bundesdruckerei) created a digital driving licence. This virtual document, which can be used by every German citizen who has the permission to drive, simplifies car rental and car sharing. It is planned that the digital driving licence will completely replace the physical document used in Germany so far.

The first version of the ID Wallet, introduced in September 2021, soon became a victim of its success. The high demand for the new app led to the server infrastructure being heavily overloaded. In addition, experts found potential security holes allowing for data and identity theft. As a reaction, the ID Wallet app was withdrawn from the app stores after only one week.

These problems can be regarded as the usual teething trouble every new technology encounters. It is expected that the server infrastructure will be extended and the security weaknesses fixed within a few weeks. All in all, the ID Wallet and the digital driving licence are generally seen as promising innovations that might lay the foundation for other SSI projects to come

# The NEW *AGE* – *digital* without CARDS?

By AUSTRIACARD

☐ Digital transformation is a condition that determines the operation, and consequently, the success of an organization. It is a fact that the recent pandemic accelerated this digital transformation, a development which, of course, will directly affect the global business network.

Similar developments have been observed by AUSTRIACARD in the banking sector. The only difference is that traditional banking cards are still considered essential items in the customer's wallet. Specifically, we have noticed that people today are placing an increasing amount of trust in card payment transactions – especially contactless payments. Wearables such as wristbands, are becoming more prevalent as a means of payment – especially favoured by parents. Wearables enable secure and seamless payment for children, allowing parents to control and track the overall available budget. This new payment process had never been an option for anyone, a few years ago.

AUSTRIACARD's micro tag is the core of our payment product portfolio. It represents a fully-fledged credit or debit card and is certified according to VISA and Mastercard specifications. Such non-card form factor products cannot be inserted into POS terminals or ATMs, but conveniently use the contactless NFC interface that customers worldwide are familiar with. It is fully customizable and each tag itself can be used with, and in, different types of wearables.

AUSTRIACARD was among the first companies to provide payment chip cards with an operating system that had been developed in-house. The operating system of the embedded chip is the heart of a smart card, guaranteeing the highest level of security. Our native operating system, ACOS, has since been successfully implemented not only for payment applications, but also for transportation and tachograph card schemes/ applications/profiles. Our latest product line, ACOS-ID, is currently powering the security of modern ID & Government programs.

AUSTRIACARD's long experience in secure payment solutions has led us to the development of an integrated digital payment solution, creating a real value for the end-user. It facilitates payments from a consumer's card account, over a variety of payment channels and across numerous use cases. We are focusing on building a digital product proposition which, when delivered to a consumer, creates a seamless multi-channel payment experience under a harmonized 'look-and-feel' – irrespective of a payment use case. Our current proposition encompasses solutions for POI, online, and P2P channels that are supported by tokenization services provided by various payment schemes and enhanced by a variety of added-value services – all available from one source, and delivered to a payment card issuer within a single wallet application framework by AUSTRIACARD.

Combining our knowledge in the field of payment and identification cards and the security standards applied in both segments, we have added a digital on-boarding solution to our portfolio. Digital on-boarding of a new customer becomes a unique user experience. By applying true customer-centric design methods, along with e-IDAS certificates, the process is as easy as possible for the customer, reducing the effort required to apply and sign up. Moreover, our customers can leverage data-driven insights to access more personalized recommendations for products and services.

## Digital without cards?

At AUSTRIACARD, we believe that cards are an integral part of digital transformation and our digital future. For many years to come, cards will still be one of the most adopted and secure ways for payment and identification, coexisting with parallel methods and digital solutions. Times are changing, and as a part of a global and interconnected world, AUSTRIACARD is using its years of experience and knowledge in digital security, and is incorporating and conveying them into new products, for an ever-evolving world.

At AUSTRIACARD we're looking forward to the future – for both physical cards and the digital frontier. ☒

# Wibu-Systems' IT SECURITY Club – Where *INNOVATION meets* community

By Oliver Winzenried, Wibu-Systems AG

Ever since it was first imagined as one of Europe's original model cities and the ideal of a visionary community come to life in bricks and mortar, Karlsruhe has been a hotbed of progress and innovation in the heart of Europe. Today's Karlsruhe is home to more than 4,000 IT enterprises, making the city one of the world's leaders in terms of IT competence per square kilometer.

Located in the Rhine valley, Europe's first super-highway for commerce and ideas, the city and the many leading centers of industry nearby, host countless businesses that are being transformed by, or are themselves powering, the digital revolution. Economic success in every sector of industry now depends on their ability to put new digital capabilities, from artificial intelligence to the connected infrastructures of Industry 4.0, to commercial use – safely and securely. IT security has become paramount, and Karlsruhe is again at the forefront of the field.

With the multitude and variety of threats in the digital world, unity in diversity is the key: Different resources, competences, and capabilities need to converge to fight a threat whose nature and origin seems to change by the hour. The House of IT Security is designed to provide that unity, by bundling the many IT security skills and resources from the region in one physical space under one physical roof: From start-up incubators to deep-rooted businesses and research institutes.

As the House of IT Security brings together the rich experience and proven competencies of the established specialists and original pioneers of the industry with the innovative spark and energy of young startups, all key players in IT security research (including the Karlsruhe Institute of Technology KIT, the Karlsruhe IT Security Initiative KA-IT-SI, and the Research Center for Information Security FZI) and business expect the House of IT Security to excel at its mission:


- To combine academic excellence with enterprising minds to boost IT security research and practice.
- To act as an amplifier for the agility and energy of growing start-ups.
- To attract international companies pursuing IT security projects and academic and commercial partnerships to Karlsruhe.
- To generate new jobs and revenue in the region.
- To become a physical beacon of IT security.

Almost 5,500 square meters of the House of IT Security are earmarked for young businesses, providing an affordable home for IT security startups setting up shop in Karlsruhe or coming from specialized local incubators like the Cyberforum or StartUpSecure of the Competence Center for Applied Security Technology (KASTEL) at the Karlsruhe Institute of Technology. With ready access to the office space they need to grow and a network of commercial and academic champions right on their doorstep, they can concentrate on their core mission: Finding new solutions to the challenges of tomorrow and turning their ideas into profitable businesses.

In its concept and its physical architecture, the House of IT Security is designed for cross-fertilization. It provides ample space to meet and share, with laboratory and training facilities and co-working spaces that will host regular cooperation ventures and project activities, and with short-term leases available to give enterprises from other fields a proverbial foot in the door in the unique IT security ecosystem of Karlsruhe.

The House of IT Security also plays host to the IT Security Club, a club that is more than a co-working space. Described as a 'unique experiment in community building', it is a space dedicated to one of the most pressing issues of our time – IT security – designed

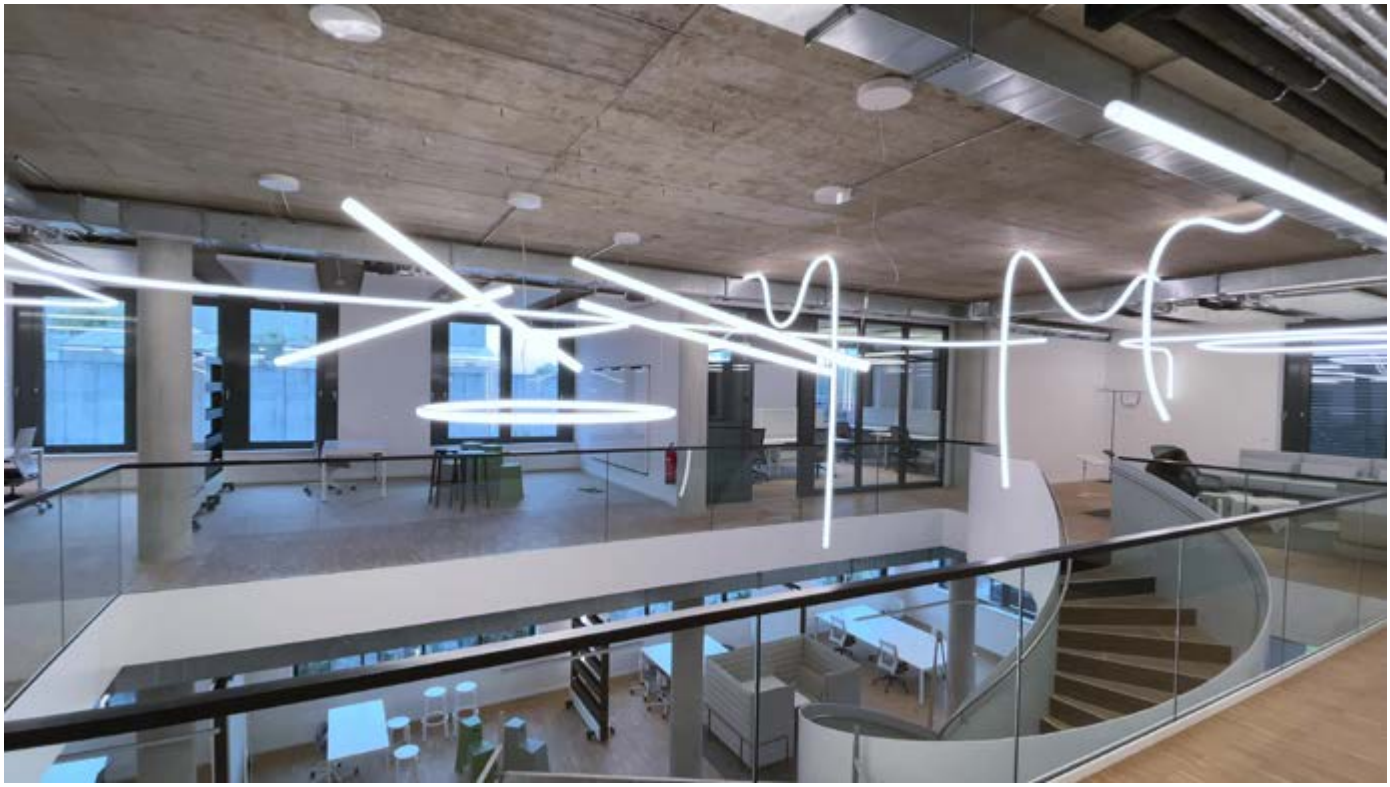
to spark creativity with its exceptional blend of institutional and commercial tenants and an agile group of IT security professionals in the Club.

The members of the IT Security Club enjoy access to like-minded professionals, top-class facilities, and an environment built to inspire commercial ambition and professional comradeship, with a range of membership packages and options for short or long-term participation in the creative atmosphere of the House of IT Security.

"The IT Security Club offers the perfect working opportunities for collaboration and confidential work in a building with excellent infrastructure and sustainable and sophisticated building technology", says Natalie Wieland, one of the two IT Security Club Managing Directors.

The IT Security Club was designed to wow both its members and their guests: The entire site is equipped with top class infrastructure and facilities, including modern building automation services and a decidedly eco-friendly architecture. This includes the indispensable IT infrastructure for successful work, like redundant fiber-optic connections, modern workstations, or specialized IT security labs, as well as the amenities that make working and staying at the IT Security Club a thoroughly enjoyable experience, including a well-stocked kitchen and bar facilities, smartly appointed work and community spaces, and attractive areas for meetings and representative work.

But please don't imagine that the IT Security Club is just a working space hub. "The IT Security Club is not your standard co-working space," says Elke Winzenried, IT Security Club Managing Director. "It is unique in that it is focused on IT security innovations in conjunction with innovation managers and project support who help the members do joint research projects with public funding". This fact alone should demonstrate how seriously Wibu-Systems is taking the idea of an IT Security Club.



In IT security, privacy and confidentiality are paramount, and the facilities are designed with care to reflect this commitment: Secure access controls and a careful layout of the premises with flexible private-public spaces and clever partitioning mean that members of the IT Security Club are safe in the knowledge that what they want to keep confidential will stay confidential, without hindering the spirit of community and free and easy communication with their peers.

With a world-leading IT security, protection, and licensing specialist next door and high-profile institutions, entrepreneurs, and researchers among the long-term tenants, the IT Security Club promises to be a hothouse for talent and ideas.

Joining the IT Security Club opens up a world of opportunity for aspiring entrepreneurs, innovative researchers, and all actors with a real stake in making the digital world secure. To give life to a dynamic and diverse community, the IT Security Club offers a comprehensive range of membership options, with monthly and yearly membership fees to match any budget.

To discover which of the many membership packages match your needs and for a private and confidential offer, please contact The IT Security Club via email at itsc@itsec.house. ☒

IT Security CLUB

*Use the QR code to watch a video on the IT Security Club*

# SILICON TRUST DIRECTORY 2021

## 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**

# HIGH SECURITY IDENTITY SOLUTIONS

BY AUSTRIACARD


AUSTRIACARD

Member of AUSTRIACARD HOLDINGS

## YOUR PARTNER OF CHOICE FOR ID

austriacard.com

## 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**

### 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, Micropross is the leading company in the supply of test and personalization solutions for the business of RFID, smartcard, and Near Field Communication (NFC). Micropross 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 Micropross.

**www.micropross.com**

## MK SMART

Established in 1999 in Vietnam, MK Group is the leading company in Southeast Asia with years of experience in providing Digital security solutions and Smart card products for the following industries: Government, Banking and Fintech, Transport, Telecom, IoT, Enterprises, and the Consumer market.

With production capacity of over 300 mio. card per annum and more than 700 employees, MK Smart (a member of MK Group) is ranked under the Top 10 largest card manufacturers globally. The companies production facilities and products are security certified by GSMA, Visa, Mastercard, Unionpay, ISO 9001 and FIDO.

www.mksmart.com

## MÜHLBAUER ID SERVICES GMBH

Founded in 1981, the Mühlbauer Group has grown to a proven one-stop-shop technology partner for the smart card, ePassport, RFID and solar back-end industry. Further business fields are the areas of micro-chip die sorting, carrier tape equipment, as well as automation, marking and traceability systems. Mühlbauer's Parts&Systems segment produces high precision components.

The Mühlbauer Group is the only one-stop-shop technology partner for the production and personalization of cards, passports and RFID applications worldwide. With around 2,800 employees, technology centers in Germany, Malaysia, China, Slovakia, the U.S. and Serbia, and a global sales and service network, we are the world's market leader in innovative equipment- and software solutions, supporting our customers in project planning, technology transfer and production ramp up.

**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**

# Inline Window Application

**IPS**

Inline Production System for ID Cards · Data Pages · Driving Licenses · Resident Permit Cards

- Fully automatic punching and inserting
- For cards and data pages
- Zero gap technology
- Full lamination for utmost durability




MELZER®

www.melzergmbh.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

We make chips intelligent


# MTCOS®

## Independent – High Secure Card Operating System

- ELECTRONIC PASSPORT
- ELECTRONIC NATIONAL ID
- ELECTRONIC TICKETING
- ELECTRONIC HEALTH
- ELECTRONIC RESIDENCE PERMIT
- ELECTRONIC DRIVING LICENSE

**MTCOS 2.5 EAL5+**

certified on IFX, NXP and ST

We are looking forward to seeing you at Trustech, Paris!
Stand: 5.2 E031

SecurITy made in Germany

Common Criteria

WIBU SYSTEMS

# What matters most about your secure license container?

- The durability of your own hardware unit?
- The ease of a software activation?
- The freedom of cloud access anytime, anywhere?

www.wibu.com/cloud






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

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

SECURITY
LICENSING
PERFECTION IN PROTECTION