

# The VAULT

## SECURED WITH SECORA™

### FEATURED ARTICLE

**SECORA™ ID X drives introduction of contactless multi-application ID solutions based on JAVA Card™**  
Infineon Technologies & cryptovision

### ALSO IN THIS ISSUE

#### Wibu-Systems

Licensing in a highly fluid environment: Maximum flexibility for ISVs and their clients

#### Infineon Technologies

Brand protection is buyer protection: SECORA™

#### Infineon Technologies & Tribe

Infineon and Tribe join hands to strengthen Singapore's Blockchain Ecosystem

#### Fingerprints

Biometrics in a card: workplace security, no matter where you are

#### Infineon Technologies

SECORA™ Pay solutions enable contactless payments with environmentally friendly card body materials



# 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](http://www.infineon.com/secora-id)



# Contents

Infineon and Tribe join hands to strengthen Singapore's Blockchain ecosystem 4

Infineon Technologies

Infineon's SECORA™ Pay solutions enable contactless payments with environmentally friendly card-based materials 6

Infineon Technologies

Biometrics in a card: workplace security, no matter where you are 8

Maria Pihlström, Fingerprints

Infineon's SECORA™ ID X drives introduction of contactless multi-application ID solutions based on JAVA Card™ 12

Infineon Technologies & cryptovision

Brand protection is buyer protection: SECORA Blockchain makes the origin and history of a product visible 16

Infineon Technologies

Licensing in a highly fluid environment: Maximum flexibility for ISVs and their clients 18

Dr. Carmen Kempka, Senior Cryptography Expert, Wibu-Systems

Silicon Trust Directory 2020 28

---

## Imprint

### THE VAULT ISSUE 29

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: Rainer Bergmann, Markus Hoffmeister, Maria Pihlström, Dr. Carmen Kempka

PHOTOS: INFINEON TECHNOLOGIES, ISTOCKPHOTO, KROWNE COMMUNICATIONS, WIBU-SYSTEMS

EDITION: January 2021. No portion of this publication may be reproduced in part or in whole without the express permission, in writing, of the publisher. All product copyrights and trademarks are the property of their respective owners. All product names, specifications, prices and other information are correct at the time of going to press but are subject to change without notice. The publisher takes no responsibility for false or misleading information or omissions.

A man with a beard and short dark hair is shown in profile, looking at a laptop screen. He is wearing a blue button-down shirt over a grey t-shirt. The background is a dark, futuristic digital space with glowing blue and green lines, nodes, and icons. A large, glowing padlock icon is visible in the upper left, and a glowing cloud icon is in the upper right. The overall aesthetic is high-tech and digital.

INFINEON  
and *TRIBE*  
join *hands* to  
STRENGTHEN  
Singapore's  
*BLOCKCHAIN*  
Ecosystem

□ Infineon is partnering with Tribe, the first Singapore Government supported blockchain ecosystem builder, which brings together government agencies, corporates and blockchain companies to foster innovation and collaboration. Infineon will provide its longstanding industry expertise in hardware security solutions and can help companies seeking to apply blockchain to discover the competitive advantages of Infineon's SECORA™ Blockchain security solutions. Selected start-ups developing applications using SECORA™ Blockchain will have the opportunity to collaborate with Infineon in time-to-market and customer development as partners at the Infineon Co-Innovation Space.

---

*"Blockchain is moving beyond Fintech into areas as diverse as logistics, brand protection, online shopping and gaming platforms. Tribe's OpenNodes give us access to a vibrant blockchain ecosystem and allow Infineon to showcase our SECORA™ Blockchain Security Solutions. We are honoured to be part of Tribe and are excited to collaborate with them on several fronts, such as supporting OpenNodes-led initiatives as a founding member and working with Tribe Academy to identify promising tech talents. I look forward to explore business opportunities together in the emerging blockchain verticals with leading ecosystem players."*

**Goh Say Yeow, Vice President, Connected Secure Systems, Infineon Technologies Asia Pacific Pte Ltd**

---

Tribe is Singapore's first government supported platform in driving neutrality, collaboration and growth of the blockchain ecosystem, comprising of OpenNodes, Tribe Accelerator, and Tribe Academy. These different initiatives come together to form a cohesive, multifaceted approach to provide a more comprehensive level of support to the blockchain industry. Tribe works closely with global corporations, government agencies, top-tier blockchain companies and late-stage start-ups to build a community that promotes blockchain collaborations

and innovations. Tribe's official partners include Enterprise Singapore, IMDA, BMW Group Asia, ConsenSys, IBM, Intel, Nielsen, PwC, R3, and Temasek amongst others.

---

*"Driving ecosystem collaboration is a key priority for Tribe as we look to advance blockchain's capabilities and its deployment across industries. As we witness a surge in industry ready solutions based on blockchain, security continues to be a key consideration and differentiator for blockchain companies. With Infineon we have a partner that is well positioned to secure blockchain applications and strengthen trust in the technology. We hope to drive Singapore's agenda to be a hotbed for blockchain innovations and real-world application, as we continue to identify and fill the gaps in the industry."*

**Joseph Lim, Head of Global Business Development, Tribe.**

---

As a leading player in blockchain, Infineon has developed the SECORA™ Blockchain, which is a fast, easy-to-use Java Card™ solution supporting best-in-class security for blockchain system implementation. It makes the application more secure and easier to design for a customer's blockchain system. By providing a safe "vault" for user credentials, SECORA™ Blockchain can reduce the final user's commercial risk and helps to increase trust in the block chain system. Infineon's extensive security expertise provides the layer of security required to protect private blockchain keys. The integration of hardware-based security into blockchain applications, such as tokens, wearables, and different module forms, makes private keys much more robust against attacks.

SECORA™ Blockchain with SPA Package is now available in volume quantities. It supports cryptoschemes like Ethereum and Bitcoin. ☒

For more information on Tribe, please proceed to <https://tribex.co>



Infineon's  
SECORA™ Pay *solutions*  
ENABLE contactless  
*payments* with  
ENVIRONMENTALLY  
*FRIENDLY* card *body*  
MATERIALS

□ Contactless payment innovations from Infineon Technologies AG contribute to a more sustainable use of resources. To support the payment industry's move towards the use of more environmentally friendly materials for smart card manufacturing, Infineon is now offering a complete, single-source solution that is easily adaptable to different projects and market requirements. SECORA™ Pay with Coil-on-Module (CoM) package comes with a newly developed antenna, specifically designed for cards made from recycled ocean-bound plastic or wood. It is the industry-wide thinnest payment module with a copper wire antenna, which allows cost-efficient card manufacturing for mass deployment.

“Infineon’s Coil on Module technology is one of the most important innovations for contactless and dual interface payment cards,” said Bjoern Scharfen, who heads the product line Payment & Ticketing Solutions at Infineon. Communication between chip module and card antenna is based on a radio frequency (RF) link, no electrical connection is required. “By using CoM, our chip solutions can be easily integrated into contactless cards made of different materials. Manufacturers can flexibly and cost-effectively change their card designs and offer consumers sustainable, long-lasting products.”

CPI Card Group Inc., a payment technology company and leading provider of credit, debit and prepaid solutions, is already deploying Infineon’s SECORA Pay solution for its new range of eco-friendly plastic cards. “Using the Infineon SECORA Pay solution enabled CPI to bring Second Wave®, our payment card that features a core made of recovered ocean-bound plastic to market quickly. The combination of inductive coupling antennas and chips made scaling this sustainable eco-focused payment card an efficient process”, said Guy DiMaggio from CPI.

## Advantages of CoM technology

Environmentally friendly materials such as wood, Polylactid (PLA) or recycled plastic are more challenging to work with compared to PVC, especially when it comes to the card manufacturing processes such as lamination and printing. These have been standardized by the card industry for decades. Infineon’s SECORA Pay solutions use inductive coupling to connect the chip module with the card antenna, which results in a number of advantages for card manufacturers and users.

The payment chip modules have a thickness of only 0.32 mm and are thus up to 50 percent thinner and up to 70 percent lighter compared to other solutions available in the market. Consequently, the CoM module provides higher flexibility concerning card construction, while the new antenna design based on state-of-the-art copper wire, is easier to embed into all known inlay sheet materials, including recycled ocean-bound plastic. Moreover, there is also no need for additional adhesive elements during the card lamination process.

Finally, CoM technology makes cards more robust and helps to meet the increasing demand for contactless solutions: with CoM, contactless cards can be produced on standard equipment for contact-based cards, without making new investments in specific machinery.

Worldwide, cards are the product of choice when it comes to contactless payments. Market research firm ABI Research expects dual interface card shipments to reach 2.2 billion pieces in 2020 (Payment and Banking Card Secure IC Technologies, August 2019). To protect natural resources and to increase environmental sustainability, leading industry players are therefore launching more ecofriendly programs like the Greener Payments Partnership (GPP) program by MasterCard. ☒





# BIOMETRICS in a *CARD: workplace* SECURITY, *no matter* where *YOU* are

By Maria Pihlström, Fingerprints

□ Increasing workplace security has been a long-standing issue for many organizations, with traditional security measures no longer aligned with modern needs. Passwords, for example, are easily hacked and carry the risk of serious data breaches. Moreover, employees have to remember an array of different codes across devices and accounts, leading not only to reuse and frustration, but costing enterprise IT departments millions a month in resetting forgotten passwords.

Unsurprisingly, then, the demand for more secure and seamless access methods has been rising. One 2019 Gartner study<sup>1</sup> predicted that 60% of large and global enterprises, along with 90% of mid-size enterprises, will implement passwordless authentication methods in over half of use cases by 2022.

This year has put even more pressure on the need for increased workplace security, as well as convenience for the employees. Although flexible working was already a growing trend, it has accelerated significantly in the light of the pandemic and remote working mandates, increasing the average cost of a workplace data breach by \$137,000<sup>2</sup>. In addition, employees have started working more flexible hours on-premise, making building access less regulated and more susceptible to attack.

To minimize crime and financial losses, enterprises need more control over who can access their buildings, or offices - wherever they might be - and access their servers and digital data. With biometrics gathering momentum beyond smartphones, it can offer more secure and convenient authentication across the workplace that could be at the office, at home or even at a café.

---

1. *Embrace a Passwordless Approach to Improve Security*, Gartner; March 6, 2019

2. <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>

## On the cards: Why biometrics?

Biometric access cards can be thought of as a modern-day key that combines access with a multiuse, such as an ID badge. Each access card is linked to one specific cardholder, who registers their fingerprint on the card. When entering a building or office, logging into any system, the card's biometrics must match the person using the card, ensuring that only authorized employees gain access.

Since unique biological traits are extremely difficult to steal and spoof, biometric access cards are more secure than traditional access cards and fobs that require PINs, or no additional authentication. Compared to existing solutions, the technology is also more convenient. You can't forget your fingerprint, after all, not to mention there's the possibility to streamline authentication across the workplace. And if it gets lost or stolen, no one else can use it. There's no need to tap or touch a shared PIN pad or reader either, as the card is contactless.

These benefits are often far simpler to realize than many enterprises imagine. Biometric cards can be integrated into existing infrastructure across offices, enabling improved workplace security that is convenient for both employers and their employees. And because the biometric data is stored and processed on the card, privacy is guaranteed for employees, while organizations don't have the cost, complexity and compliance headaches associated with managing biometric databases.

## Adding security and convenience where it matters

Use cases for biometric access cards are numerous. Besides unlocking doors, the cards can also be used for any other new or existing authentication access point across the workplace, such as logging into work computers or digital files, accessing time and attendance systems, and resetting alarm systems.

The benefits of increased and more convenient security reach far beyond keeping burglars out. From preventing industry espionage to managing personnel in vital industries, let's take a look at three examples where biometric access cards can add security where it matters.

## Examples of where it can be used - Healthcare

In Healthcare whether it is for certain wards, drugs cabinets or operation rooms – it is crucial. Moreover, with a two-factor authentication for many access points or to access patient data, adding additional pressure to often busy workdays. Combining security and convenience, biometric cards can strengthen access control systems, while removing a point of friction for many healthcare professionals. The UK's NHS is just one example that's recently announced it's investing £40 million in implementing biometrics to remedy staff stress and frustration with the legacy IT system access process.<sup>3</sup>

In a pharmacy setting, biometric access cards can also ensure that only qualified employees have access to certain medications. Similarly, it can conveniently unlock the issuance of medicine in digital systems for permitted staff and allow them – and only them – to review and update the personal health information of their patients.

## Keeping corporate secrets

Corporations and enterprises hold many highly sensitive files that, if stolen or otherwise compromised, could damage the company or individuals. From legal offices to accountancy firms, biometric access cards could not only keep offices highly secure, but also lock devices and certain files on a company's system.

By locking digital files with biometrics, only employees working

3. UK looks to replace passwords with biometric technology to reduce NHS login time, *Biometric Update*; January 7th 2020 VI

“ *Labs and R&D departments are often subject to industry espionage. In this type of workplace, biometric access cards can ensure sensitive information stays under lock and (digital) key*

on a particular project would have access to the information, ensuring that confidential information is no longer at the mercy of easily hacked passwords. And when files do disappear or fall into the wrong hands, a meticulous record showing who last had access to the office or information, can facilitate a smoother investigation of the data breach.

## **R&D departments**

Labs and R&D departments are often subject to industry espionage. In this type of workplace, biometric access cards can ensure sensitive information stays under lock and (digital) key.

But ideas are not the only thing kept safe by the cards. Because labs can contain dangerous materials, substances and machinery, controlled access is even more important. Biometrics can enable more controlled and secure access, ensuring hazardous premises are only accessible to trained and authorized personnel.

Research departments are also often sensitive and sterile test environments and require meticulous logs of who has entered an area or operated a machine. Biometric security systems can reduce errors in attendance logging, creating more predictable test environments and, ultimately, facilitating more accurate test results.

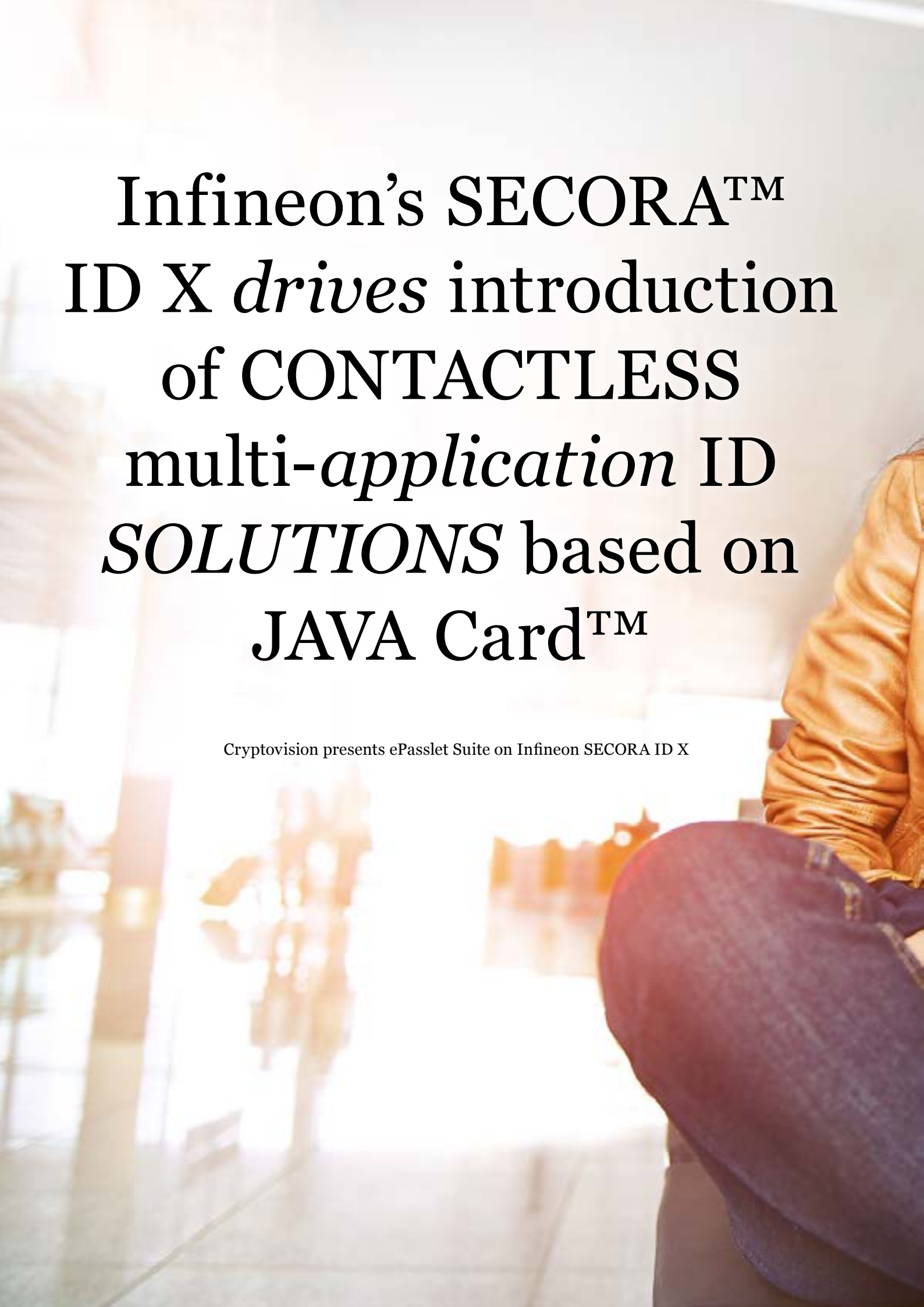
## **Beyond cost savings and worryless workdays**

Hacked and forgotten passwords cost IT departments millions a year, while lost keys and forgotten passwords are a number one frustration for many employees.

Biometric access cards can provide a more convenient and secure authentication solution for both physical and logical access control, offering a solution to security breaches and the need to remember multiple strong passwords.

But the technology can go beyond just cost savings for IT teams and reducing daily annoyances. By offering improved security in high-stake industries, biometrics can ensure that medication is authorized by the right person, compromising information is kept confidential, and inventors keep control of their intellectual property.

In this way, biometric access cards bring a whole new dimension to worryless workdays, unlocking a modern workplace security system that adds convenient security where it truly matters. ☒



**Infineon's SECORA™  
ID X *drives* introduction  
of CONTACTLESS  
*multi-application* ID  
*SOLUTIONS* based on  
JAVA Card™**

Cryptovision presents ePasslet Suite on Infineon SECORA ID X





□ Infineon Technologies AG has extended its easy-to-integrate security solutions for contactless electronic ID documents. SECORA™ ID X is the company's new flagship for highly secured yet versatile government ID solutions targeting customized applications. The solution's particularly large user memory of up to 450 kByte allows the realization of a broad variety of eID products, ranging from identification only, to multifunctional cards that combine identification, digital signature and secured web access.

To accelerate the introduction of locally customized ID documents, Infineon provides the SECORA™ ID X open platform with all the necessary tools for easy implementation. Chip and operating system are certified according to Common Criteria EAL 6+, hence fulfilling highest security requirements of eGovernment applications. Besides enabling multi-application and country-specific customization, SECORA™ ID

X also allows post issuance, i.e. activation of the card in the field by the document owner. This will further enhance acceptance and convenience of eGovernment applications.

All members of Infineon's SECORA™ ID platform combine chip, operating software and applets to facilitate the design and introduction of new ID products and solutions. They are based on Java Card™ Standard v3.0.5 software and are offered with multiple applets for personalization of the documents. While innovative chip packaging such as Coil-on-Module remains key in smart card production, contactless performance is crucial for the growing number of contactless cards.

SECORA™ ID X will be provided with the ePasslet Suite by cryptovision GmbH. With the help of cryptovision's ePasslet Suite, users of SECORA™ ID X will make putting numerous eID functions into practice easier and with greater flexibility.

“ We are delighted to have reached a further milestone on our path to offer modular, standard-based eID solutions on all major chip platforms. Government customers across the world will benefit from this broadened portfolio - said cryptovision's CEO, Markus Hoffmeister.

Cryptovision's ePasslet Suite on SECORA™ ID X provides applets for various eID document applications, including electronic passports, eIDAS-compliant ID and signature cards, international electronic driver's licenses, electronic health cards (eHIC), custom national eID cards and more. ePasslet Suite V3 also supports ICAO LDS 2.0, an extension of electronic passports with electronic visas and entry and exit stamps.

“We are delighted to have reached a further milestone on our path to offer modular, standard-based eID solutions on all major chip platforms. Government customers across the world will benefit from this broadened portfolio,” said cryptovision's CEO, Markus Hoffmeister.

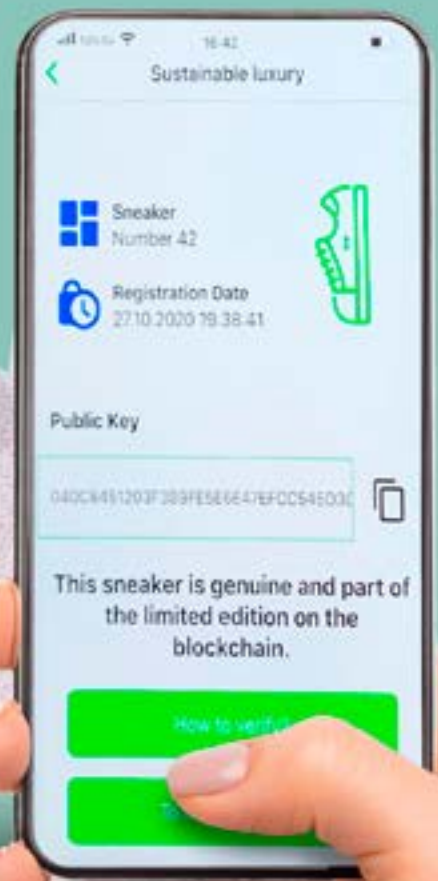
In addition, ePasslet Suite on SECORA™ ID X can be freely customized through various configuration options. It can evolve to support new use cases and applications while retaining

Common Criteria (CC) certification, thereby enabling multi-application cards and documents.

ePasslet Suite on SECORA™ ID X is being certified according to Common Criteria (CC) EAL 5+. It is available in three editions, offering cost-efficient configurations for standard, as well as high-end and customized ID document solutions. Samples of the solution are now available on request.

With Infineon's SECORA™ ID X as an additional platform for ePasslet Suite, cryptovision is extending its offering for international eID customers: Infineon's expertise is based on more than 200 government ID projects that cover more than 75 percent of the world's population. ☒

*Brand* PROTECTION  
is *BUYER* protection:  
SECORA™ Blockchain  
makes the ORIGIN and  
*HISTORY* of a product  
VISIBLE





“ *The information about manufacturer and product can be stored in the blockchain as individual data blocks that build on each other. This can allow anyone to access the decentralized data register from anywhere.* ”

□ Infineon Technologies AG has developed a customized security solution for blockchain applications that improves brand and consumer protection. The new SECORA™ Blockchain security solution is integrated into the branded product and connects to the blockchain via NFC technology – thereby linking the real world with the digital world.

By storing information in the blockchain, the manufacturer can document the authenticity of the product, feature a limited edition or demonstrate the sustainability of the production e.g. its compliance with environmental standards. Consumers in turn can access the information stored in the Blockchain via a mobile device and an app.

SECORA™ Blockchain combines a tiny cryptochip with a radio antenna in a flat housing with a total thickness of max. 300µm. It can be attached barely visible behind a label or on the product itself and hence is easy to integrate. As a hardware-based solution, SECORA™ Blockchain has a decisive advantage over other blockchain access options: It is protected against both hardware- and software-based attacks.

Another essential advantage: SECORA™ Blockchain can encrypt data and signatures with a private key. The product with an integrated chip can thus directly and easily establish a connection to the corresponding blockchain entry with an NFC-enabled mobile device. The signature key, which authenticates the identity of the product, is not generated on


the mobile device, but in the cryptochip and is securely stored therein, unlike other solutions on the market. This further increases the security of the application.

SECORA™ Blockchain can be used for a wide range of products, from fashion and footwear, to electronics or healthcare. At the virtual trade fair electronica 2020, Infineon presented the functionality and use cases of the innovative solution in cooperation with the block chain company block42.

The information about manufacturer and product can be stored in the blockchain as individual data blocks that build on each other. This can allow anyone to access the decentralized data register from anywhere. Besides origin, changes to the products, use of original spare parts or changes of ownership of limited collector's items can be continuously documented.

However, it is also important here that access to the blockchain is protected to prevent data manipulation. In this way, the brand and reputation of manufacturers can be protected and the sale of counterfeits be prevented.

SECORA™ Blockchain with SPA Package is now available in volume quantities. It supports cryptoschemes like Ethereum, Bitcoin, ETR ERC-20. Additionally, Infineon's Blockchain Security2Go starter kit enables blockchain designers to quickly develop easy-to-use access solutions for blockchain applications. ☒

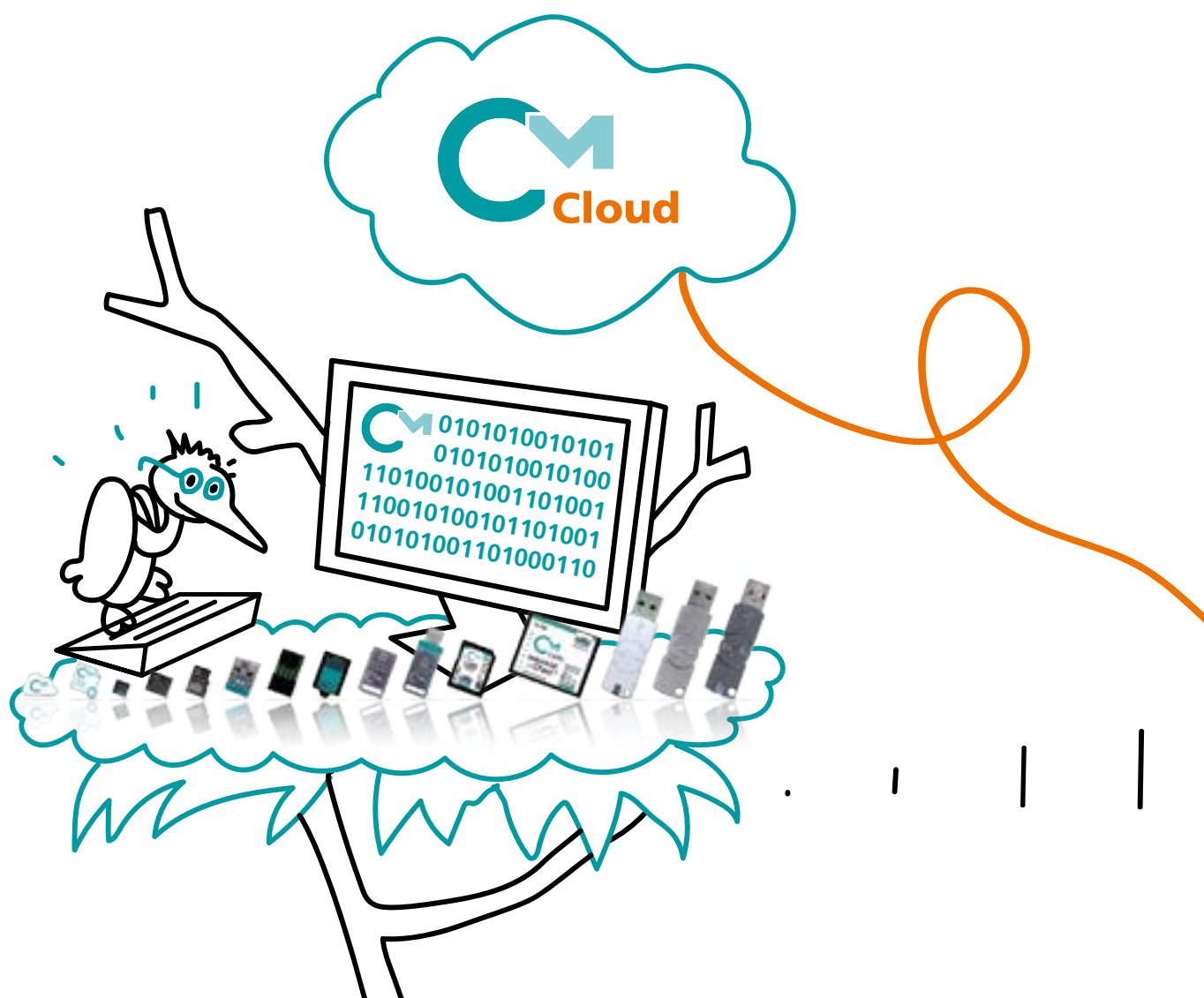


*Licensing* in a HIGHLY  
FLUID environment:  
Maximum *FLEXIBILITY*  
for ISVs and *their*  
CLIENTS

Dr. Carmen Kempka, Senior Cryptography Expert, Wibu-Systems

```
elif operation == "MIRROR_X":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end add back the deselected mirror modifier object
mirror_ob.select=1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
mirror_ob.select = 0
```



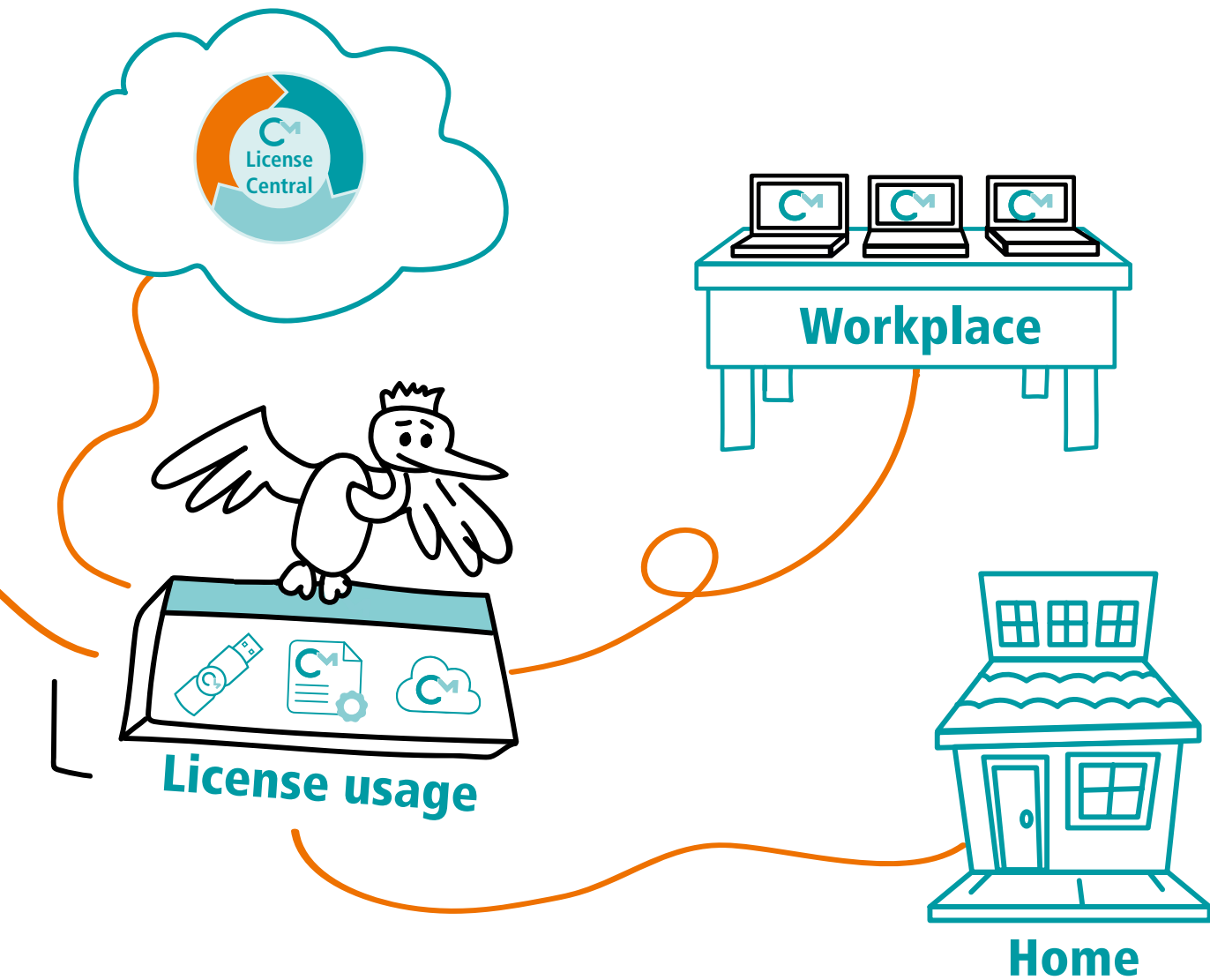
□ The year 2020 has shown us that sometimes, very suddenly, we need to be very adaptive. Wibu-Systems provides independent software vendors (ISVs) with a licensing model unparalleled in versatility, while maintaining high security standards. With a licensing infrastructure relying on standardized cryptographic algorithms, rather than proprietary solutions, the company offers protection against piracy, reverse engineering, tampering and malicious attacks.

### Several dimensions of flexibility

Each customer, each situation and each use case have their individual requirements. User A might want to work offline in a pay-per-use setup, while User B shares a network license of an annual subscription with their colleagues, and User C uses a trial subscription to a SaaS application in the cloud.

Customer D wants to protect an IoT device against tampering while customer E wants to protect their desktop application against reverse engineering. Customer F wants to bind their license to a single device, and Customer G requires additional key material within secure hardware. Moreover, circumstances are subject to change: User A might want to switch from pay-per-use to a monthly subscription, User B might have to work remotely as well as in-house and be able to access the license from different devices and locations, and User C might want to upgrade their trial license to the full version.

A good licensing framework needs to provide flexibility in more than one dimension. To keep things simple, the ISV should not have to think about which of the endless possibilities of environments their software is used in when creating their protected application. In an optimal setting, the protected code can stay the same while the license is adapted to the



environment and situation at hand. In fact, requirements might change, as we have seen in the beginning of 2020, where employees had to switch from on-premise work to remote within days. The licensing solution of Wibu-Systems offers several dimensions of flexibility.

**Automated or customized:** with CodeMeter Protection Suite, applications and libraries can be encrypted either in a completely automated fashion with no manual effort required, or in a more customized way by encrypting individual functions or even weaving cryptographic calls into the code. Cryptographic methods are used by default, and licenses can carry additional key material customizable by the ISV, which can be used by the protected software.

**Flexibility in the licensing model:** when creating the protected code, the software vendor can, but doesn't have

to, think about the hardware binding or licensing model of a client's license. The same protected piece of software can be used with several license models like pay-per-use, monthly subscriptions, trial or full versions, floating or single user licenses, or permanent licenses. This offers a high level of adaptiveness: changing the licensing model only requires an update of the license itself; the protected application does not need to be modified.

**Flexibility in the way and degree licenses are bound to a device:** Licenses are stored on a license container. A license container can be a secure hardware element directly connected to a device, or to a license server in the network. Computer-bound software license containers or user-based license containers in the cloud offer mobility for both offline and online usage.

“*Monitoring of the license usage makes it easier for ISVs to adapt their software and licensing model to their customer’s needs, or to detect and prevent malicious usage.*”

Hardware license containers are available for several hardware interfaces, for example **CmDongle** for USB, or **CmASIC** for ASIC. SD, microSD and CF are also among the supported interfaces. They can be used as secure elements to store key material and do cryptographic operations. They can also be used as a certificate vault to store X.509 certificates and to identify devices uniquely.

A **CmActLicense** is a license container in the form of a secure file, which is bound to attributes of the target device. Which and how many attributes are used in the binding, as well as the strictness of the binding, is customizable by the ISV.

The newest license container type and next logical step in Wibu-Systems’ lineup is a license container in the cloud, namely a CmCloudContainer, hosted by Wibu-Systems itself. This licensing solution is called CmCloud and was released in September 2020. A CmCloudContainer offers the maximal level of mobility. It can be accessed from everywhere through an Internet connection and is ideal for software usage because it's not bound to a certain device or location.

### **CmCloudContainer: A new container type for optimal mobility and security**

A CmCloudContainer is tailored to offer the best solution in security, high performance, and high availability; all of this has been incorporated early in the development process. CmCloud

offers many advantages: In a CmCloudContainer, the license always stays accessible and manageable by the ISV. Securely stored in a CmCloudContainer, the license never resides on a client device or any untrusted environment. This way, the client can neither copy nor lose their license.

Since ISVs always have access to CmCloud and their license containers, they can easily modify and adapt licenses for their customers, without the need for any interaction with them. This way, licenses can, for example, be updated from trial to the full version, or from pay-per-use to a monthly subscription, without re-activation or software updates on the client side. In the same way, licenses can easily be withdrawn or locked in the case of contract cancellation, or illegal license usage and fraud. No blacklisting of license containers is necessary.

Real-time monitoring of the license usage makes it easier for ISVs to adapt their software and licensing model to their customer’s needs, or to detect and prevent malicious usage.

Since the license container is kept in the cloud, no additional infrastructure like VPN or additional hardware is needed to access a license when working remotely out of office, or on different devices. A CmCloud license does not bind the license to a certain device. However, the number of devices which can use a CmCloud license at the same time can be restricted, and access to the CmCloud license requires a credential on the client device.



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**





## **Supporting our customers in quarantine time**

At the beginning of 2020, the home office became omnipresent in our work life very suddenly, without the time to prepare for any notable changes in infrastructure. To make license access possible from arbitrary places, a pre-release version of CmCloud was set up in May 2020. During this pre-release phase, Wibusystems provided a free of charge CmCloudContainer to their customers, allowing license access when working remotely. The only required prerequisites for this setup were an Internet connection and cryptographic credentials for license access. The pre-release proved to be stable, and we could confidently release CmCloud in September.

## **Cloud based automatable license deployment**

Regardless of the used container type, with CodeMeter License Central, licenses can be managed in the cloud, and activated on the client side when needed, either on a hardware dongle, a CmActLicense soft container, or on a CmCloudContainer. Licenses can, but do not have to, be restricted to a certain license container type or hardware binding scheme.

The complete lifecycle of a license from creation to deployment and activation can be automated: CodeMeter License Central can easily be integrated in existing ERP, CRM, and back office systems to deliver software, create licenses automatically and transfer licenses to the client's license container.





# MTCOS<sup>®</sup>

Independent – High Secure  
Chip Operating System



ELECTRONIC  
PASSPORT



ELECTRONIC  
NATIONAL ID



ELECTRONIC  
TICKETING



ELECTRONIC  
HEALTH



ELECTRONIC  
RESIDENCE  
PERMIT



ELECTRONIC  
DRIVING  
LICENSE



We hope to see you at one  
of the upcoming events!



	<b>CmDongle</b>	<b>CmActLicense</b>	<b>CmCloudContainer</b>
<b>Cryptographic operations in secure environment</b>	×		×
<b>Secure key storage</b>	Highest	High	Highest
<b>Unique device authentication</b>	×	×	
<b>Certificate vault</b>	×		
<b>Hardware binding</b>		×	
<b>Access from everywhere</b>			×
<b>Offline usage</b>	×	×	
<b>Monitoring</b>	×	×	×
<b>Real-time monitoring</b>			×
<b>License management in the Cloud (CodeMeter License Central)</b>	×	×	×

## Comparing the different license container types

Which container type or licensing model is most suitable needs to be decided individually for each use case. Hardware license containers add to security by acting as secure elements for key and certificate storage, and enable device authentication. They are optimal for a setting where cryptographic operations need to be done within secure hardware.

Hardware license containers can, for example, give IoT devices an all-around protection ranging from anti reverse engineering techniques and copy protection, to integrity protection. Cryptographic methods shield the devices from piracy and manipulation attacks. Unique device authentication is realized using cryptographic techniques and key material protected within the secure hardware.

CmActLicense containers are cryptographically protected software licenses that are stored directly on a device and therefore do not require additional hardware. They can be bound to a device's hardware attributes and are optimal for offline usage.

While hardware dongles offer security by protecting licenses within secure elements, CmCloudContainers offer security through the fact that the license and its key material never leaves the CmCloud hosted by Wibu-Systems. Cryptographic operations are performed within the cloud. Cloud licenses can be accessed from everywhere given the correct credentials, and do not restrict usage to a certain device or location. Since the licenses remain in the cloud, license usage in CmCloud can be monitored real-time by the ISV.

## Freedom of choice

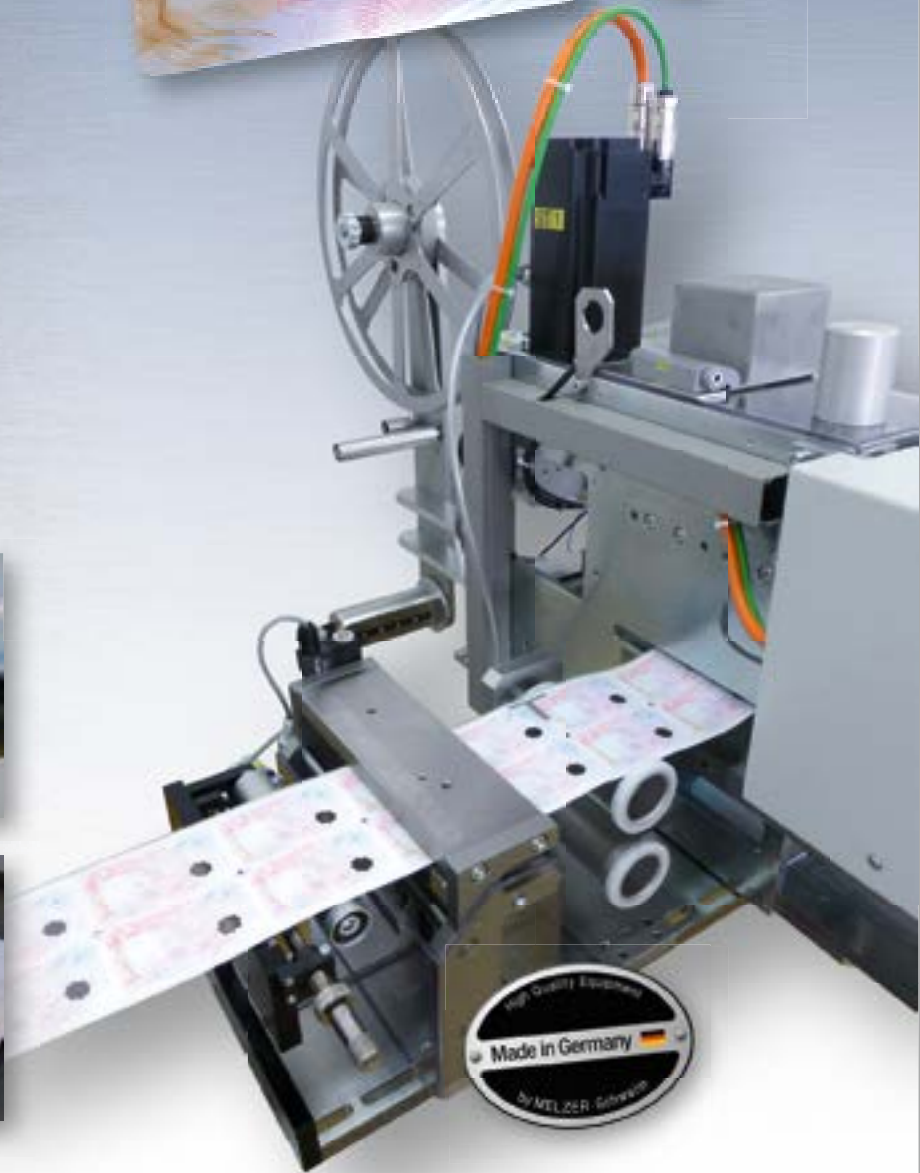
Flexibility and adaptiveness are essential not only in days like these. This adaptiveness is achieved with a licensing framework offering suitable degrees of freedom, while being tailored for compatibility and interchangeability between licensing models. You have the freedom of choice. ☒

# 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



INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

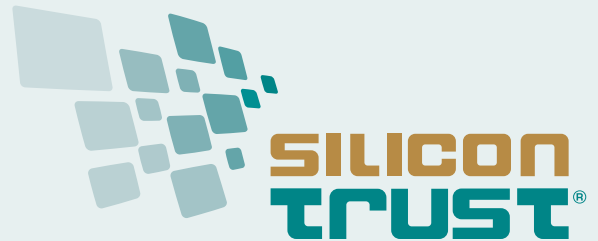
**MELZER**<sup>®</sup>

Please visit us at: **ID4AFRICA** · Johannesburg, South Africa · **Booth: B3** |  
**ICAO TRIP** · Montreal, Canada · Booth: 50 | **Labelexpo Europe** · Brussels, Belgium · Booth: 6C10 more ▶ [www.melzergmbh.com](http://www.melzergmbh.com)

---

# SILICON TRUST DIRECTORY 2020

---



## 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](http://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](http://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](http://www.aisec.fraunhofer.de)



# We create your eID solution

- Standardized, multi-app & bespoke eID documents
- Tools for easy personalisation
- eID application integration
- Document PKI

Subscribe to our NEWSLETTER now!



## 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](http://www.advanide.com)

### ATOS



Atos SE is an international information technology services company with 2014 annual revenue of € 9 billion and 86,000 employees in 66 countries.

Serving a global client base, it delivers IT services through Consulting & Systems Integration, Managed Operations, and transactional services through Worldline, the European leader and a global player in the payments services industry. It works with clients across different business sectors: Manufacturing, Retail & Transportation; Public & Health; Financial Services; Telcos, Media & Utilities.

[www.atos.net](http://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](http://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>

### 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](http://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](http://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.

[www.cryptovision.com](http://www.cryptovision.com)

### DE LA RUE



De La Rue is a leading provider of sophisticated products and services that keep nations, their economies and their populations secure. At the forefront of identity management and security, De La Rue is a trusted partner of governments, central banks and commercial organisations around the globe.

[www.delarue.com](http://www.delarue.com)

## DIGITAL IDENTIFICATION SOLUTIONS



Digital Identification Solutions is a global provider of advanced identification solutions, specialized in secure government and corporate applications for ID cards and ePassports/Visa. By applying innovative technologies, they develop unique, scalable credential solutions, which perfectly meet the ever-changing demands of international customers.

[www.digital-identification.com](http://www.digital-identification.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](http://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, prelamines, LaserCard® optical security media technology, and FARGO® card printers.

[www.hidglobal.com](http://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](http://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](http://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](http://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. Our system and solutions business unit offers advanced issuance solutions and software for integrators and operators in all targeted industries.

## 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

Member of the KURZ Group

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 protection 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](http://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](http://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](http://www.pav.de)

## POLYGRAPH COMBINE UKRAINA



State Enterprise "Polygraph Combine "Ukraine" for securities' production" is a state company that has more than 40 years of experience in providing printing solutions.

Polygraph Combine "Ukraine" 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-ukraine.gov.ua](http://www.pk-ukraine.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](http://www.precisebiometrics.com)

## PRIMEKEY



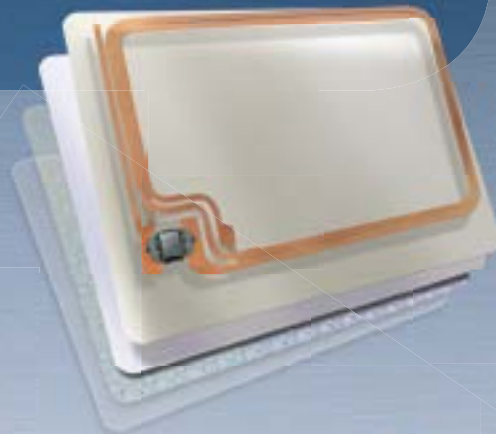
One of the world's leading companies for PKI solutions, PrimeKey Solutions AB has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security

software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

[www.primekey.com](http://www.primekey.com)



# 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**<sup>®</sup>

[www.melzergmbh.com](http://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](http://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](http://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 conceptualize, promote and implement various projects along the value chain.

[www.sipua-consulting.com](http://www.sipua-consulting.com)

## 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](http://www.unitedaccess.com)

## WATCHDATA TECHNOLOGIES



Watchdata Technologies is a recognized pioneer in digital authentication and transaction security. Founded in Beijing in 1994, its international headquarters are in Singapore. With 11

regional offices the company serves customers in over 50 countries. Watchdata customers include mobile network operators, financial institutions, transport operators, governments and leading business enterprises. Watchdata solutions provide daily convenience and security to over 1 billion mobile subscribers, 80 million e-banking customers and 50 million commuters.

[www.watchdata.com](http://www.watchdata.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](http://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](http://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](http://www.x-infotech.com)



# Integrity Guard – the smartest digital security technology in the industry

You need security? Relax with Integrity Guard!

With more than 1.5 billion chips sold, Integrity Guard is setting the technological standard for chip-based security. It bundles several highly sophisticated digital security mechanisms that combine to cover a broad spectrum of potential attacks. Integrity Guard has been developed for applications with high data security requirements for a particularly long life cycle, such as government-issued electronic ID documents (passports, national ID and health care cards).

## Security chips with Integrity Guard feature:

- › Robust security for demanding needs
- › Even in the CPU core, data is always encrypted
- › Harmless events don't cause false alarms
- › Chip architecture reduces need for costly updates
- › Automated security features for faster time to market



[www.infineon.com/integrityguard](http://www.infineon.com/integrityguard)



## Let CodeMeter inspire you with new license-driven business models

- Protect your digital assets from piracy and reverse engineering
- Secure the integrity of your endpoints from tampering
- Implement license-based readily adaptable business models

Customer centric approach

From the cloud down to FPGAs

Digital global marketplace

Software, firmware, and sensitive data

Brown field and green field



Don't wait any longer  
Start protecting your IP now!  
[s.wibu.com/sdk-cm](http://s.wibu.com/sdk-cm)

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



SECURITY  
LICENSING  
PERFECTION IN PROTECTION