NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2013 | #25

# The VAULT

FEATURED ARTICLE

## Infineon's SECORA™ID accelerates eID project execution

Infineon Technologies

ALSO IN THIS ISSUE

**Paragon ID**
Ready for the thinnest eDatapage challenge

**The Silicon Trust**
Unveiling the ID4Africa Identity Council

**AVTOR**
Transforming tokens and smart cards

**Mühlbauer ID Services**
Government solutions for the Republic of Fiji

**VFS Global**
What's next for online citizen services?

**Wibu-Systems**
Software licensing in the cloud

**cryptovision**
A new German security architecture for next generation ID and IoT requirements

**The Silicon Trust**
Embracing System-on-Card



# 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

Infineon


# Contents




## Imprint

**THE VAULT**
Published bi-annually by Krowne Communications GmbH, Berlin.
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge
EDITORIAL CONTRIBUTIONS: Steve Atkins, Hervé Naullet, Markus Moesenbacher, Arnaud De La Chapelle, Markus Hoffmeister, Klaus Schmeh, Viacheslav Tatianin, David Paine, Lara Schmaus
PHOTOS: ID4AFRICA, WIBU SYSTEMS, INFINEON TECHNOLOGIES, ISTOCKPHOTO, AUSTRIACARD, MÜHLBAUER ID SERVICES, PARAGON ID, CRYPTOVISION, KROWNE COMMUNICATIONS, AVTOR LLC, COGNITEC, MASKTECH, MELZER MACHINENBAU,
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE


EDITION: November 2019 : 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.

# *UNVEILING* the ID4AFRICA *Identity* COUNCIL

By Steve Atkins, Silicon Trust


Earlier this year, the ID4Africa Movement announced the appointment of Ambassadors from 43 African nations for its 2019 Ambassador Class. This impressive expansion in representation – up from 29 countries in 2018 – reflected a strong endorsement from the African Governments of the ID4Africa Ambassadors Program, and a clear recognition of the importance of the evolving role the Ambassadors were playing.

☐ Of note is the degree of geographic inclusivity attained by the program in 2019, which now stretches beyond sub-Saharan Africa, to include Northern Africa, as well as the sovereign islands off the African coast.

Commenting on this achievement, Dr. Joseph J. Atick, Executive Chairman of ID4Africa, said: "I am excited to see the Program become the largest institutionalized body for south-south cooperation around identity matters in Africa. While the growth in the ranks of the Ambassadors is remarkable, what is even more significant is the way in which their role has evolved. While they continue to act as key liaisons between the ID4Africa Movement and their individual countries, we are empowering the group to become a collective thought leadership body, that can provide Pan-African guidance and promote the exchange of experiences and knowledge among the represented countries themselves."

The ID4Africa Ambassadors are senior-level government officials (appointed one per country) that work for government identity stakeholders in their country. Selected based on merit, passion, and experience, the Ambassadors are key drivers within the Movement, who not only serve to establish and maintain active collaboration between the ID4Africa General Secretariat and the identity stakeholders, but also influence the agenda and direction of the Movement. They help keep the Movement informed on issues that are pertinent and ensure that their respective countries' priorities in identity management are part of the Movement's collective agenda.

Said Atick, "We want to retain these Ambassadors so they stay working with their institutions and the only way we can do that is by empowering them to make decisions by themselves. Otherwise the brain drain will continue to happen in Africa and talent will be attracted to go to the private sector. By creating powerful institutions and empowering these people to complement their national institutions I think we can help African governments retain talent and even re-enforce it, by building more talent to support the activities and plans for institutions like the ID4Africa Identity Council (IIC)."

They also ensure that their nations are well represented in their delegations to the Annual General Meetings (AGM). In their collective action and through the IIC, this role is expanding to include guidance and support of the decision-making process for the development of Pan-African identity ecosystems.

The Silicon Trust was honoured to be there and act as independent observers during the vote counting for the election of the IIC's President and Vice-President, which saw the election of Mory Camara (Guinea) as President and Emmanuel K. Brown (Ghana) as Vice President.

"The IIC is basically the operational arm of the ID4Africa Movement. It represents all the shared experience of the countries in terms of the establishment of Digital Identity and we have those who are very advanced and others who have a long way to go," said Mory Camara, President, ID4Africa Identity Council.

"The Goal is to share those experiences, advice, consult, assist wherever we can; we have a lot of expertise – technical, legal, procedural, financial, so it's a chance for Africa to put into practice all the recommendations, the strategies and the lessons that we have learnt throughout the five years' existence of the ID4Africa movement," he added.

ID4Africa appoints one Ambassador per African country per year – subject to a term limit of 4 years. Considering the term expiration of certain ambassadors, as well as unrepresented countries, the Movement opens the Annual Call for Ambassadors during the 4th quarter of each year. In building the 2020 Class of Ambassadors, ID4Africa accepted applications from the following 14 countries: Angola, Benin, Botswana, Comoros, Republic of Congo, Egypt, Equatorial Guinea, Ethiopia, Malawi, Mali, Mozambique, Seychelles, Sudan & Zimbabwe. ☒

*To learn more about the ID4Africa Ambassadors Program, and to apply, please visit the Ambassadors website at www.id4africa-ambassadors.org.*

*The next ID4AFRICA Annual General Meeting will be held in Marrakesh, Morocco, June 2-4, 2020*

# READY for *the* THINNEST *eDATAPAGE Challenge*

By Hervé Naullet, Paragon ID

By Hervé Naullet, Paragon ID

☐ It has been almost 20 years since the first rollout of the ICAO electronic/biometric passports. For most of these programs, the personalized data & picture of the citizen were securely printed and protected onto a paper-based datapage, and electronically stored in the contactless component located inside the cover of the passport.

Recently, a significant number of biometric passports are switching to a polycarbonate based datapage, where the citizen data and photograph are laser engraved within the polycarbonate layer. The polycarbonate (PC) material provides unique benefits, such as the ability to be a mono-bloc assembly, as well as offering advanced security features similar to those available for eID Cards, Driver Licenses or resident permit cards. Similarly, such PC assembly is a great placeholder for the contactless component and its antenna, transforming the datapage into an eDatapage.

Some specific challenges have to be addressed, starting with the negative user experience of handling a thick rigid polycarbonate eDatapage within a paper based passport booklet that was once very flexible. The other challenge is also to ensure that the eDatapage is securely attached to the booklet and that it does not separate from the cover page or from the other visa pages. It is vital that such a security sensitive travel document does not fall apart. Manufacturing eDatapages also requires a unique know-how and dedicated equipment, thus making the technology gap potentially impressive, but also threatening, because of the required investment and learning curve.

As an expert in contactless technologies for the eID and ePassport markets, Paragon ID has been working over the recent years to address these very specific challenges, with the aim of supporting national printers and smart card manufacturers involved in passport programs in their transition to such technology.

A first breakthrough is an ultra-thin and fully white contactless inlay assembly, embedding innovative inductive coupling technology based on copper wired antenna and the Infineon CoM-CL module. Nowadays, the standard thickness of available eDatapages is within on average 800µm or even above the 1000µm mark. Thanks to Paragon ID owned technology, the passport booklet would be equipped with a thin fully ICAO compliant 100% PC eDatapage, with the potential of being less than 500µm. As discussed with industry experts, a thinner eDatapage is not just about making savings on material. It also has a significant impact on the durability of the booklet itself, not forgetting that a biometric passport could suffer from severe usage conditions.




Combined with the Infineon thin module, the inlay is fully white on both sides, meaning it does not require an extra layer to whiten the assembly. By construction, the module insertion is “anti-crack” enabled, ensuring high durability even within harsh conditions. As the inlay is fully flat with almost no extra thickness within the module area, there are very limited constraints in regards to the security design. The assembly can also benefit from see-through windows enabling some more advanced security features. Overall, such an eDatapage can embed all known security capabilities should these be tactile, printed, or hologram-related features. This ultra-thin inlay can also be made available equipped with a flex and highly durable hinge. Converted into an eDatapage relying upon conventional flat press technology, the eDatapage can easily be sown together with visa pages, for a biometric passport benefiting from a great aesthetic, compared to booklets made with a thick datapage and rigid hinge. It should be noted that thanks to the specially designed hinge structure, the eDatapage is a 100% PC monobloc assembly: the eDatapage cannot be delaminated within its structure. The hinge itself can be secured enabling specific characteristics.

As mentioned above, there is no need for investment into specific hinge related equipment, as the eDatapage assembly is obtained equipped with the hinge right after the lamination process. The manufacturing of eDatapages can easily be achieved without specific additional investment or skill acquisition. It’s worth noting that the stitching of the hinge has been proven onto standard book binding equipment.

The adoption of 100% polycarbonate eDatapages, allowing for new security features, is becoming a necessity. Carefully assessing and selecting the right technology can make this transition effort significantly easier. Choosing a more flexible, thinner and more durable eDatapage to be inserted in highly secure biometric travel documents will speed up the adoption process by citizens and by security sensitive governmental authorities. ☒

*More information, contact Hervé Naullet at Paragon ID: Herve.Naullet@paragon-id.com*

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


By Markus Moesenbacher, Infineon Technologies

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

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

## Java Card™ Technology

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

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

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

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

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

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

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

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

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

## Java Card Forum

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

## Infineon SECORA™ brand – how it started

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

## SECORA™ ID is the Infineon solution allowing easy eID introduction

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

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

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

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

## The Solution components

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

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

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

## SECORA™ ID Offering

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

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

## SECORA™ ID portfolio comprises the S and X variants.

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

## Use Case Examples

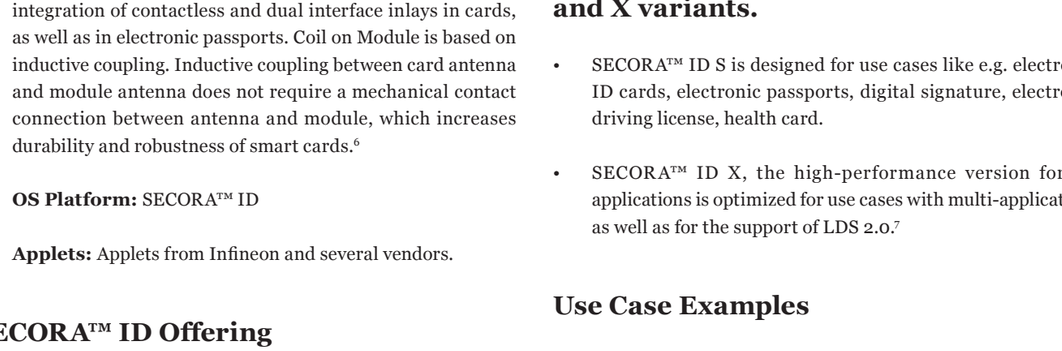
**eID (electronic Identification) with ICAO 9303 eMRTD:**

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

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

**eID with ICAO 9303 eMRTD and digital signature:**

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




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

**eDL (electronic driving license) based on ISO 18013:**

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

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

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

Requirements for this use case are as follows:

- eID card for identification and authentication, which can be extended during its life time with an e-health card application once the specification is in place.
- The ePasslet Suite by cryptovision GmbH could support this use case as this solution is optimized for multi-application. The Java Card platform allows post issuance, which is necessary to extend the functionality of the card in the field after issuance of the card.


## Conclusion

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

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

## Sources & Notes

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

MASKTECH

We make chips intelligent


MTCOS® – ID CHIP SOLUTIONS
FOR eGOVERNMENT APPLICATIONS

- High Security Operating System (MTCOS®), e.g. ePassports, eIDs, eHealth cards
- Independent worldwide supplier
- More than 65 eID-document references
- Up to EAL5+ Common Criteria certified on a unique variety of chip platforms

SecurITy made in Germany

Common Criteria

MaskTech GmbH • Nordostpark 45 • 90411 Nuernberg • Germany • sales@masktech.de • www.masktech.de • +49(0) 911 95 51 49 0



# ONLINE and *beyond* – what's *NEXT* for *the delivery* of CITIZEN services?

By Arnaud De La Chapelle, VFS Global

Customers today expect their needs will be met in a fast, frictionless manner. The likes of tech leaders such the FAANG companies (Facebook, Amazon, Apple, Netflix and Google) are showing the way, competing to deliver faster, cheaper and more user-friendly services – on-demand, anywhere, anytime – which means that in this customer-centric, connected world, the bar has never been set higher. Customers now expect the same sort of service in their interactions with the public sector too.

Recognising this need, governments are actively assessing how they can reform existing citizen services, while staying within budget controls. For example, currently, public services regularly require manual forms that have to be printed and mailed, rather than offer an end-to-end online experience where it is possible to do so, including for payments. The same goes for working hours at public offices which are often limited, with customers having to visit personally for every requirement.

Just like in the private sector, citizens are increasingly demanding more user-friendly services in the government sector too. A report by the McKinsey Center for Government, for example, which surveyed 17,000 US citizens looking at their experience with state service points in the US, found that satisfaction with private sector services was two and a half times higher than that for public services. Participants expressed negative feelings about the complexity of processes, the slow speed of service, and the effort required to navigate through processes. Those surveyed said they cared most about speed, simplicity, and efficiency – key elements of the interaction "process" with government – over all other aspects of their service experience.

This is not the best case scenario for the public sector. Delivering services to citizens is central to what governments, and their agencies, do. The most palpable interactions people have with their governments are for duties such as paying tax, renewing driving licenses, or applying for benefits. High quality services are therefore vital in engendering trust in the public sector.

The problem is that governments generally think about what they want from a service and how best to make it work for their processes, rather than what their customers are looking for and what they find easiest. As the McKinsey report outlined, government agencies tend to focus on individual 'touchpoints' in their interactions with citizens (for example, accepting an application), rather than considering a citizen's end-to-end journey through a process (such as obtaining a license). The report found that those agencies that managed the entire end-to-end journey achieved higher levels of customer satisfaction. They also developed more effective ways to collaborate internally across functions and levels to deliver their services.

Indeed, a good starting point for governments is to think of the basic premise that it all starts with customers' identity. Enabling individuals to create identity will enhance the opportunities at a later stage to realise cross-collaboration across different functions.

I recently spoke at the fifth annual International e-Governance Conference, held in Estonia. The setting could not have been more appropriate, given the huge strides that the Estonian government has made in citizen services. Estonia is probably the only country in the world where 99% of the public services are available online 24/7 – in fact, the only things where e-services are not in place are for marriages, divorces and real-estate transactions.

But the Estonian thought process was not to go 'digital for digital's sake' – another trap governments often fall into. Estonia first introduced an e-tax declaration, offering a better way of doing taxes that the citizen was keen to adopt, rather than government.

Now, its citizen services have expanded to the point where Estonians can vote via their laptops. They can appeal against parking tickets online. Rather than people having to input data time and time again, it follows a 'once and once-only' policy; if they're applying for a loan, for example, information is obtained from elsewhere in the system. They don't have to fill out forms at the surgery as doctors can access patient records online.

Health data held online can often "frighten the horses". The key to a good identity – and crucial to engendering trust among citizens – is a robust database with security safeguards. For Estonia, a central principle is that the individual is the owner of their own information and the country doesn't hold any data centrally – instead, its 'X-Road' system connects individual servers through encrypted pathways, storing information locally (again, that key point of thinking about cross-collaboration). A medical practice will hold its own data, as will a tax office. When a user requests a piece of information, it is delivered by a process that has been described as via a series of locks on a canal. Even a record that's accessible to medical specialists can be restricted from another doctor's view if that person doesn't want it seen. And every time a state employee looks at a person's secure data, it is recorded online, as accessing data for no reason is a criminal offence.

As Arthur Mickoleit, an analyst at Gartner who specializes in digital government, has pointed out, Estonia got the foundations right early in the process. This included digitising registers held by public bodies to provide the necessary information to support e-services, building the X-Road platform, and giving citizens the means to securely access online services by providing digital ID cards and making digital signatures equivalent to handwritten signatures.

As a result, Estonia has reached an unprecedented level of transparency in governance and built broad trust in its digital society, saving over 1,400 years of working time annually.

It's also vital to realise that 'online only' and going digital for digital's sake does not necessarily work for everyone, such as older citizens, those with disabilities, or those with poor internet connectivity.

That's why in Oman, the Ministry of Regional Municipalities introduced the 'Injaz Hall' (injaz means achievement in Arabic), a one-stop-shop for municipal services, housing all such services across 44 regions under one roof. Applications and approval processes (for car licences, shop licences, building permits and more) were streamlined and standardized. Since implementation, the average approval for each application has been reduced from 30 working days to 5 working days (a circa 83% reduction in processing time). Furthermore, the revenue collected from municipal services also increased dramatically: at the end of July 2012, the collected amount was about 7 million OMR (US$18 million), about 15 times the amount collected in 2008. Because of these achievements, Injaz Hall received the global UN Public Service Award for improving the delivery of public services.

At VFS Global, we have been managing similar high-volume large-scale identity and citizen programmes for governments of South Africa, India, the United Arab Emirates, and several African countries. Programmes include in-country passport services, foreigner registration, driving licenses, birth certificates, a range of civic permits, licenses and registrations, across a range of one-stop-shop, front office, digital and door-to-door services.

We recently worked with the Delhi government on its 'home delivery of public services' scheme, believed to be the first time a government has launched such a programme. Under the scheme, Delhiites can register or apply for 40 services — including learners and permanent driving licences, transfer of ownership of vehicle and change in address, new water connections, new ration cards and their disabled pension, among others — without standing in long queues at government offices. Citizens are able to contact a call centre number, available 24 hours a day, 7 days a week, to enquire about what documents they need to register for a service. A facilitator then visits the person's home (between 9am and 9pm seven days a week) to help fill in application forms and take any biometric data. The application is then transferred electronically to the relevant department. Launching the scheme, the government compared it to as easy as ordering a pizza. The scheme also serves the needs of those less mobile or able to use online channels as easily, such as the elderly or disabled.

In the UAE, on behalf of the Ministry of Health and Prevention, VFS Global has set up and manages Medical Examination Centers for Residency Visa purposes in Dubai.In February and April of 2018, two state-of- the-art Medical Examination Centres were launched enabling resident expatriates to complete their mandatory health checks for their residency visas. The centres deliver seamless medical testing services for 12 hours a day, 6 days a week, and deliver test reports in 48 hours turnaround time, with the option of receiving test results via email or SMS. Customers are also provided with professional call centre and email support and a dedicated information website for end-to- end details on fees, services and booking an appointment.

Indeed, one-stop-shops combining the best of online delivery, such as multichannel options, together with in-person contact, tend to be the most successful, as a report for the World Bank found. It reported that, although there are different models of these kinds of one-stop-shops adopted worldwide, the best includes four common features: access, personalization, speed, and interaction. Increasing access means supplementing bricks-and-mortar centres with electronic and mobile services; personalization refers to providing information based on citizens interests and needs; speed concerns reducing transaction times and involves re-engineering and simplifying processes and procedures; while interaction refers to engaging citizens, from receiving feedback from citizens to engaging them as co-creators of one-stop-shops.

Governments that leverage this customer service mindset, offer multiple channels of service delivery and focus on service quality are most likely to achieve this – exactly the sort of mindset employed by the tech leaders that have set that bar where it is today. ☒

# EMBRACING System-on-Card *TECHNOLOGY*

## Smart payments are driving acceptance of system-on-card but security is still paramount

By Steve Atkins, The Silicon Trust

With the rising acceptance of smart and contactless payments, there is a growing popularity for 'system-on-cards' (e.g. with integrated biometric authentication functionality), as well as IoT payments that focus on wearable payment accessories. This growth of digital payments also requires enhanced security, through encryption and tokenization for cards and additional form factors.

The trends are heightening the need for security and performance, especially in a multi-application context. As popular payment methods extend beyond cash and smart cards towards contactless and mobile form factors, hardware-based security mechanisms featuring embedded Secure Elements (eSE) will become increasingly important. These Secure Elements will protect the huge data streams flowing from digital and IoT transactions, safe-guard payment transactions, and protect the identity and integrity of end users.

In this new and complex multi-channel environment, hardware-based IoT security capabilities have to be built into each application layer, to ensure that users do not have to worry about fraud or theft of their identity.

Companies engaging within these smart payment eco-systems must ensure the necessary contactless performance in terms of card robustness, flexibility and endurance, while mastering the full ecosystem spanning IC's, inlays, packages, approved payment applets and personalization. They must also deliver hardware-based security capabilities to protect payment data in complex multi-channel environments, as well as supporting multiple international and national standards - both proprietary and open.

Payments are going digital – with today's users expecting a fast, convenient and often contactless experience with the option of using different form factors. In fact, contactless payment cards and "tap and go" transactions using cards, wearables or mobile devices are increasingly replacing cash and contact-based transactions.

### Wearables in focus

The overwhelming success of contactless cards is driving demand for wearable payments. Gartner forecasts that wearable form factors are set to rise dramatically in popularity, with global sales projected to grow from around 310 million devices in 2017 to over 500 million by 2021. Many experts have earmarked payment as the "killer app" for wearables.

According to a Mastercard press release, over 175 million Europeans are interested in paying with wearable devices. This press release states that almost one quarter of all Europeans expect to start using "tap and go" contactless wearables, such as smart watches, bracelets and key rings for everyday expenses. ☒




# 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 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

infineon

# A *new* GERMAN *security* architecture for NEXT *GENERATION* ID and IoT *requirements*

By Markus Hoffmeister & Klaus Schmeh, cryptovision GmbH

The Cryptographic Service Provider (CSP) module, based on an architecture developed by governmental cyber security experts in Germany, is an innovative and effective approach to implementing cryptographic security functions across a diverse array of sensitive applications. It takes security development to a new level, by enabling smooth implementations and evaluation for systems integrators, thus making a complex process more efficient. This new approach is not only used for secure IoT designs, but also for electronic ID applications.

## Adding a new layer for faster, more efficient security development

Separating the cryptographic functionality from the application is a mature and proven security concept. The CSP module, a new solution which is based on an architecture developed in Germany by the Federal Office for Information Security (BSI) and specified by the standards BSI TR-03151 and BSI TR-03153, implements this concept in a new fashion.

The CSP module stores the cryptographic keys along with the basic crypto functions in an embedded Secure Element (eSE). Contrary to conventional crypto-module designs, the CSP module adds an additional software layer inside the eSE, that provides functionality on a more application-oriented level. The application has no direct access to the basic crypto functions, but calls the application-oriented routines instead.

*The separation provided by this additional layer allows for higher security levels to be reached through software-only implementation.*

With this additional layer, it is especially convenient to deploy the eSE in security applications. Compared to conventional architectures, an integration based on a CSP module is faster and less prone to faults, as it requires less cryptographic expert knowledge. Moreover, the separation provided by this additional layer allows for higher security levels to be reached through software-only implementation. This is because evaluating an application based on a CSP module according to Common Criteria or similar standards is easier than with other designs: the CSP hardware module can be certified up to, for example, CC EAL4+ or higher, whereas the application software layer on the eSE normally requires only a lower level. In practice, this means that the certification process can be accelerated.

## The first implementation “Made in Germany” – cryptovision’s Jacolyn CSP

In the first large-scale German implementation, the CSP module is currently required in the Technische Sicherheitseinrichtung (TSE), a new high security solution legally required from January 2020 to prevent tax-fraud at the POS. This application is economically and politically of high strategic relevance, as it will help to prevent tax fraud, which is costing the German state hundreds of millions of Euros per year.

cryptovision’s Jacolyn CSP is used in different offerings by Bundesdruckerei GmbH, such as removable hardware tokens and to secure a cloud-based solution developed by Bundesdruckerei and Deutsche Fiskal.

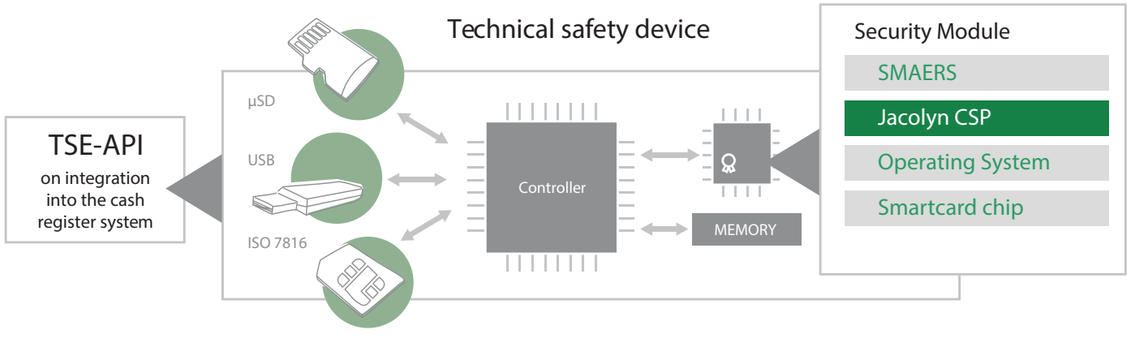
However, the cryptovision CSP module can be implemented in many more security scenarios. For instance, it provides the means to cryptographically protect a wide range of security-critical Internet of Things (IoT) devices. It is especially attractive for IoT components with medium (e.g., wearables, smart homes) to high security (e.g. smart grids, banking) requirements.

## Basis for next generation eID documents and applications

The CSP architecture was developed with a new eID document generation in mind. With the possibilities provided by new chip platforms, eID card applications can be developed, certified and brought to market in a more efficient manner. Among the applications that can be implemented in the additional layer are protocol handlers for eID protocols, such as EAC and PACE. The eID solution provider receives a solution that provides all the functionality and the security certifications necessary to easily integrate it into an eID system.

Looking beyond the card itself, utilizing hardware with a CSP module architecture is an attractive solution when designing eID usage schemes. For example, eVoting machines with CSP modules could easily be used to both check the legitimacy of the document holder to vote, as well as securely record the vote in a private fashion.

A similar scheme might be used for electronic passports, where automated kiosks with CSP modules could validate the identity of the passport holder at check in, automated border control gates with CSPs could be used to facilitate customs and immigration checks, and even the final boarding at the gates could be unattended and counted by gates with CSPs ☒








## CSP Use Case Example: Fair play at the checkout

Electronic cash register systems usually store all transaction data they process on an integrated hard drive. The operator of such a device – typically a retailer, restaurateur, taxi driver etc. – later forwards these data to the financial authority for tax checks.

However, with some IT expertise it is possible to manipulate the data stored in a cash register. A skilled operator can easily seize this vulnerability to evade taxes and social security contributions.

In order to prevent this kind of tax fraud, some electronic cash registers are protected with physical means and encryption. As the operators of cash registers usually have little interest in implementing such security measures, many states require them to do so by law (this is referred to as “fiscalisation”). In Germany, for instance, the legislator stipulates that electronic cash registers must be equipped with a so-called “Technical Security Device (TSE)” from January 1st, 2020 onwards.

The mandatory use of a TSE in Germany is laid down in a legal directive titled “Kassensicherungsverordnung” (Cash Register Protection Directive), abbreviated as KassenSichV. Fiscalisation according to the KassenSichV affects many industries, including retailers, supermarkets, gastronomy, and POS system operators.

According to the KassenSichV, an electronic cash register must record every business transaction that happens on a non-volatile storage medium. Among other things, the time, the nature of the operation, the method of payment, and the serial number of the electronic recording system need to be electronically signed and written into a record file. Accounting programs and ERP systems are required to log similar data.

With its partner and shareholder Bundesdruckerei GmbH, cryptovision offers an advanced TSE implementation based on its Jacolyn CSP. The CSP will be used in both solutions offered by Bundesdruckerei for the fiscalisation market: A local, token-based offering, as well as a cloud-based solution. It is expected that both of these fiscalisation solutions will find wide-spread use after January 1st, when the KassenSichV enters into force.


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!

www.cryptovision.com

Meet us @

**Omnisecure**
Berlin
20 – 22 January

**Mindshare 2020**
Gelsenkirchen
19 – 20 May

**Identity Week / SDW**
London
9 – 11 June
Booth #S23

**6th ID4Africa Annual Meeting**
Marrakesh
2 – 4 June
Booth #C26




# *Comprehensive* GOVERNMENT Solutions *for* the *REPUBLIC* of FIJI:

## Mühlbauer Implements New Passport Solution

By Lara Schmaus, Mühlbauer ID Services

As a part of its major project to modernize the country's security infrastructure, the Government of the Republic of Fiji decided to evolve its next generation of passports to ePassports. The current passport is a machine-readable document with paper data page, without chip and without digital photo, signature and fingerprints – a fact which has increased concerns regarding the document's security and integrity.

With the experience of numerous, successfully realized projects in the past decades, Mühlbauer was selected to handle and implement a customized, up-to-date, highly-secure solution for the personalization and issuance of state-of-the-art ePassports.

Suva, September 2019: Prime Minister Bainimarama at the official launch of the new Fijian e-Passports

### The Project Scope

The project comprises the specification, customization, delivery and installation of the necessary IT and security infrastructure (hard- and software) for the personalization (printing) and issuance of four types of ePassports (Ordinary ePassport, Official ePassport, Emergency ePassport & Diplomatic ePassport).

Furthermore, Mühlbauer provided services such as consulting, and comprehensive know-how transfer by conducting valuable trainings for the local staff of the Fijian Department of Immigration (DOI). The company provides production support, service and maintenance as well. The project's key cornerstones


*"The launch of new e-Passports will bring about benefits to all our citizens, both at home and those travelling abroad, as they will consolidate security requirements at our own borders and ease travel at ports of entry around the globe*

were the effective change management and accompanying system ramp-up support. Furthermore, Mühlbauer integrated the existing infrastructure of the Republic of Fiji's Border Management System (BMS) into the new ePassport system. This sophisticated consolidation of both systems generates excellent synergies and subsequently increases the security in a very efficient manner.

## Successful Implementation of Mühlbauer Systems

Mühlbauer delivered the first ePassports in a record time of only 12 weeks upon design release. After the successful factory acceptance test (FAT) at the Mühlbauer headquarters in Germany at the end of July 2019, integration tests were conducted and the equipment was shipped to the Republic of Fiji, where the installation at the customer's site took place and the solution was successfully put into operation in the beginning of September 2019.

## Secure Identity Documents for all Citizens

The new Fijian e-Passports contain a new range of sophisticated security features that will make it much more difficult for people to enter the country illegally, and thus establish a more secure border control process, which in turn brings greater integrity to the country's immigration system. "The launch of new e-Passports will bring about benefits to all our citizens, both at home and those travelling abroad, as they will consolidate security requirements at our own borders and ease travel at ports of entry around the globe," highlighted Hon. Prime Minister Voreqe Bainimarama while launching the new e-Passports in the Fijian capital Suva.


All in all, this marks an ideal starting point for the future issuance of modern and secure ePassports. The republic of Fiji is taking the next step to a sweeping digital government transformation that will touch all corners of Fijian society and secure the country's borders. ☒


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

# Software *Licensing* *in* the *CLOUD*: *FLEXIBILITY* is KING


By David Paine, Wibu-Systems

☐ Does a day go by now when you don't hear a reference to the term "Cloud" computing? For all intents and purposes, the "Cloud" is ubiquitous, the universal enabler behind everything, from our personalized music streaming services, to the next IoT invention that allows us to control something remotely with voice commands, all from the comfort of our own living room. Beyond consumer comforts, you hear about the Cloud most everywhere in the business and industrial world as well – with terms like software as a service, platform as a service, and data storage and access in the Cloud to name just a few.

It's more of the same in the software licensing world as well. Cloud computing affords a high level of scalability, flexibility and elasticity that has made a dramatic impact to the way ISVs can license software. Most consumers now fully embrace the new licensing models enabled by the Cloud, like on-demand, pay-per-use, and other short-range, consumption-based approaches.

In this article, we'll delve deeper into Cloud licensing, but before going down that path, perhaps it would be helpful to re-trace the origins of Cloud computing and agree upon a definition that will help make sense in the software licensing world, at least for the purposes of this article.

## Cloud Computing: Where did it begin?

The term Cloud was used to refer to platforms for distributed computing as early as 1993; today it is generally used to describe data centers available to many users over the Internet, perhaps best personified by the introduction of Amazon's Web Services in 2006. Ten years prior, a group of technologists at Compaq discussed software and file access in the web via their term Cloud computing-enabled applications. Others believe that the earliest instance of Cloud computing was invented by Joseph Licklider in the 1960s with his work on ARPANET to connect people and data from anywhere at any time, which was considered to be the pre-curser to the Internet. Soon thereafter, the Cloud symbol appeared to represent Internet-based networks of computing equipment in almost every network diagram.

But is there one universally accepted definition for the Cloud? Wikipedia defines Cloud computing as the "on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user." In other Web searches, you might find definitions like "the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer".

Or perhaps an even broader and simpler definition: "Cloud computing is a general term for anything that involves delivering hosted services over the Internet." This description has given rise to the use of the term Cloud computing by vendors in the broadest of terms and caused some level of confusion as to whether an application is truly Cloud based or not.

For our purposes here, let's just say that Cloud computing is the "processing of data by a remote device" to make the definition as broad as possible.

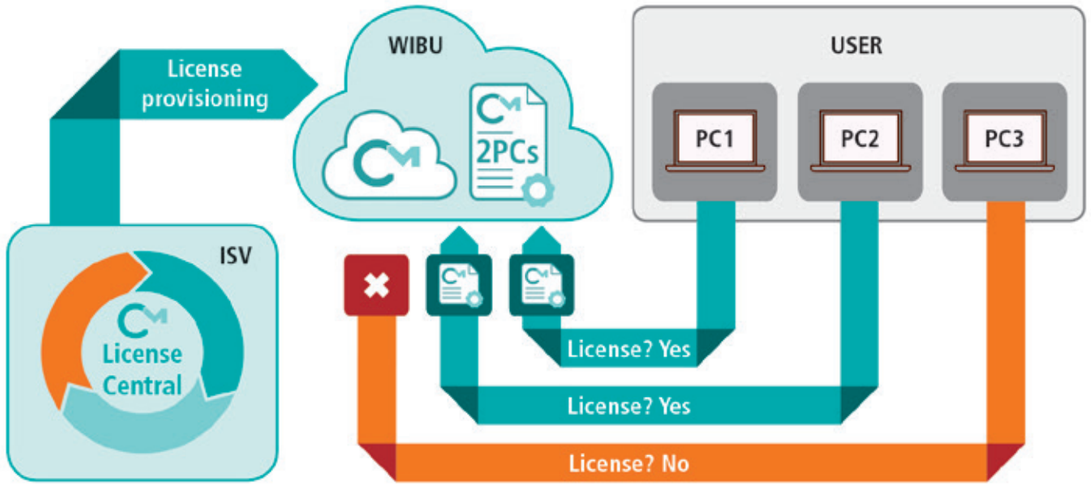
Now, let's take a look at the many options that can exist for Cloud licensing.

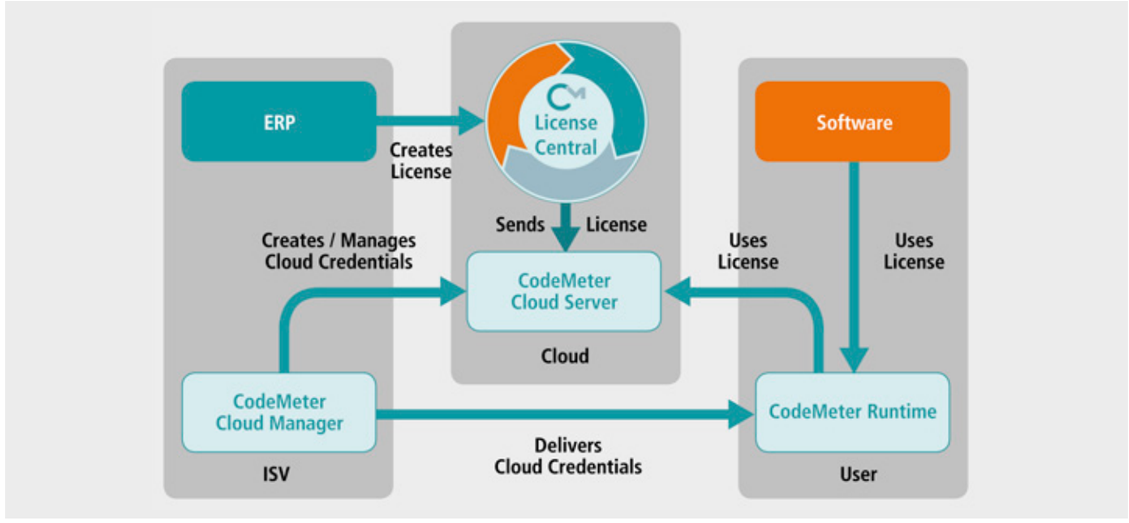
**Cloud Licenses for Local Applications:**
Software developers want to enable their users to access local software with a license kept in the Cloud.

In this case, the software is a classic desktop application, which the ISV sells to users and delivers on a traditional CD or as a download. The user receives not only the software itself, but also an activation code in the form of a ticket that is created by the License Management System, in this scenario, CodeMeter License Central. When creating the ticket, the ISV can determine how many devices the software can operate on at the same time and for how long it can be used without a permanent connection to the Internet. Within this scenario, the process is flexible enough so that the user can continue to work with the software even after reaching the maximum number of devices, and transparent enough for the ISV to uncover fraudulent use and take the necessary countermeasures.

**Cloud Licenses for SaaS Applications:**
Software developers supply their users with SaaS solutions operated in the Cloud. The required licenses might be tied to a single user or a given number of devices.
ISVs can offer users a SaaS application with unrestricted or temporary licenses for different features. The licenses for SaaS applications are created in the same manner that is used for on-premise licenses; they only differ in the binding scheme.

**Authentication for SaaS Applications:**
ISVs provide their users with a reliable means of authentication for using their SaaS applications, using private keys kept in local licenses, stored securely on a dongle or computer binding.
In this scenario, the SaaS software creates a challenge that the local application responds to by signing it with the private key kept in the local license. Up in the Cloud, the SaaS application user's




the public key to verify the identity of the user, with the users' identities managed and recorded in the Cloud according to your specific needs.

**Standard Applications in Private Clouds:**
Users might want to install and run software independently on their own private Clouds.

A private Cloud would typically be a farm of virtual machines operated in a company's own data center or at a specialized provider on other hardware known neither to you nor to the user.

## License Provisioning in the Cloud: Hypothetical Use Case

To describe a common license provisioning process in the Cloud, let's look at a hypothetical example with a fictional ISV called Aardvark Technologies and their customer, Wombat, Inc. The software purchased by Wombat needs to be licensed properly to ensure its legitimate use, to protect both the ISV's revenue and the customer against usage audits. Aardvark places the software on their website where Wombat can download it. Aardvark uses the CodeMeter License Central licensing system from Wibu-Systems to manage its provisioning capabilities in the Cloud. Aardvark takes the process a step further by encrypting its software with CodeMeter, which protects the software from illegal copying or reverse engineering, because only those with the proper license key can decrypt and use the software.

Upon download of the software, Wombat has several licensing options available and all can be managed via Cloud licensing:

- Wombat Inc. might decide that they are best served with soft licensing since they know that the software will only be run on a specific computer and nowhere else. In that case, Aardvark Technologies would request a fingerprint file that Wombat Inc. can easily generate using a special tool that has been integrated into the software. Using this file, Aardvark Technologies can create a license file for Wombat Inc. to install: this can be installed in seconds and grants entitlement to use the software.

- Wombat Inc. might decide they need more flexibility, wanting to purchase a single license that can be used on various machines. Aardvark can provide Wombat customer with a special USB dongle that would be required for the software to operate on each machine and can only be physically attached to one computer at a time, preserving the license integrity. This then provides a clear path to the stated requirement, since the dongle can only be physically plugged into one computer at a time.

These two examples illustrate the use of license provisioning in the Cloud. Aardvark Technologies can choose to host CodeMeter License Central on their own servers (private Cloud) or to have it professionally hosted by Wibu-Systems itself. Though this latter approach may be considered a public Cloud, the reality is that they have exclusive access to their own instance of the service, so it doesn't have to be a public Cloud where multiple users are hosted on the same site. This approach provides yet another level of security.

This form of Cloud provisioning offers great flexibility to the ISV, as no special software needs to be installed by the ISV in order to achieve their licensing goals.

## Licenses in the Cloud: More Flexibility

Here are some additional use cases where Cloud licenses come into play and provide needed flexibility to address even the most complicated licensing scenarios.

**Let's Play:** Peter is sitting at home playing on his own favorite computer game, "Beam Me Up", when his best friend Simon calls him on his mobile and asks if they could play the game together at Simon's house. Peter heads over to Simon's house and they sit at Simon's computer. Because "Beam Me Up" is licensed in the Cloud, Peter is able to log in to his account, download his license, and continue to play the game, this time in two-player mode with Simon.

**Cad-Me-Up:** Wolfgang is an architect who travels frequently with his job. Half of the time he sits in his office working on his desktop computer using an expensive CAD package, Cad-me-up; the rest of the time, he needs to be at a customer site presenting his work on his laptop. The software is too expensive to purchase two licenses, but this is ok, because the license is stored in the Cloud and Wolfgang is able to run the license on either machine under a single user license.

**Flexi-Licensing:** Let's go back to Wombat Inc: They have many consultants working for them, who frequently work remotely from customer sites. George and Roger are two such consultants, both visiting their clients on the same day. On one particular day, George finds that he needs to use a rather expensive piece of software. Both he and Roger have it installed on their laptops but Wombat only purchased a single license for the software due to the prohibitive cost. George calls Roger to confirm that Roger does not need the software on that particular day. George is able to run the software using the single license that Wombat Inc. has purchased and is therefore entitled to use. If Roger subsequently tried to use the software, he would be automatically informed that the single license was already in use. It would then be possible for Wombat Inc. to purchase a second license (that Roger would then be able to use immediately), if the business case justified it, or transfer the license to Roger when George completes his work.

All of these scenarios are made possible because the license itself is stored and can be provisioned in the Cloud. Together with a license server operated in the Cloud, Cloud licensing provides a great deal of flexibility for ISVs to meet the unique needs of each customer, by unveiling a host of new licensing scenarios and business models. ☒

# *Transforming* TOKENS and *SMART* Cards *into* universal SECURITY *Instruments*

By Viacheslav Tatianin, AVTOR LLC


SmartCard-338

SecureToken-338

Digital technologies now proliferate all dimensions of modern business and social life, meaning that rooted IT security is now a 'must-have' principle for big corporations, government agencies, and SMEs. The digital shift we have been part of has reinforced the need for the application of high-security tools – even for common cases.

AVTOR is a Ukrainian vendor; one of the first integrators of cybersecurity solutions in public and corporate sectors and has an extensive portfolio of successful projects with financial institutions, energy and infrastructure. The cumulative knowledge in IT security and defense that it has accrued since 1994, has allowed AVTOR to produce high-quality software and hardware solutions that can be adapted to individual client's needs.

The flagship solutions of our company are hardware and software solutions in the field of cryptographic protection of information, data transfer security, an in-house developed Public Key Infrastructure system, secure special telecommunication, electronic signing solutions, access control and many others.

The core of the AVTOR's security solutions is smart card technology empowered by "UkrCOS®", our own smart card operating system. Smart card solutions have opened a broad range of possibilities for securing systems from SCADA level to value chains in a secure and efficient way. In this narrow niche, we offer solutions in different form factors and interfaces, such as:

- Smart cards CryptoCard-338;
- USB SecureToken-338;
- MicroSD with a smart chip.

CryptoCard and SecureToken are designed for authorization control, electronic document flow, authentication of users and secure storing of keys, and the MicroSD secures financial transactions.

These previously mentioned solutions are developed on highly secure smart chips from global leading vendors – specifically Infineon Technologies.

For that reason, AVTOR's solutions have three levels of security:

1. Technological – based on the technology of smart chip production;
2. Hardware – based on the security of the smart chip;
3. Software – based on the "UkrCOS®" operating system.

Our Operating System "UkrCOS®" is a unique solution and a source of corporate pride.It was fully developed by AVTOR, and is now being used in all company solutions. The main feature of the "UkrCOS®" is the simultaneous data transfer management, memory distribution for data processing, and secure operation of all applications.

"UkrCOS®" empowers the hardware security devices to become a universal instrument in securing transactions, access control, authentication, qualified digital signing etc. Universality and highly secure reliability of AVTOR's solutions have made it become a leading vendor in Ukrainian market, with a permanently growing client base.

At the same time, AVTOR's presence is now being felt beyond the Ukrainian market. The strategic goal of the company is the development of new solutions adapted and certified for penetration into the global market of cybersecurity. ☒

*For further information please visit www.avtor.ua*

# 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®

**Please visit us at: TRUSTECH** · Cannes, France · Booth: RIV A054 | **HSP EMEA** · Lisbon, Portugal | **ICAO TRIP** · Montreal, Canada · Booth: 50

more ▷

**www.melzergmbh.com**


# SILICON TRUST DIRECTORY 2019

## THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

The Silicon Trust is a well-established marketing program for smart card solutions with high visibility in the worldwide government and identification (ID) markets. With over 30 companies along the value chain, the Silicon Trust forms a strong community of like-minded companies.

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

- Educating government decision makers about technical possibilities of ID systems and solutions
- Development and implementation of marketing material and educational events
- Bringing together leading players from the public and private sectors with industry and government decision makers
- Identifying the latest ID projects, programs and technical trends

## EXECUTIVE COUNCIL

**The Executive Council has been the steering committee of the Silicon Trust since 2008. It drives the Silicon Trust by defining the topics and directions of the program's publications, workshops and meetings.**

### INFINEON TECHNOLOGIES

Infineon Technologies AG is a world leader in semiconductors. Infineon offers products and system solutions addressing three central challenges to modern society: energy efficiency, mobility, and security. In the 2016 fiscal year (ending September 30), the company reported sales of Euro 6,5 billion with about 36,000 employees worldwide. Infineon is the world's leading vendor of secure chip card ICs used for passports, ID cards, payment cards, mobile subscriber authentication (SIM cards), access cards and trusted-computing solutions as well as being a technology driver in the hardware-based security field.
**www.infineon.com**

## ADVISORY BOARD

**The Silicon Trust Advisory Board supports the Executive Council in defining the direction of the program in terms of public policy and scientific relevance.**

### BSI

Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security. It has been established in 1991 as a high level federal public agency within the area of responsibility of the Ministry of the Interior. The BSI's ultimate ambition is the protection of information and communication.
Especially in the area of smart card technology, BSI is responsible for the design and definition of secure solution requirements for governmental identification documents. The German ePassport has been introduced in 2005, the second ePassport generation followed 2007, and starting in 2010 the all-new German eID card has opened a new trustworthy approach to Internet authentication for all German citizens. Security of all these documents is based on BSI specifications, developed in close collaboration with European/international standardization bodies and leading industry partners.
**www.bsi.bund.de**

### FRAUNHOFER AISEC

Fraunhofer AISEC supports firms from all industries and service sectors in securing their systems, infrastructures, products and offerings. The institution develops qualitatively high-value security technologies, which increase the reliability, trustworthiness and tamper-resistance of IT-based systems and products. The approximately 80 members of the Fraunhofer AISEC scientific and technical staff balance economic needs, user-friendliness, and security requirements to develop optimally tailored concepts and solutions.
The security test labs are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyze the security of products and hardware components as well as software products and applications. In our laboratories, functionality, interoperability and compliance are tested to give clients targeted, effective advice. Strategic partnerships with global corporations as well as with internationally recognized universities guarantee scientific excellence as well as its market-driven implementation.
**www.aisec.fraunhofer.de**

## SILICON TRUST PARTNERS

**Partners of the Silicon Trust are a vital element of the program. The partners represent all aspects of the value chain and are international representatives of the ID industry. They all share one common goal – to create awareness, to educate and to promote the need for silicon-based security technologies.**

### AdvanIDe

Advanced ID Electronics – is one of the leading silicon distributors, focused on components for RFID transponders, chip cards and RFID readers and terminals. Thanks to its optimized semiconductor supply chain, AdvanIDe can guarantee manufacturers of smart cards, RFID transponders and readers the most efficient access to the latest semiconductors.
**www.advanide.com**

### ATOS

Atos 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**

### 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/**

### 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**

### CHARISMATHICS

charismathics® has been pioneering the global identity management arena since 2005 and is offering security products and services for a variety of industries ranging from corporate to finance, from e-government to health services, from e-education to telecommunications. The company delivers PKI security solutions addressing traditional smart cards, convenient USB keys, handy soft tokens or even cutting edge mobile applications.
**www.charismathics.com**

### COGNITEC

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

### 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**

### 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**

### 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**

### 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.d**

### MELZER

With 60 years of experience MELZER has been internationally recognised and established as the leading equipment supplier for the production of the most advanced ID documents, Smart Cards, DIF Cards, RFID Inlays and e-Covers for Passports. Customized solutions, the modular machine system and the lean production approach ensure and maintain unsurpassed yield rates, flexibility and profitability. The MELZER product portfolio also includes a broad range of versatile RFID converting equipment.
**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 in order to accelerate their development and strengthen them as the leader on their market, constituting a major milestone in the life of both companies.
**www.micropross.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**

### 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**

### 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



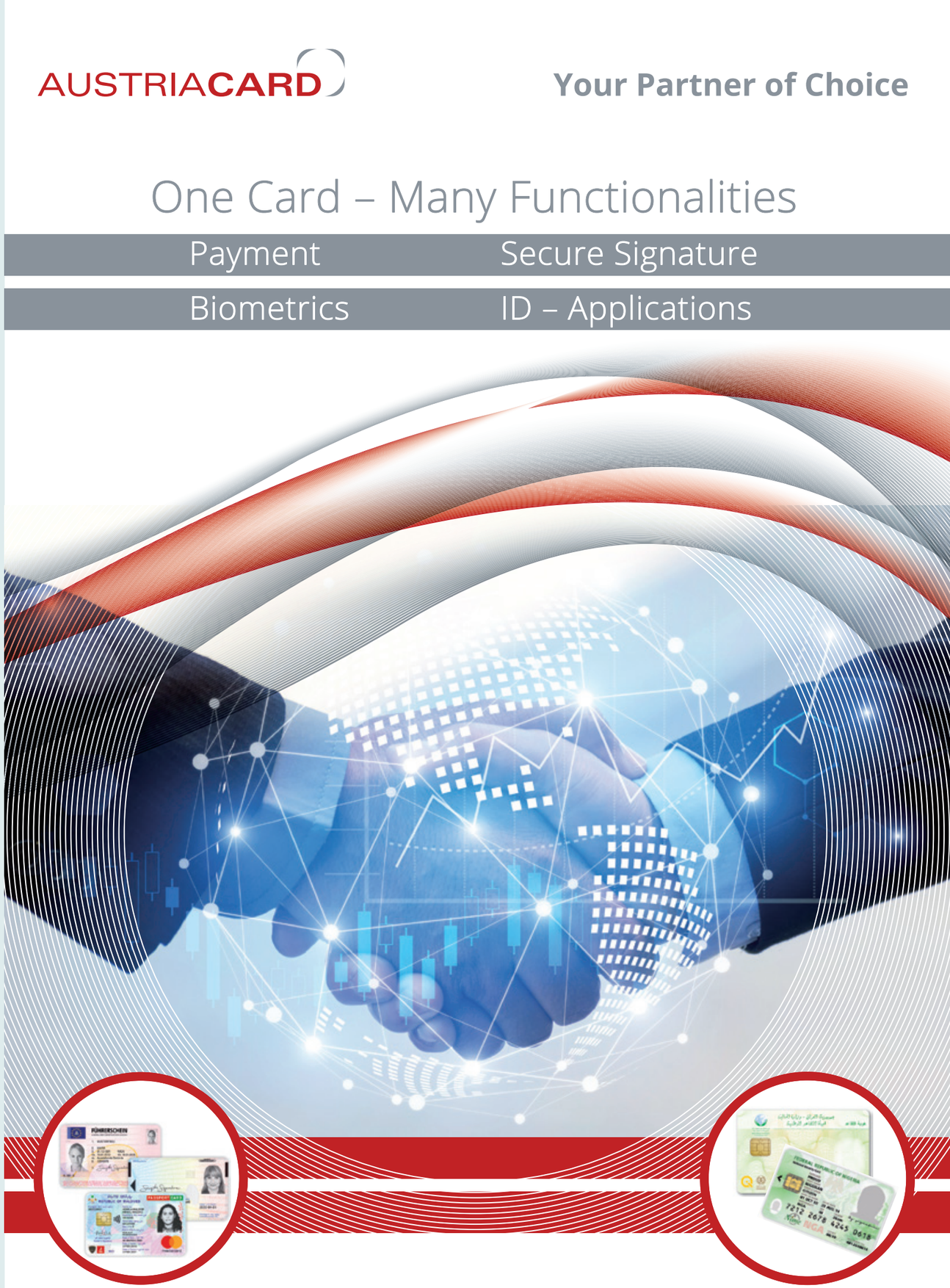
AUSTRIACARD

Your Partner of Choice

One Card – Many Functionalities

Payment | Secure Signature

Biometrics | ID – Applications



www.austriacardag.com

ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.
**www.pwpw.pl**

SMARTRAC N.V.

SMARTRAC is the leading developer, manufacturer, and supplier of RFID and NFC transponders and inlays. The company produces ready-made and customized transponders and inlays used in access control, animal identification, automated fare collection, border control, RFID-based car immobilizers, electronic product identification, industry, libraries and media management, laundry, logistics, mobile & smart media, public transport, retail, and many more. SMARTRAC was founded in 2000, went public in July 2006, and trades as a stock corporation under Dutch law with its registered headquarters in Amsterdam. The company currently employs about 4,000 employees and maintains a global research and development, production, and sales network.
**www.smartrac-group.com**

TELETRUST

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the quality seal "IT Security made in Germany" and runs the IT expert certification programs "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Engineer for System Security" (T.E.S.S.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.
**www.teletrust.de**

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.co**

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**

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**



Cognitec

# The trusted face recognition company since 2002

## Most experienced and highly trusted

Cognitec has been providing face recognition systems to government and commercial clients worldwide for almost 20 years. Proud to maintain a stable, leading position in the industry, we are committed to delivering the best solutions available on the market.

## Focused research and development

We use state-of-the-art machine learning techniques and deep learning principles to achieve continuous advancement of the various algorithms contained in our core technology.

## Reliable customer service

Cognitec's clients rely on collaborative customer service, fast response times and competent work.

## Superior technology

Our algorithms perform the most important face recognition tasks with market-leading speed and accuracy. Independent evaluation tests and real-life installations continue to prove the exceptional performance of Cognitec's technology.

## Successful projects worldwide

Alongside image database searches that prevent ID fraud and support criminal investigations, Cognitec's technology drives cutting-edge video security, eGate, people analytics, and photo indexing solutions.

www.cognitec.com | info@cognitec.com

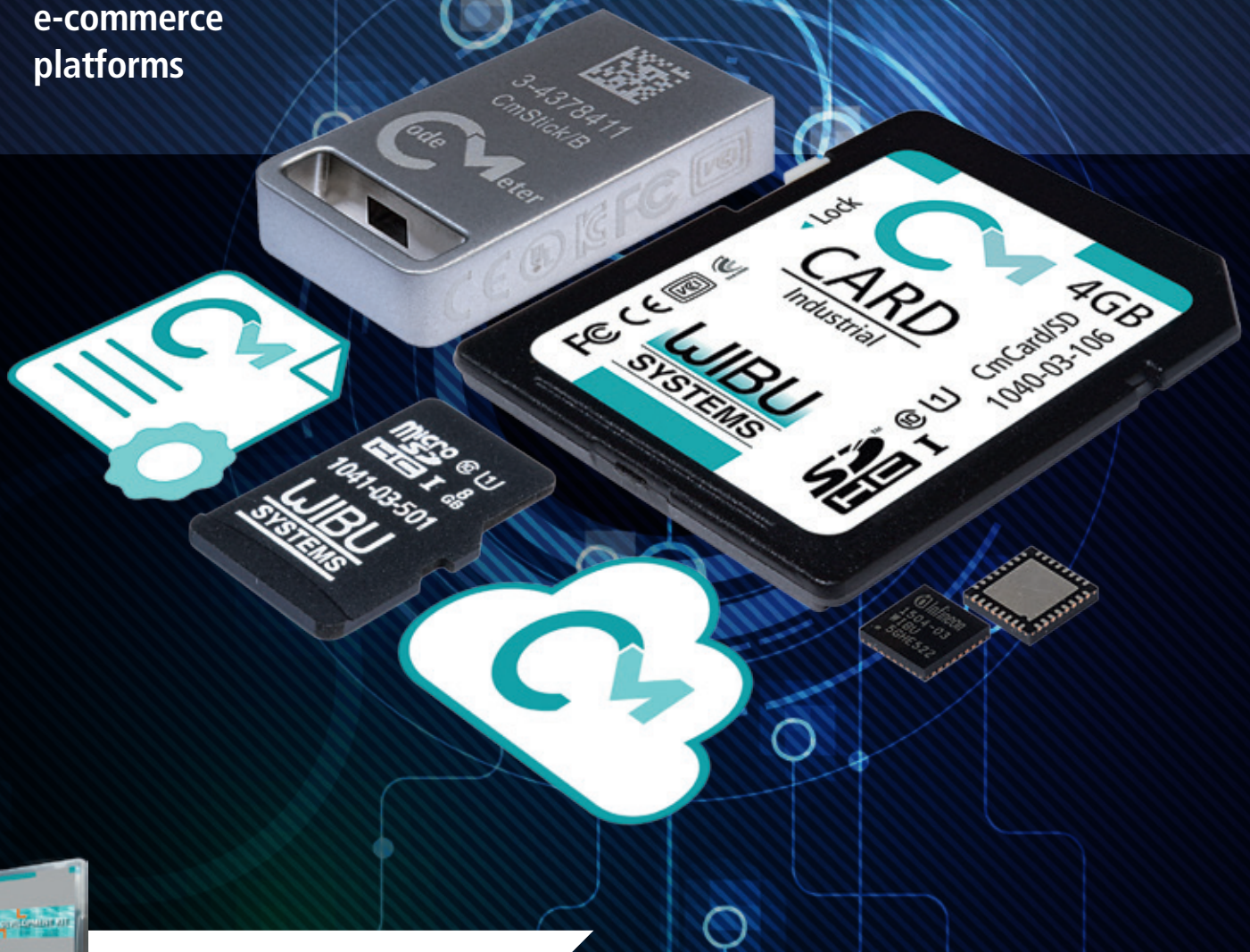
WIBU SYSTEMS

# Are you thinking of software protection?

## Think CodeMeter!

- Licenses in hardware, software, and cloud containers
- Support for x86, ARM, MIPS and PPC
- Compatibility with PCs, mobile units, embedded systems, PLCs, and microcontrollers
- Seamless interface with ERP, CRM, and e-commerce platforms

30 YEARS 1989-2019
propelling your business to new heights




Don't wait any longer
Start protecting your IP now!
s.wibu.com/sdk-cm

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

SECURITY
LICENSING
PERFECTION IN PROTECTION