

NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2018

The VAULT

The BLOCKCHAIN Issue

Infineon & Xian bring
Blockchain to the car

New hope for Post-
Quantum Cryptography

Gemalto & R3 bring
Blockchain to Digital ID

Blockchain Blues -
The end of eID Cards?



Meet us at
Riviera
J045

EAL5+ certified MTCOS[®] 2.5 on IFX, NXP, ST

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

Contents

Back-end license issuing for forward thinking customers 4

Daniela Previtali, Wibu-Systems

Infineon and XAIN to collaborate on bringing blockchain into the car 11

New hope for post-quantum cryptography 12

Robert Bach, Infineon Technologies

World's first TPM for cybersecurity in the connected car 17

Gemalto and R3 pilot blockchain technology for digital ID 18

Blockchain blues - the end of eID cards? 20

Markus Hoffmeister and Klaus Schmeh, cryptovision

PrimeKey PKI in a box – still hot after 6 years! 24

Jiannis Papadakis, PrimeKey

How a stolen connected car could threaten a whole city 26

Marjolaine Lombard, cyber security marketing consultant, ATOS

Adding identity to the internet of things to improve security and traceability 28

Orestis Mavropoulos, AUSTRIACARD

I haven't been everywhere, but it's on my list 30

John Peters, OVD Kinegram

Introducing The Silicon Trust 33

Imprint

THE VAULT

Published bi-annually by Krowne Communications GmbH, Berlin.

PUBLISHER: Krowne Communications GmbH, Steve Atkins, Sächsische Straße 6, 10707 Berlin

EDITOR-IN-CHIEF: Steve Atkins

ART DIRECTOR: Lana Petersen

PARTNER DIRECTOR: Yvonne Runge

EDITORIAL CONTRIBUTIONS: Daniela Previtali, Robert Bach, Markus Hoffmeister, Klaus Schmeh, Jiannis Papadakis, Steve Atkins, Marjolaine Lombard, Orestis Mavropoulos, John Peters

PHOTOS: WIBU SYSTEMS, INFINEON TECHNOLOGIES, ISTOCKPHOTO, AUSTRIACARD, ATOS, OVD KINEGRAM, CRYPTOVISION, PRIMEKEY, GEMALTO

PRINTING: DRUCKEREI HÄUSER KG, COLOGNE

EDITION: November 2018

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.

Back-End LICENSE Issuing for FORWARD *THINKING* Customers

By Daniela Previtali, Wibu-Systems

□ Introduction

Everyone knows about the danger of a malicious cyber-attack upon their company's data systems. While it is true that many such attacks are perpetrated upon what is commonly known as 'front-end' – that part of a software system that allows usage and interaction by an individual employee, many attacks and malicious misuse are just as focused upon the 'back-end' of such systems. These back-end systems are often part of a company's digital delivery system for their products.

Figures published by HACKMAGEDDON in their latest June 2018 report¹ show an estimated 50% plus of cyber-attacks targeting the back-end of company's data systems. Almost 85% of such attacks are credited to cyber-crime, the search for data or intent upon making money from such an attack.

But it's not just data or money that malicious actors are after. In the world of industrial espionage, the focus is to steal proprietary software or valuable IP data that resides in these 'back-end' systems. From industrial design algorithms to gaming software, there is a whole spectrum of assets that cyber criminals can profit from.

That's why there is a need for secure back-end processes that allow controlled access management to sensitive data and license issuance for software delivery: protecting the access equals protecting the assets from theft or tampering, and ultimately from considerable losses.

This sentiment was echoed by Frank Felten, Vice President of PTV Group in a recent interview² with Wibu-Systems, who said, "It's important in our markets that we ensure that our software doesn't get cracked and the IP taken without someone paying for it. The opportunity to use different license containers but all leading back into the same standardized back-end process is of high value to us."

Reducing the human element for software license issuing

However, applying access and license control to secure a company's software solutions, that are in turn accessed from a back-end infrastructure, is best done with the minimum of human interaction where possible.

This is a best practice that is embraced by many companies who are using or delivering digital products.

While there is a vital need for delivering software complete with its license, the requirement to make the actual issuing of said licenses and access to a company's software products as painless as possible is a necessary step on the road to digital product delivery. And one that performs better when integrated within the company's own back-end infrastructure.

"In our opinion, the best approach in such situations," said Oliver Winzenried, CEO and Founder, Wibu-Systems, "is to ensure that the license is not created manually, but is automatically generated by the company's back-end ordering system."

License generation solution meets SAP

In this area, Wibu-Systems has been mindful to ensure that their licensing software solutions can be fully integrated into a customer's ordering system. Probably the best known and most widely used example of a back-end ordering system is SAP; used in the majority of companies to facilitate a number of purchasing and accounting actions.

Giving an example of back-end integration into such a system, Rüdiger Kügler, Security Expert at Wibu-Systems said³, "Most of our customers are using SAP to generate their orders. In partnership with Austrian-based INFORMATICS, Wibu-Systems built a license generation solution that is integrated into SAP. An employee of the customer generates the order in SAP⁴. A connection between SAP and Wibu-Systems CodeMeter License Center creates the license in the license lifecycle system. The license travels first back to SAP as a ticket and is then delivered as an email or a printed activation code for the end user of our customers to activate the software product".

The benefits for Wibu-Systems customers who opt for incorporating CodeMeter licensing into their SAP back-end purchasing systems are clear. As the company is already using SAP, it is easy to use the Purchase Order generator in the system for the creation of the required licenses. This integration reduces costs for the generation and delivery of the required license and reduces possible human errors and subsequent support costs.

However, the integration of Wibu-Systems CodeMeter software licensing solution into a customer's back-end systems is not just bound to SAP. The company has gone to great lengths to ensure that they can integrate their license issuing services into a number of customers' back-end systems, across a variety of industries and markets.

Securing medical IP through time-base licensing – Agfa Healthcare

Wibu-Systems' secure back-end license and entitlement management system doesn't just simplify the workflow, but also adds a number of monetization capabilities, by leveraging the full versatility of CodeMeter licensing models.

For instance, Wibu-Systems implemented a solution for time-based licensing that allowed healthcare providers to use a computed radiography package powered by Agfa HealthCare's Easy Payment Scheme. The solution allows healthcare providers to pay as they go, with a fixed down-payment followed by equal and regular instalments, keeping upfront capital investment low and cost management easy.

When signing up for Agfa HealthCare's digital imaging solution, the healthcare provider gets a full digital package upfront, including all necessary equipment and software.

Through a web-based interactive portal the healthcare provider is invited to pay regular instalments. Each payment ensures the use of the system through to the next instalment date. The affordable and predictable recurring pricing model allowed Agfa HealthCare to gain new market quota, especially with small businesses and in emerging areas.

The Easy Payment Scheme is based on a payment platform, where the end user pays for regular – typically monthly or quarterly – instalments. The payment platform is linked to an encryption platform. Upon completion of the payment, a ticket can be downloaded to renew the software license, releasing the software to be used until the next instalment is due.

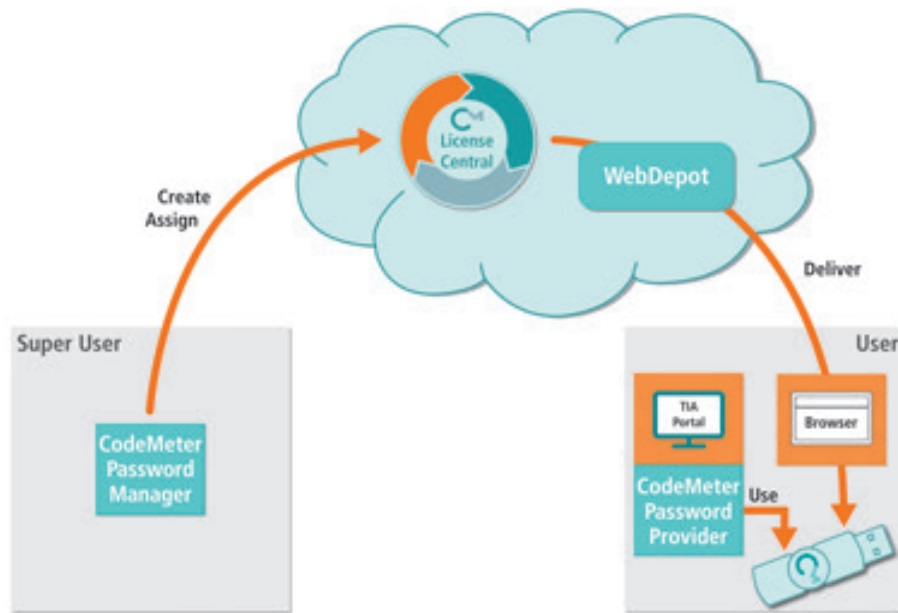
Wibu-Systems proved to be the only company capable of implementing the encryption and time-based licensing solution on Agfa HealthCare's proprietary operating system. Wibu-Systems' CodeMeter Protection Suite combines strong protection functionality with ease of use. This way, CodeMeter acts as a deterrent against the illegal and fraudulent use of Agfa HealthCare's Easy Payment Scheme. It offers Agfa HealthCare an easy way to control the use of the software and to protect its intellectual property against illegal or fraudulent use.

Integrating CodeMeter with industrial back-end systems – Siemens

The integration of access control into a customer's back-end system does not necessarily mean the integration of a singular licensing model. There is always the possibility of integrating multiple models within the back-end system in terms of both software and hardware-based licensing (such as incorporating a secure hardware or software element into the solution flow).

Industrial giant Siemens developed a Totally Integrated Automation Portal (TIA Portal[®]) that provides unrestricted access to their complete range of digitalized automation services, from digital planning and integrated engineering to transparent operation. With the TIA Portal, engineers can benefit from a shorter time-to-market thanks to innovative simulation tools, boost the productivity of their plants with additional diagnostic and energy management functions, and enjoy greater flexibility made possible with more coordinated teamwork.

Siemens customers rely on the TIA Portal to program their programmable logic controllers. To do so, they use programming languages that are compliant with the IEC 61131 standard. Part 3 of this standard relates to the use



of ladder diagrams, function block diagrams, structured text, instruction lists, and sequential function charts. The building blocks can be any one of four different types:

- OB – Organization Block
- FB – Function Block
- FC – Function
- DB – Data Block

The first three types can be password protected. A generic password protection solution is usually not strong enough by nature. By comparison, the password management solution based on CodeMeter is extremely robust.

Wibu-Systems created a back-end solution that consisted of several intertwined software and hardware elements:

- CodeMeter License Central, the cloud and database-derived solution for license lifecycle management
- CodeMeter WebDepot, the user portal for license activation
- CodeMeter Password Manager, the tool for password and entitlement management
- CodeMeter Password Provider, the interface module between CodeMeter technology and the TIA Portal
- CodeMeter Sticks, the USB hardware secure elements where passwords are stored

Wibu-Systems developed a password provider for the Siemens Totally Integrated Automation (TIA) Portal V14 SP1 or higher based on their Password API. The engineering data that are stored in the TIA Portal are often very sensitive in nature. While online teamwork is highly effective, logical access controls are paramount to make sure that only entitled users can view and edit only those projects they have full rights to.

With Siemens' Password API, Wibu-Systems created a password provider that streamlines know-how and write protection and, in turn, increases the access control and engineering data protection measures. Rather than being susceptible to disclosure, passwords could be securely stored in Wibu-Systems' CmDongles, hardware secure repositories that come in several form factors, including USB sticks (with optional flash memory), memory cards (SD, microSD, CF, and CFast type), and ASICs. Access controls by timer or unit counter govern the ability to access or edit the engineering data.

CmDongles are operated with CodeMeter, Wibu-Systems' flagship technology that incorporates state-of-the-art proprietary encryption methods based on public symmetric and asymmetric standards, like AES 256-bit, RSA 4096-bit, and ECC. Its specific password management tool is flexible enough to allow the creation and administration of passwords in accordance with the customers' requirements and secure enough to safeguard the digital identity of the TIA Portal's users. Passwords can now be transferred online or offline, conferring additional versatility to the solution.

Speaking on the subject of incorporating a Wibu-System solution into a Siemens TIA Portal, Oliver Winzenried, CEO and founder of Wibu-Systems, said, "We are obsessed with security and therefore glad to be able to offer a small, but significant building block to the TIA Portal. With our CodeMeter password management technology, manufacturers can easily manage and protect their invaluable digital know-how. The cloud-based deployment of passwords facilitated by CodeMeter License Central simplifies their distribution and assignment."

CodeMeter License Central allows the user to create, manage, and distribute their licenses. Even complex licensing models can be mapped in a quick, straightforward manner to meet customer requirements.



CodeMeter for secure licensed digital delivery and IP protection across all industries

But it doesn't stop there. Many companies are now incorporating Wibu-Systems CodeMeter solution into their back-end infrastructure to facilitate a secure digital delivery of their products. CodeMeter allows the end user to apply a comprehensive range of license models that include both traditional models like single user licenses or network licenses, as well as modern consumption and user-based license models. License models are defined through Product Codes and Product Item Options. (See Table 1)

For example, Dataton, a major player in the international infotainment industry, uses CodeMeter while monetizing software-realized features and protecting their IP invested in multi-display production and presentation systems for cultural installations and live events.

CodeMeter is also used in the automotive market by Bosch – ESI(tronic). The company uses a license-based subscription model for their diagnostic software solutions for the aftermarket workshop business, where experts provide advice, repair and maintenance services for all makes.

Conclusion

Integrating access management and license issuing into a company's back-end infrastructure or customer portals makes a lot of sense. Wibu-Systems CodeMeter can provide cybersecurity capabilities to intelligent device manufacturers who want to safeguard firmware upgrades and updates, to software publishers that need to protect their intellectual property from counterfeiting and reverse engineering, and to users who want to be sure the software they run is genuine and has not been tampered with.

Perhaps more important in terms of back-end integration, CodeMeter includes the entitlement aspect, from the creation of licenses, to their online or offline delivery, transfer, or remote management. In doing so, Wibu-Systems is supporting the migration to a dynamic industrial economy, where new license-based business models can create additional revenue and responsive pricing models for unlimited access to the market for all vendors and users. Companies don't have to manually issue a software license – it is automatically generated from their back-end infrastructure. As Frank Felten, Vice President of PTV Group commented, "Our customers are not interested in licensing, but in using our products."

A point of view, I suspect, shared by many. ☒

Sources.

¹ <https://www.hackmageddon.com/2018/07/23/june-2018-cyber-attacks-statistics/>

² <https://silicontrust.wordpress.com/2018/08/21/ptv-group-monetizing-mobility-software-on-a-global-scale/>

³ <https://silicontrust.wordpress.com/2015/05/19/video-software-protection-licensing-and-security-from-wibu-systems/>

⁴ <https://www.wibu.com/wibu-systems-webinars/webinar-lean-license-management-via-sap.html>

CODEMETER LICENSE MODELS FROM WIBU-SYSTEMS (TABLE 1)

Single User License	The license is stored on a local device or a CmDongle plugged into a local PC. The software runs on the same computer/machine.
Single User License in a Virtual Machine	The license is bound to a virtual machine. If copying the virtual machine, the license becomes invalid. If moving the virtual machine, you decide whether the license will stay valid (high availability) or become invalid.
Network License	The license is stored on a license server in the network. It is used by PCs as a floating license.
Feature-on-Demand License	Individual licenses are used to activate specific product features and modules. This allows you to generate extra turnover through the sale of add-ons.
Perpetual License	The license is issued permanently and never expires.
Demo / Trial License	The user can only access the features of your software specified by you for a limited time.
Rental, Leasing, Subscription License	You specify for how long the license is valid. CodeMeter License Central can automatically extend the validity of the license.
Pay-per-Use License	Billing is based on the number of units used. You can decide whether the billing unit is based on time or function and whether the settlement should take place before or after consumption.
License with Software Assurance	This is a perpetual license including a maintenance agreement. During the maintenance entitlement period, users have automatic access to updates. Updates that are made available once the maintenance agreement expires cannot be used with this license. Updates that have been made available within the maintenance period can be used even after the expiration of the contract.
License with Downgrade-Right	The license covers the right to optionally use older versions of a program. With this type of license, a customer can migrate all clients to the new version at a later date, and the software publisher is not required to sell old releases.
License with Upgrade-Right	The license covers the right to optionally use newer versions of a program. With this type of license, revenues will not drop before the release of a new version.
Grace Period License	A software that is distributed with a grace period license can be used for a limited time without activation. Once the grace period expires, activation becomes necessary.

Volume License	The customer, usually a key account, is sent a large number of licenses to cover the many seats needed. Software publishers can define whether each individual computer should be activated or the system needs to be policed by audit.
High Availability License	The user owns a redundant license server ("2 out of 3" principle). This architecture ensures the availability of software in the event of a license server failure.
Hot Standby License	The user owns a second license server that automatically comes into use in the event of a failure affecting the main license server. The use of the backup server is logged and can be limited to a maximum duration.
Cold Standby License	The user owns a second license server or an emergency dongle that can be used in the event of a failure affecting the main license server. The use of the backup server or the emergency dongle is logged and can be limited to a maximum duration.
Overflow License	The user is entitled to use more licenses than the volume he purchased. The use in excess is logged and can be limited in terms of period of validity and volume. This model allows the billing of the licenses that are actually used.
Borrowable License	The user is entitled to borrow a license for use on a local computer (CmActLicense) or CmDongle for a fixed period of time. During this time, the license remains allocated to the license server and cannot be used otherwise. When the borrowing time expires, the license is automatically made available again on the license server and can no longer be accessed locally. It is possible to return the license manually to the server or renew a borrowed license.
Transferable License	The user is entitled to permanently transfer a license to another PC or onto a CmDongle. It is possible to specify whether this can be done online or completely offline.
Named User License	The license is associated with a user name.
Computer-bound License	The license is associated with a specific computer.
Time Zone License	The license can only be used in the specified geographical region (time zone).
Country-Based License	The license can only be used in the country that the software vendor has whitelisted or did not exclude in a blacklist.

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 Asia · Hanoi, Vietnam |
HSP EMEA 2019 · Malta | RFID Journal LIVE! · Phoenix, USA

more ▶

www.melzergmbh.com

INFINEON and XAIN to collaborate on *bringing* BLOCKCHAIN into *the car*

Infineon Technologies AG and XAIN have agreed to work together on bringing blockchain technology into the car. The Munich semiconductor maker and the Berlin-based start-up have signed a corresponding Memorandum of Understanding at Infineon's 1st Automotive Cybersecurity Forum, which took place today in Munich. The goal of the collaboration is to test possible applications and develop suitable ones to market maturity. A first demonstrator shows how access rights, e.g. for car sharing, can be granted decentrally with a smartphone app.

□ "Cybersecurity is crucial for the data-driven mobility of the future", says Peter Schiefer, President of Infineon's Automotive Division. "Blockchain technology has enormous potential in this regard, but its use requires a high degree of coordination between the selected blockchain methodology and the security hardware installed in the car itself. We will be working together with XAIN to achieve this level of configuration."


A blockchain is a decentralized database that enables speedy transactions and particularly secure, tamper-free storage. In connection with cars, feasible applications for this technology include automated payments, keyless access for car sharing schemes, on-demand services, tuning protection and automated driving functions. Essentially, it is all about the granting of access rights – to the car itself or to specific data in the vehicle. An example involving specific data is when insurance companies offer low rates for car owners with good driving habits.

All of Infineon's 2nd generation AURIX™ microcontrollers can provide support for blockchain functionality in cars already today. This support is based on an embedded hardware security module (HSM) that complies with the highest level of the EVITA security standard. An HSM consists of special computing and storage units within the microcontroller. It performs the cryptographic operations and is protected by a dedicated firewall of its own. The 2nd generation AURIX microcontrollers thus have a secured memory for the digital key used for identification in the blockchain and are able to perform blockchain operations, such as hashing or digital signing, swiftly and securely. Certified security controllers such as the OPTIGA™ TPM 2.0 from Infineon for automotive applications, allow even higher security levels to be reached.



However, the creation of new data blocks still represents a challenge for the conventional microcontrollers used in cars. Due to the enormous amounts of required computing power, the so-called mining, as used in the context of cryptocurrencies, up to this point in time has been executed by high-performance processors. XAIN, however, is working on a new process that can also be performed on devices that need to be economical in their use of energy – such as microcontrollers in cars.

"We aim to turn cars into fully-fledged network participants", says Leif-Nissen Lundbæk, founder and CEO of XAIN AG. "As well as being important for offline and real-time capabilities, this also enables a particularly high level of privacy protection in connection with AI technologies. It ensures that private data for machine learning is kept exclusively in local storage. The goal of our collaboration with Infineon is to advance the use of XAIN's AI technology in cars." ☒



NEW HOPE for *Post-Quantum* CRYPTOGRAPHY

By Robert Bach, Infineon Technologies

As a pioneer in the development of encryption mechanisms that can withstand the computing power of future quantum computers, Infineon is already preparing for the smooth transition from currently used security protocols to post-quantum cryptography (PQC). In a world of quantum computers, PQC should provide a level of security comparable with what RSA and ECC provide today in the classical computing world.



□ Post-quantum cryptography refers to new cryptographic algorithms (usually public-key algorithms) which are expected to be efficiently secured against an attack using a quantum computer.

However, as appropriate quantum computers are not commercially available yet, real-life experiments with PQC are almost impossible today and can only be partly simulated. Nonetheless, academia and businesses are intensely researching PQC to have efficient encryption technologies in place once quantum computers would hit the market.

The Quantum Computer

A quantum computer uses “qubits” that can exist in any superposition rather than bits (0 or 1) in a conventional device. Consequently, certain calculations can be performed simultaneously and far faster than ever before, solving problems that would require unattainable amounts of conventional computing power today. With operations that are thousands of times faster, quantum computers offer new possibilities, for instance, for searching large databases, for chemical or physical simulations, and in material design, etc. However, this

“ *The phantom of the quantum computer is keeping academia and the IT industry on high alert. At Infineon, we are proud to be the first to transfer PQC onto contactless smart cards.*
-Thomas Pöppelmann, Infineon

operating power may also allow the decoding of currently used encryption algorithms that are practically impossible to decode with technologies available today.

Due to their computing power, quantum computers have the disruptive potential to break various currently used encryption algorithms. Infineon Technologies AG is ready to provide a smooth transition from today's security protocols to next-generation post-quantum cryptography (PQC). The company has already successfully demonstrated the first PQC implementation on a commercially available contactless security chip, as used for electronic ID documents. This places Infineon in the pioneering position for encryption that withstands quantum computing power.

Quantum Computer attacks

Quantum computer attacks on today's cryptography are expected to become reality within the next 15 to 20 years. Once available, quantum computers could solve certain calculations much faster than today's computers, threatening even best currently known security algorithms such as RSA and ECC. Various internet standards like Transport Layer Security (TLS), S/MIME or PGP/ GPG use cryptography based on RSA or ECC to protect data communication with smart cards, computers, servers or industrial control systems. Online banking on "https" sites or "instant messaging" encryption on mobile phones are well-known examples.

The impact on cryptography will be dramatic: most public-key algorithms currently in use are expected to be broken easily by adequate quantum computers including RSA and ECC-based public-key cryptography algorithms. The most vulnerable applications concerning quantum-computer attacks are those where asymmetric cryptography is used:

- Communication protocols: Authentication protocols verifying the authenticity via digital certificate provided through a PKI infrastructure. Various internet standards (e.g. Transport Layer Security (TLS), S/MIME, PGP, and GPG.)
- Digital signatures: Digital signatures are increasingly replacing traditional, manual signing of contracts. They protect signed contracts by verifying every bit of the document against a digital signature. Public key, i.e. asymmetric, algorithms secure sign and/or verify data through digital signature algorithms.

There are applications, for instance, energy infrastructure, space et al., where products' lifetime of 15-30 years is common. Thus, these applications and corresponding devices / infrastructure will be in use when quantum computers become a reality. Therefore, system designers must already think about migration from traditional asymmetric cryptography to PQC. This does not imply that PQC algorithms must mandatorily be implemented now, but rather a forward-looking strategy must be in place.

Governmental applications are critical, especially due to the fact that identity theft or misuse can have major consequences. Government ID applications include travel documents (ePassport) and ID cards – often equipped with digital signature functionality.

Standardization bodies are expected to agree on one or multiple PQC algorithms within the next few years before governments and industries mandate the migration. Infineon is actively participating in the development and standardization process in order to enable a smooth transition and to address security challenges that may arise in the advent of quantum computers.

To better respond to security threats that are yet to come, Infineon continuously collaborates with the academic community, customers and partners. And pushes for future standards that can be executed efficiently and securely on small and embedded devices.

There is New Hope

New Hope is a post-quantum key-exchange algorithm, developed by Erdem Akim, Léo Ducas, Peter Schwabe and Thomas Pöppelmann, one of Infineon's security and cryptography experts. The development of New Hope received the very prestigious Facebook Internet Defense Prize 2016.

New Hope offers a 256-bit security level, has performance advantages over previous work due to the use of a better suited error distribution, a new reconciliation mechanism, efficient defense against backdoors and so-called "all-for-the-price-of-one" attacks. Google has integrated the New Hope algorithm into its Chrome Canary browser during an experiment to test the practicality of post-quantum cryptography. The experiment was deemed successful.

"The phantom of the quantum computer is keeping academia and the IT industry on high alert," said Thomas Pöppelmann from Infineon's Chip Card & Security Division, who co-developed the New Hope algorithm. "At Infineon, we are proud to be the first to transfer PQC onto contactless smart

cards. Our challenges comprised the small chip size and limited memory capacity to store and execute such a complex algorithm as well as the transaction speed."

Chip memory size and computation time are key

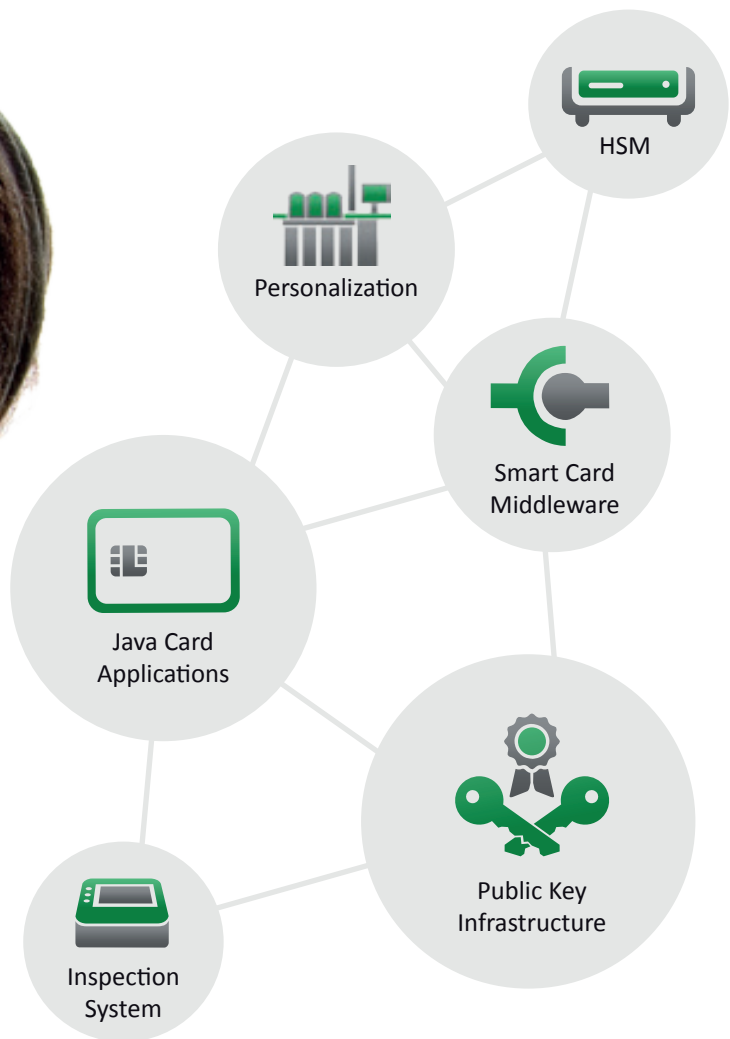
Security experts at Infineon's Munich headquarters and the Center of Excellence for contactless technologies in Graz, Austria, made a breakthrough in this field. They implemented a post-quantum key exchange scheme on a commercially available contactless smart card chip, as used for electronic ID documents. Key exchange schemes are used to establish an encrypted channel between two parties. The deployed algorithm is a variant of New Hope.

The small chip size and limited storage space for storing and executing such a complex algorithm, as well as the transmission speed were challenging, but puts Infineon in a leading position in this field of encryption that withstands quantum computing power.

In 2017 this achievement was awarded with two SESAMES Awards for post-quantum cryptography on a contactless security chip.

"Demonstrating post-quantum cryptography on a contactless security chip puts Infineon in a leading position in this field," said Thomas Rosteck, Division President Chip Card & Security, Infineon Technologies. "Our security solutions rely on trusted and standardized private and public key algorithms. To better respond to security threats that are yet to come, we continuously collaborate with the academic community, customers and partners. And we push for future standards that can be executed efficiently and securely on small and embedded devices." ☒

We create your eID Solution



Subscribe to our NEWSLETTER now!



World's *first* TPM for CYBERSECURITY in the *connected CAR*



□ Infineon Technologies AG is enabling a crucial step toward greater cybersecurity in the connected car. The Munich-based company is the world's first semiconductor manufacturer to put a Trusted Platform Module (TPM) specifically for automotive applications on the market. The new OPTIGA™ TPM 2.0 protects communication between the car manufacturer and the car which increasingly turns into a computer on wheels. A number of car manufacturers already designed in Infineon's OPTIGA TPM.

The TPM is a hardware-based security solution that has proven its worth in IT security. By using it, car manufacturers can incorporate sensitive security keys for assigning access rights, authentication and data encryption in the car in a protected way. The TPM can also be updated, so that the level of security can be kept up to date throughout the vehicle's service life.

"As a computer on wheels, the connected car benefits from the experience of the IT industry," said Martin Brunner, expert for automotive security at Infineon. "In the complex interplay between software, network and cloud, security hardware creates the solid foundation for secured communication. Backed by Infineon's many years of expertise in the automotive and security areas, we have optimized the OPTIGA TPM for automotive applications. It is easy to integrate and substantially increases cybersecurity – from production to recycling of connected cars."

Secured communication throughout the vehicle's service life

Mobility of the future requires the exchange of huge volumes of data. Cars send real-time traffic information to the cloud or receive updates from the manufacturer "over the air", for example to update software quickly and in a cost effective manner. The senders and recipients of that data, whether car makers or individual components in the car, require cryptographic security keys to authenticate themselves. These critical keys are particularly protected against logical and physical attacks in the OPTIGA TPM, as if they were in a safe.

Furthermore, incorporating the first or initial key into the vehicle is a particularly sensitive moment for car makers. When the TPM is used, this step can be carried out in Infineon's certified production environment. After that, the keys are protected against unauthorized access; there is no need for further special security precautions throughout the various stages of the – often globally distributed – value chain.

The TPM likewise generates, stores and administers further security keys for communication within the vehicle. And it is also used to detect faulty or manipulated software and components in the vehicle and initiate troubleshooting by the manufacturer in such a case.

Whereas a vehicle has an average service life time of 12 to 15 years, security features and algorithms keep on being developed and enhanced on a continuous basis. The TPM's firmware can be updated by remote access so the security it offers can be kept up-to-date – including the cryptographic mechanisms (cryptoagility).

The new OPTIGA TPM 2.0 SLI 9670 from Infineon is a plug & play solution for automotive applications. It is especially suited for use in a central gateway, the telematics unit or the infotainment system of the vehicle.

The SLI 9670 consists of an attack-resistant security chip and high-performance firmware developed in accordance with the latest security standard. The firmware enables immediate use of security features, such as encryption, decryption, signing and verification. The TPM can be integrated quickly and easily in the system thanks to the open source software stack (TSS stack) for the host processor, which is also provided by Infineon. It has an SPI interface, an extended temperature range from -40°C to 105°C and the advanced encryption algorithms RSA-2048, ECC-256 and SHA-256. ☒



GEMALTO and R3 *pilot*
***BLOCKCHAIN* technology**
for *Digital* ID

Who are you, and can you prove it? The new Gemalto Trust ID Network enables users to give digital service providers fully verified and secured answers to these simple yet critical questions.

By creating and managing their own ‘Self-Sovereign’ Digital ID, users can enroll with a host of different digital banking, eCommerce and eGovernment services, without having to go through repeated due diligence processes for each of them. This innovative distributed approach to Digital ID management enables service providers to leverage ubiquitous identities certified by trusted parties, whilst putting users firmly in control of their data.

□ Blockchain technology is ideal for supporting digital transactions that are based on trusted and verified identities, without exposing sensitive data to the threat of hacking and cyber-attack. With Trust ID Network, user control is facilitated via the ID Wallet, a convenient and secure mobile app. Here users can add personal data to their digital identity, have it certified, and give consent to share it with chosen service providers. Only ‘attestations’ issued by trusted parties are stored on the blockchain, keeping personal data under sole control of users.

Banks can lead the creation of new Digital ID ecosystems

To comply with new regulations*, financial institutions must implement robust KYC (Know Your Customer) procedures, rigorous data privacy and protection, as well as strong customer authentication. They are therefore ideally positioned to lead the self-sovereign Digital ID revolution. Other service providers that rely on verified customer identities, such as public services, mobile operators and airlines, can also reap significant benefits, including the opportunity to share ID management costs. As further stakeholders join a self-sovereign ID ecosystem, richer identities are built, supporting an even wider range of use cases.

Gemalto builds on the unique features of R3’s Corda blockchain platform

Gemalto deploys its Trust ID Network application and data protection solutions on the latest version of the Corda platform, the world’s foremost enterprise blockchain solution built by R3.

It provides full privacy, security and immutability along with a streamlined integration for service providers and the ability to support mission critical identity services. R3 already works with over 200 financial institutions and other partners worldwide.

A wide range of stakeholders are being invited to participate in one of several Trust ID Network pilots that will launch later this year.

“Empowering customers to manage and control their own digital identity based on blockchain technology is nothing short of revolutionary and we’re very pleased to be collaborating with Gemalto on the Trust ID Network,” said David E. Rutter, CEO of R3. “The Corda platform’s unique privacy features offer the ideal basis for a secure, easy-to-deploy decentralized ID management platform.”

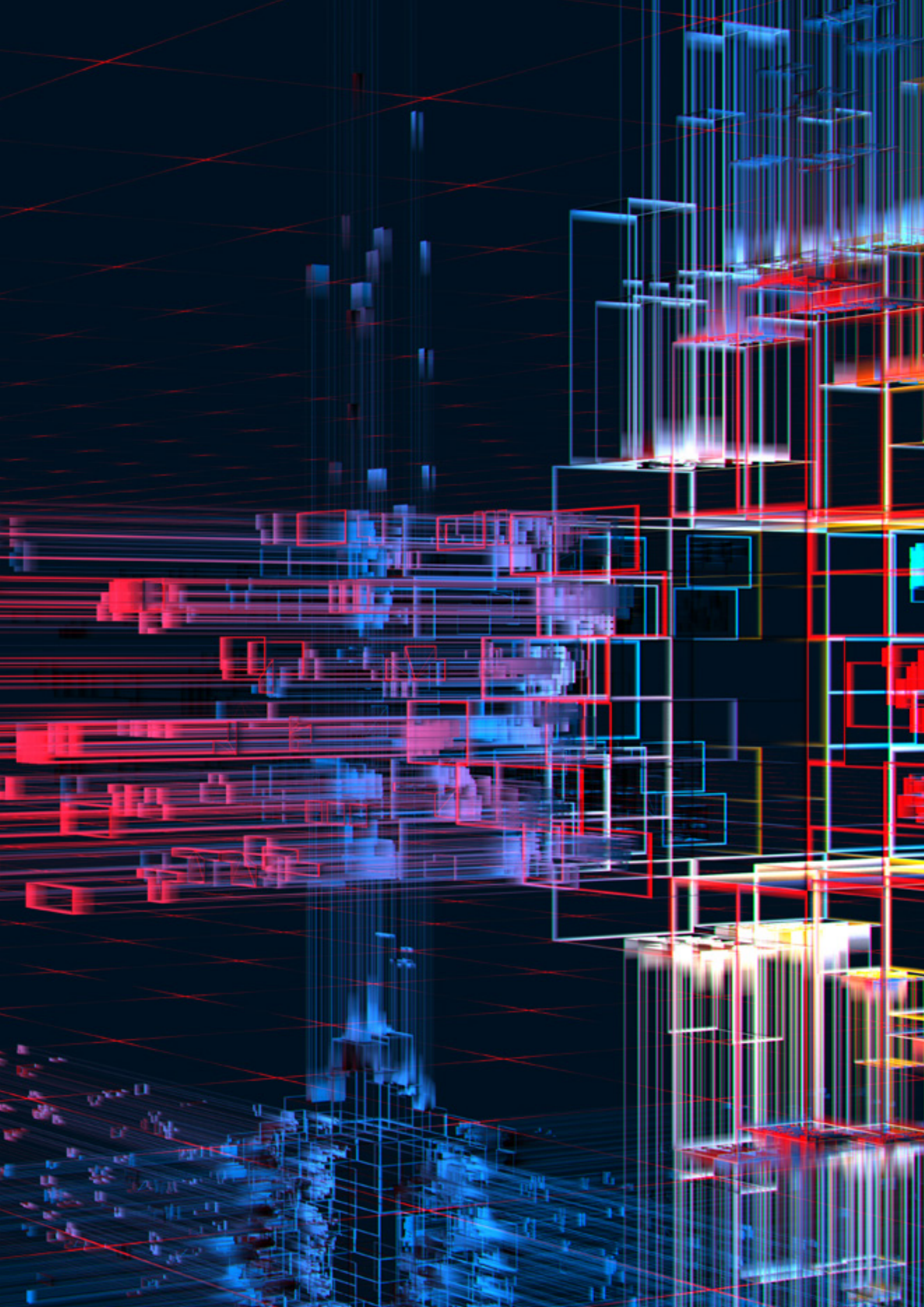
“Trust ID Network solves the profound weaknesses of traditional, ‘siloes’ identity frameworks: the clumsy user experience, rising costs and difficulties in complying with stricter regulations. It’s the perfect illustration of Gemalto’s ability to combine proven Digital Identity solutions and new technologies such as the blockchain,” said Bertrand Knopf, EVP Banking & Payment for Gemalto. “Financial institutions are best-placed to lead this self-sovereign identity revolution, but it will prove similarly attractive to a wide array of other service providers.” ☒

**In the EU, relevant regulations include AMLD 4 & 5, the GDPR (General Data Protection Regulation) and PSD2 (second Payment Services Directive)*

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

By Markus Hoffmeister and Klaus Schmeh, cryptovision

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



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

-Benjamin Drisch, cryptovision

□ What are the security implications?

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

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

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

Blockchain for Identity and Data Management

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

Data Bridge Market Research 2018

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

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

Is blockchain replacing conventional PKI and eID systems?

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

Benjamin Drisch, cryptovision

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

The benefit of a key being stored on an eID card is less clear when it comes to blockchain-based authentication. As an eID card is an authentication solution in itself, it can be questioned whether a

blockchain-based authentication system is even necessary when such a card is available. In addition, the involvement of a card issuing authority contradicts the main benefit of a blockchain: to establish a trusted infrastructure without involving a trusted third party. At this point it is important to note that not requiring a trusted third party is not the only advantage of a blockchain. Other purported benefits include fault tolerance, high availability and lower operation costs.

Conclusion

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

cryptovision

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

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



PrimeKey PKI in a BOX – *still* HOT after 6 *YEARS!*

By Jiannis Papadakis, PrimeKey

□ It all started around 2008/2009 when we saw the need to make PKI easier to digest, to move away from the standard PKI project with minimum two weeks of installation and the pre-requisite of having PKI and HSM expertise available. Our goal was to reduce the installation complexity, time to deployment and also to provide a reliable update function. One of the critical parts of the solution was to integrate an HSM and we decided to approach Utimaco as there was already an established partnership. Utimaco liked our idea and has since then been the selected HSM integrated in our PrimeKey appliance solution.

The first appliance solution was released in 2012, and we have since then offered both the PKI software EJBCA Enterprise and the signing software SignServer Enterprise in ready-to-use Appliance versions. They are called the PKI Appliance and the SignServer Appliance, and they are today two of the most popular products in the PrimeKey range.

Our objectives with the PKI Appliance and SignServer Appliance are, and have always been, to offer the most cost-efficient, easy and secure way to deploy an enterprise PKI solution, and the wide customer acceptance of it has proven us right. Since 2012 the revenue from the Appliance business has gone from zero to 25% of the PrimeKey total revenue and based on customer and market feedback, we continue to invest in the next generation of technology and platform.

So why is the PKI Appliance so popular? Most companies who use the PKI Appliance say they appreciate how it gives predictability to the project and the operational costs connected to their PKI. As a customer of the PKI Appliance or SignServer Appliance you:

- don't have to take care of licensing, installation, hardening, administration, maintenance and management of all the underlying components required for a PKI or Signing service. (OS, DB, HSM, WebServers).
- automatically* get access to combined hardware and software, 8/5 or 24/7, support and maintenance services.
- get a FIPS 140-2 level 3 certified HSM built-in to your Appliance (Utimaco CryptoServer SE52). The HSM is integrated in to your PKI to the maximum extent possible and thus minimizing administration and management efforts required when it comes to those very specialized and critical devices. Not to mention the training costs and efforts required when it comes to best practice HSM usage.
- get the possibility to install and run multiple and independent CA instances in one software installation. The CA installations are logically secured against each other and at no additional licensing costs.
- get access* to the continuous evolution of the PrimeKey PKI Appliance and SignServer Appliance.
- get a solution that is prepared for integration into hybrid infrastructures allowing you to utilize the flexibility and agility of PrimeKey's offering.

“Compared to the software based solution the Appliance reduces the efforts for setup and maintenance considerably, and it fits for most use cases and architectural requirements.”

– Alexander Winnen, Senior Security Consultant at Siemens

The number of customers continues to grow, which we're of course really happy about. We also see that new markets and market segments discover our technology, and that our long-term customers continue to appreciate the platform. Do you think your organization would benefit from using an Appliance in your PKI solution? Get in touch and we'll be happy to talk about your needs! ☒

**For customers with support agreements.*

During Trustech you can find PrimeKey and Utimaco, in booth LER B 021.



HOW a *stolen* connected CAR COULD threaten a *whole* CITY

By Marjolaine Lombard, Cyber Security Marketing Consultant, ATOS

□ *From the theft of a connected car to a city held hostage: one giant leap for cybersecurity*

In September 2018, researchers from KU Leuven University and Belgium succeeded in stealing a Tesla Model S in a few seconds. They were able to do it not by stealing the physical keys of the vehicle, but by cloning its key fob, a small and programmable token used to access a physical object. They then just had to

duplicate the signal that was used to unlock the car and the deed was done.

Cyberattacks targeting connected cars such as Tesla are indeed impressive. However, they are just the scratching the surface of security issues that threaten intelligent transportation systems (ITS). The Tesla stolen key fobs raised other issues. After discovering the hack, Tesla thanked the researchers and offered

to patch its customers cars with a software update and an optional 'PIN to Drive' feature requiring the users to enter a PIN before being able to drive. These measures are here to prevent future cyberattacks of the same type, but what if the customer did not install the update? The same theft could happen again. Or, worse, what if the patch update was diverted from its main function if a hacker intercepted it?

ITS are meant to improve security and safety, as well as efficiency. To achieve these results, they rely on sensors, data collection, analysis, control and communication technologies. The more there are, the more potential vulnerabilities can be found, with potential of ITS significantly growing over the years. Traffic monitoring, vehicle safety, transit signal priority, ramp metering... All these applications can enhance the daily life of citizens and prevent transportation accidents, but require a lot of data collection and transmission for further analysis and provide potential cyberattack gateways for hackers. If hackers could take control of the traffic system of a city, they could cause major hazards and casualties.

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), globally known as V2X, technologies security plays a major role in ITS. Connected vehicles communicate through wireless networks to share information with other vehicles and transportation infrastructures, with an on-board unit (V2X Gateway) inside the vehicle communicating information to its environment. According to the Connected Vehicle Reference Implementation Architecture (CVRIA), the security solutions must focus on 3 core elements: confidentiality, integrity and availability.

- Confidentiality: only authorized stakeholders should be allowed to access the content of the messages exchanged in a V2X environment.
- Integrity: to ensure the reliability of the messages exchanged, the security solutions must protect them from being altered by unauthorized stakeholders, otherwise ITS applications could be threatened.
- Availability: operational systems and information must be provided, even in risky situations, especially for critical information.

Typically, distributed denial of service (DDoS) attacks can threaten the availability of an application by trying to exhaust its resources. Malwares can be used to hack electronic control units (ECU) firmwares in a car and block the use of the car until, for example, a ransom is paid. So, what can be done to secure the ITS?

First of all, communication must be protected to prevent attackers from manipulating data. Security solutions based on the secure storage and processing of cryptographic keys are used to provide integrity and authenticity of data required for the reliability of the messages exchanged in V2X. Moreover, encrypting those messages will ensure that only authorized stakeholders could access the information. The monitoring of software running on application controllers also enhance the integrity of ITS. Dedicated secure elements can provide a highly secure answer to these challenges.

Data protection and privacy of ITS is also provided through V2X Public Key Infrastructure (V2X-PKI). V2X security can use pseudonym digital signatures to keep the integrity of the messages shared, allowing automotive infrastructures and vehicles to trust each other. Certificates are issued by Enrolment and Authorization Authorities (EA & AA) and can then be trusted and verified at any time.

In Atos, we chose to secure the V2X environment with these solutions through our Horus Security Suite for ITS. We implemented security controllers as dedicated Secure Elements (V2X-HSM) therefore not affecting the complete board design and sustain the required automotive qualifications and requested performance for automotive applications. Atos Secure Elements (V2X-HSM) rely on the well-known CardOS® which performs the cryptographic functionality over standard interfaces like SPI or I2C. CardOS is a multifunctional native operating system, which provides a high level of flexibility by adapting the file structure.

As modern vehicles use up to 120 ECUs to communicate in an ITS environment, it becomes critical to be able to generate cryptographic keys quickly and efficiently that will be used for signature creation, authentication, as well as message encryption and decryption. With CardOS for IoT, all these state-of-the-art cryptographic functionalities are provided. Coupled with our solution Horus PKI, it becomes easy to implement certificate lifecycle management and ensure data integrity.

ITS services will evolve quickly and exponentially in the years to come. From manufacturers, to end users, cities and application providers, the entire ecosystem will have to adapt to new technologies that could have a huge impact on society if they turn out to be defective. If we do not want the future to be made up of stolen Teslas and cities held hostage, we need to carefully consider security by design! ☒

Adding *IDENTITY* to the INTERNET of *Things* to *improve* SECURITY and *TRACEABILITY*

By Orestis Mavropoulos, AUSTRIACARD

The promise of the Internet of Things (IoT) was always to create “smart” objects. To get data from the physical world to gain insights. These “smart” objects are computers with additional functionalities when connected to the Internet. Our mobile phone is a computer that makes phone calls. Our car is a computer with wheels and an engine. The connectivity of such devices, while beneficial, leaves them vulnerable to attack by threat actors.

□ IoT is a term that has attracted considerable attention as well as confusion. IoT, in the eyes of the general public, is full of questions. What is IoT? What are the benefits of adopting IoT? What happens to the Internet? What is a Thing?

While not the first reference to IoT, but definitely the most accurate, was made by Weiser in 1991, in his paper discussing the computer of the 21st century. He states “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.” Using IoT, information technology will be a part of our environment the same way written word is a part of our daily lives. Technology will be so evident that we will start perceiving it as a natural part of life. When viewed in that light, IoT is a vision in our quest to enhance our environment. We want more from our environment and IoT is a way to achieve it.

The vision of making our environment smarter, more in tune with our day to day lives, gives rise to a plethora of questions. Some of those questions are technical in nature. For example, how can we connect such a vast number of devices? How can we make IoT devices consume fewer resources? On the other hand, other questions about IoT are quite philosophical. Who owns the

data that IoT devices generate? Who can profit from that data? If a self-driving vehicle causes an accident, who is to blame? Is it the owner of the vehicle or the manufacturer? What happens if the accident is a fatality?

One of the most significant concerns about IoT is that it is not secure. The adoption of IoT to everyday devices was the day when people started to distrust and fear technology. It is scary for a parent to hear a strange voice talking to their children through a connected toy. It is scary to think that someone might be stalking you through your security cameras. It is scary to think that a glucose sensor which someone depends on can be compromised and used to harm.

Philosophical questions cannot be answered in the same straightforward manner as the technical ones. But such questions are the ones that need to be addressed to dispel the fear and uncertainty surrounding IoT. The main challenge here is one of trust. An important question in IoT, is how to provide identification-based connectivity to devices without relying on users or other stakeholders? Devices need the ability to uniquely identify themselves to other devices and services. Device authentication enables the application of end-to-end



security mechanisms to protect an IoT solution. Furthermore, it facilitates the use of traceability and auditability in the various states of an IoT system. The unique identifier can be used to determine the chain of causality during security analysis.

In the IoT, the role of identity management is expanding. It is no longer just about identifying people and managing their access to different types of data (i.e. sensitive data, non-sensitive data, device data, etc.). Identity and Access Management systems (IAM) must be able to identify devices, sensors, monitors, and manage their access to sensitive and non-sensitive data. A Public Key Infrastructure (PKI) most commonly thought of as a way of authenticating websites and encrypting data for e-commerce using SSL/TLS certificates, provides a scalable and flexible solution that can help authenticate devices in IoT.

NAUTILUS employs a certificate-based identification and access management service, named NAUTILUS IAM, for IoT devices on different form factors that are infrastructure agnostic. Stakeholders are able to deploy NAUTILUS IAM in their own premises or use NAUTILUS IAM as a service. The unique identity of each device is provided by leaf certificates that are generated when a device is provisioned using intermediate

certificates of the stakeholders. Certificates are stored in secure elements that provide hardware-verified boot and end-to-end authentication root of trust. Based on the unique identity of devices, NAUTILUS offers a platform for developing IoT solutions for individual cases.

The NAUTILUS platform is about solving precise problems and providing clear business outcomes. The aim of the platform is to facilitate the identification of revenue streams from collected information, while securing that information in multiple layers. In the IoT, the information starts in the physical world. It is captured by edge devices, then communicated, processed, stored in the cloud. Finally, it is sent back to the edge. The platform can be deployed in every part of the life cycle of information. In each part of the transmission, the NAUTILUS platform offers additional security layers to protect the integrity of the devices and information. The security mechanisms are adapted to each layer to offer the least stress without compromising security. NAUTILUS's platform focus on security intends to alleviate any fears surrounding IoT. ☒



Global travel is predicted to reach 5 million arrivals per day in 2030.

I haven't been **EVERYWHERE,** *BUT* it's on *my* **LIST**

International travel has become such a natural part of our lives that the World Tourism Organization predicts a global average of 5 million arrivals per day in the year 2030. For airports to cope with these huge numbers, IATA has recently launched the ONE ID INITIATIVE, promoting opportunities for a seamless, walking pace passenger experience when crossing borders. Today, OVD Kinegram is developing products and solutions that will contribute to making this programme a reality.

To learn more about the e-Gate Mobile solution, please visit www.kinegram.com.
For more information please contact john.peters@kinegram.com

□ Tomorrow's Travel - Already Today

More and more countries are adopting a “trusted traveler” approach, where biographic and biometric details of individuals are pre-registered in secure databases during a visit to the country. During the flight booking process for a subsequent visit to that country, the pre-registered traveler may use a mobile app capable of deriving his identity from his electronic passport and transferring it temporarily to his smartphone using near-field communication (NFC). He also takes a selfie, to confirm that he is the rightful holder of that passport. The app then requests approval for entering the country. Once this is granted, the airline will issue the flight tickets.



Trusted traveler programs and smart apps allow for convenience in traveling. Machine-readable passports and biometric data gathered by cameras enable a walking-pace entry to the destination country.

During the check-in at the airport, the airline confirms that the biographic and biometric data sent in advance via the app do match those of the traveler and the travel documents he presents. In parallel, the traveler’s passport is inspected for authenticity, and the validated biographic and biometric data from the chip are sent to the country of destination. The traveler receives a notification that his boarding pass has been confirmed and that he may proceed to board his plane.

Upon arrival at the airport of his destination country, he selects the lane for pre-registered travelers. At the entrance to this lane, the machine-readable zone (MRZ) of his passport will be scanned briefly. This triggers a selection from the database of the pre-registered facial images which correspond to the data of the MRZ. The traveler’s facial biometrics are captured using overhead cameras, and compared with the pre-positioned facial images from the database. If the match is satisfactory, the gates will open automatically and allow the traveler to conveniently and effortlessly enter the country.

Convenience Versus Confidence

1. Making this process happen will require advancements in airport infrastructure and mobile devices - but most importantly, absolute confidence in the claimed identity of travelers will be required. This is where the future of travel comes back to the present, and to our most crucial and indispensable physical documents – our passports, which will remain the cornerstone in establishing our identities for many years to come. The extent to which these documents can be authenticated determines the trade-off between convenience and security.

To understand this better, let us look at “False-Rejects” in facial recognition. How can these be distinguished from actual fraudulent attempts to enter a country? With the readily-available Mobile e-Gate App from OVD Kinegram, the immigration officer can use his smartphone to inspect the traveler and his passport:

1. He scans the MRZ of the traveler’s passport. The corresponding biographic data are displayed on the phone, any inconsistencies in the MRZ are highlighted.
2. Via NFC, the app accesses the chip data when the phone is positioned on the passport. Via ICAO basic access control protocol, the photo and biographic data on the chip are displayed on the phone.
3. The immigration officer compares the photo in the passport, the photo from the chip, and the actual person standing in front of him.
4. If still unsure, the officer captures a live video of the traveler’s face, which the software transforms into a facial template for comparison purposes. A positive match between the live image and the photo from the chip is reassurance that the biometric data in the chip match the traveler.



Immigration officers can use the Mobile e-Gate App to verify travelers' identities.

Comprehensive Security - The Triangle of Trust

The Mobile e-Gate app allows the officer to confirm the Country Signing Certificates by accessing the corresponding country signing public key stored in the ICAO PKD. Once this has been verified, the immigration officer has a high level of confidence that the passport is valid and that the biometric data in the chip match the traveler. In short, he can be sure of the document, the chip, and the person.

With the Mobile e-Gate App, OVD Kinegram proposes a solution that enables both convenience of travel and security on the highest level. In combination with physical security features such as the KINEGRAM, governments have an unparalleled solution at hand for securely establishing a traveler's identity and the authenticity of his documents.

This becomes evident when we consider situations where the Country Signing Certificates cannot be verified. According to ICAO recommendations, if the electronic data on the passport cannot be fully authenticated, the document should be treated as a non-electronic passport. In this case, the Mobile e-Gate App enables the Immigration Officer to inspect the physical security features on the document without any prior knowledge or training. With the touch of a button, a photographic image of the data page of a sample document is displayed on the phone, enabling a side-by-side comparison with the actual document. Additionally, the kinematic movements of sophisticated security features such as the KINEGRAM can be displayed as a video, again for comparison purposes.

Beyond Airport Borders

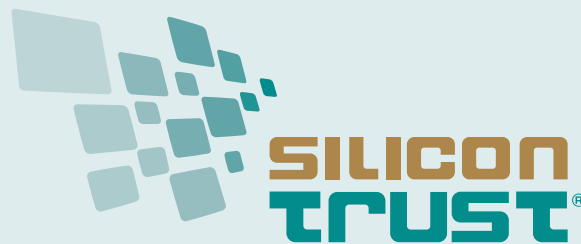
The Mobile e-Gate App may also be useful in border crossing situations other than air travel, where there is little or no infrastructure to support automatic inspection. Examples would be harbors or ports, or land border crossings by car, train or coach. This smartphone app has taken many of the inspection processes that the traveler experiences while using an e-Gate and replicated them for use in a mobile device.



Use cases for the Mobile e-Gate App in different border crossing situations.

Unlike fully automated border crossings, the Mobile e-Gate App allows for a smart decision based on facial recognition via algorithms, in support of human face matching by the officer. The officer has the opportunity to focus more on the behavior and mood of the traveler. The App further enables the inspection of even the most sophisticated physical security features. It is a crucial tool in establishing the triangle of trust, making sure the traveler in question is the right person holding a valid document with an authentic chip. ☒

SILICON TRUST DIRECTORY 2018



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

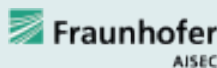
Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security.

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.

ABNote



ABnote™ is a leading global supplier of secure documents, services and solutions. If you have a credit card or an identity card, or have received a gift or loyalty card, or any other plastic card, chances are that you have used an ABnote product. If you have interacted with a financial institution, or have used your smart phone to make a payment, you have likely taken advantage of an ABnote service.

We are proud of our legacy – over 200 years of manufacturing high quality, tamper-resistant products to governments, financial institutions, retailers and other organizations throughout the world. Today, our products and technology encompass multiple markets, keeping pace with today's rapidly changing requirements for convenient and secure transactions.

www.abnote.com

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

AGFA



Agfa is commercially active worldwide through wholly owned sales organizations in more than 40 countries. In 2014 the Group achieved a turnover of € 2,6 billion. Agfa develops, produces and sells special films for the card industry. PETix™ is a range of high-performance polyester films, for cards with a life-time above 10 years and a high chemical, scratch and thermal resistance.

www.agfa.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

BALTECH



BALTECH is specialized in ISO14443/15693/NFC Reader technology. The core competencies are RF-Interface technology and sophisticated high level functionalities supporting the latest card technologies and security mechanisms. All products are 100% developed and manufactured in-house. This is the basis for customization capabilities offered to deliver application tailored, cost optimized products from readers up to terminals with individual functionalities for various applications.

www.baltech.de

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

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, prelamines, LaserCard® optical security media technology, and FARGO® card printers.

www.hidglobal.com

HJP CONSULTING



HJP Consulting (HJP) with headquarters near Paderborn, Germany, is an internationally operating firm of IT consultants specialized in the planning, procurement and approval of smart card solutions with focus on e-identity and e-health applications. The manufacturer-independent specialists at HJP supervise large-scale projects for introducing e-passports and eID systems at both the technical and strategic level. The firm's consulting services encompass the areas of system architecture, software specification, tenders, quality and security management as well as project management.

www.hjp-consulting.com

THE IDENTIV GROUP



Identiv provides secure identification (Secure ID) solutions that allow people to gain access to the buildings, networks, information, systems and services they need – while ensuring that the physical facilities and digital assets of the organizations they interact with are protected. Based in Orange County, California, it is a technology-driven company with significant experience in diverse markets, and is uniquely equipped to address the needs of customers worldwide in an evolving technological landscape.

www.identiv-group.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 micro-controllers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

MELZER



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

MIKRON



MIKRON was founded in 1964. With main activities in semiconductor manufacturing (Power Management Products and RFID) MIKRON is an important player within the financial strong industrial group of JSFC SISTEMA. MIKRON has about 1600 employees and is with a capacity of 50 Mio inlays and labels per month and a chip capacity of about 100 Mio per month the largest RFID manufacturer in Europe. Major activities are within the RFID and Industrial/Consumer market. Joint Venture and cooperation for technology will secure strong standing within the fast growing future market.

www.mikron-semi.com

OPEN LIMIT



OpenLimit SignCubes AG (www.openlimit.com) was founded in 2002 and is a wholly-owned subsidiary of the publicly traded OpenLimit Holding AG. The company is headquartered in Baar, Switzerland and has a subsidiary in Berlin, Germany. The group currently employs more than 60 highly qualified employees.

www.openlimit.com

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

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

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 EJBICA 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 ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.

www.pwpw.pl

REINER SCT



REINER SCT Kartengeräte GmbH & Co. KG, based in Furtwangen (Black Forest), Germany, is a leading manufacturer of OTP generators and smartcard readers for eCards, electronic signature and online banking in Germany. REINER SCT also develops products for secure online authentication, time attendance and access control. The technology company employs 45 staff and is part of the global and family-owned REINER group.

www.reiner-sct.com

ROLIC



Rolic Technologies Ltd. is an innovative Swiss high-tech company headquartered in Allschwil (Basel). Rolic modifies surfaces on a nano scale with polarized light to achieve unique optical effects and to manage light. New industry standards were set for LCD TVs, forgery-proof security devices and efficient OLED lighting products. Highly skilled staff in the Swiss headquarter continually develop, refine and extend Rolic's proprietary core technologies. The subsidiary Rolic Technologies B.V. (Eindhoven, Netherlands) engineers industrial solutions for the global customer basis.

www.rolic.com

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

T-SYSTEMS



Drawing on a global infrastructure of data centers and networks, T-Systems operates information and communication technology (ICT) systems for multinational corporations and public sector institutions. T-Systems provides integrated solutions for the networked future of business and society. With offices in over 20 countries and global delivery capability, the Telekom subsidiary provides support to companies in all industries. Some 50,000 employees combine expertise with ICT innovations to add significant value to customers' core business all over the world.

www.t-systems.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

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 AG (WIBU®), 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 PC-, embedded-, mobile- and cloud-based models.

www.wibu.com

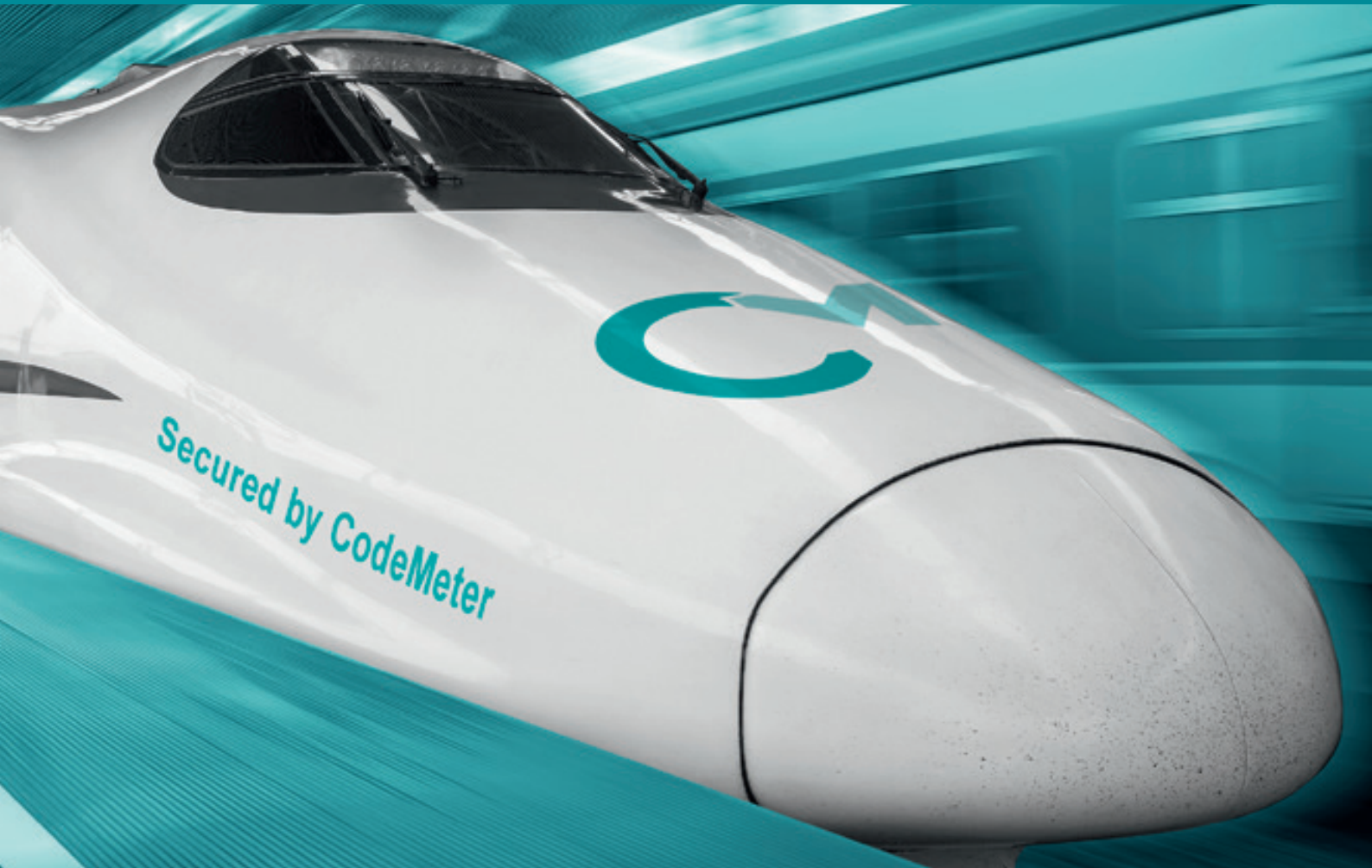
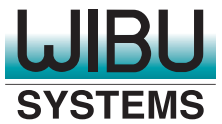
X INFOTECH



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.

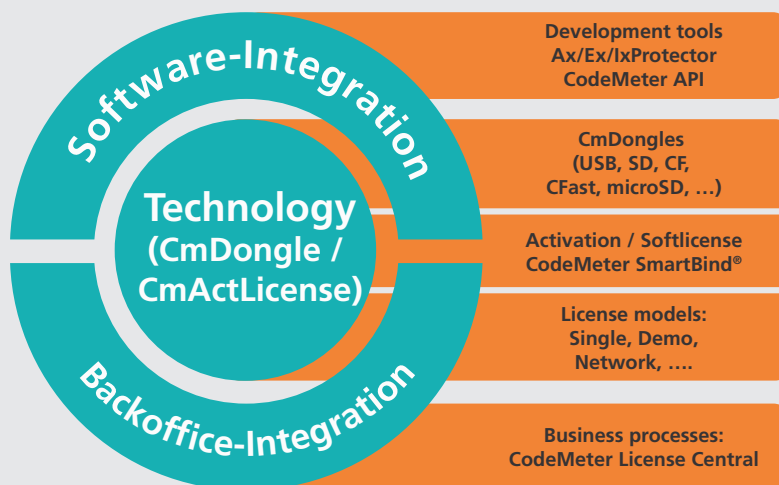
www.x-infotech.com

CodeMeter stands up for Industrie 4.0



CodeMeter for Industrie 4.0 – Watch the full Video – www.wibu.com/40

New business models for software publishers and device manufacturers



In its mission to deliver the most secure, unique, and versatile technology, Wibu-Systems has developed CodeMeter®, a comprehensive, award-winning suite of hardware and software solutions for **computers, embedded systems, mobile devices, PLCs, and microcontrollers** that incorporates internationally patented processes dedicated to protecting the integrity of digital assets.

With its motto “**Perfection in Protection, Licensing, and Security**”, Wibu-Systems supports ISVs and OEMs in their fight to **safeguard the intellectual property** of their applications against illicit and fraudulent use, reverse engineering, tampering, sabotage, espionage, and cyber-attacks, while generating new **software-feature based business models** fully integrated with ERP, CRM, and e-commerce platforms.

The unparalleled lineup of **hardware secure elements** (USB dongles, SD cards, microSD cards, CF cards, CFast cards, ASICs) designed to withstand high fluctuations in temperature, humidity, and vibration, coupled with the support of all mainstream operating systems and M2M communication standards makes CodeMeter the ideal candidate for both **brown and green field** applications.

//CODiE//
2017 SIIA CODiE WINNER

**SECURITY
LICENSING
PERFECTION IN PROTECTION**

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

“Coil on Module” – chip module
with antenna at the rear-side
of the module

card body 100%
polycarbonate



radio communication between
card antenna and chip
module antenna

wired card antenna

Go contactless with Coil on Module (CoM)

- › CoM is designed to simplify your transition from contact-based to dual-interface card production
- › CoM delivers a new level of card body robustness and reliability
- › CoM is THE solution for 10 years life time – essential for ID documents

