NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2017 | #20

The VAULT

APPLICATIONS
Airport - the future of Checkpoint Delta
Authentication - bridging the credentials gap

TECHNOLOGY
A new encryption paradigm
Virtual token - a smart card alternative?

INSIGHTS
De La Rue on Next generation ID
Bringing IoT securely into the developing world

NEXT GENERATION IDENTITY SOLUTIONS

FIND
WHAT LIES BEYOND THE EXPECTED

Border Control
Justice & Public Safety
Civil Identity

SMART SEARCH & MATCH

www.wcc-group.com

Contents

At the Airport: The Future of Checkpoint Delta 4
By Sanjay Dharwadker – WCC Smart Search & Match

Next generation ID solutions for healthy and stable societies 8
An interview with Ulrich Walter, De La Rue

Bridging the gap between physical and mobile credentials 12
By Steve Warne, HID Global

“Are you looking at me?” 16
By Elke Oberg, Cognitec Systems

A new Encryption Paradigm for a new Industrial Age 18
By Daniela Previtali, Wibu-Systems

Citizen Identity Management - A view of the market 22

Utilizing the synergies between passports and eID cards 24
By Veronica Atkins, Silicon Trust

Virtual Token – A smart card alternative that makes sense? 28
By Klaus Schmeh, cryptovision

New IoT technology and a solid chain of trust 32
By and with Andreas Philipp, PrimeKey

Bridging the gap between IoT and the developing world 34
By Richard Eyo, Department of Mathematics and Information Security
Royal Holloway, University of London

Data capture when you want and where you want it 40
By Chimezie Emewulu, Seamfix

Silicon Trust Directory 2017 42

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: VERONICA ATKINS
ART DIRECTOR: LANA PETERSEN
EDITORIAL CONTRIBUTIONS: SANJAY DHARWADKER, DANIELA PREVITALI, KLAUS SCHMEH, STEVE WARNE, RICHARD EYO, ULRICH WALTER, BENJAMIN DRISCH, ELKE OBERG
PHOTOS: WIBU-SYSTEMS, ISTOCKPHOTO, WCC, HID GLOBAL, ISTOCKPHOTO, DE LA RUE

PRINTING: DRUCKEREI HÄUSER KG, COLOGNE

EDITION: SPRING 2017

AT THE *AIRPORT*: The Future of *Checkpoint Delta*

By Sanjay Dharwadker – WCC Smart Search & Match

Shrouded in the mysteries of Cold War espionage stories, Checkpoint Charlie has captured our imaginations as the ultimate border crossing for over half a century now. When the Berlin Wall finally came down, it had 14 checkpoints known by the names of their respective neighborhoods. But earlier, they bore signage in the aviator alphabet – Alpha, Bravo, Charlie. Somehow, the name of the Friedrichstraße crossing persisted: Checkpoint Charlie. Even as a tourist attraction, it remains a reminder of a sad aspect of nation-state politics: that of dividing people from people.

Today, this drama has shifted to the Airport – a microcosm to be examined in great detail by anyone dealing in security policy, strategy, or technology. No doubt, 9/11 and its aftermath have been the most important reason for this focus. The airport is a true twenty-first-century icon, not just in scale, but also in opportunity; for example, of great architecture and commerce. But alongside, there are the vulnerabilities of post-cold-war politics and terrorism. In a world that wavers between borderless globalization and xenophobia, the airport has to be many things at once for its different users. It unites in a single location both the ideas and the reality of security, territory, and population. It brings together a complex web of local, national, and international laws, as well as surveillance for conflicting reasons – on behalf of companies, governments, and individuals. It connects many social spheres, and must provide containment amidst an illusion of infinite freedom. Thus, the airport is both the definition of an immense problem, as well as a statement of its grand solution.

> *"Already the mobile phone and biometric payment authentication, between the power of one and the authority of the other, provide even greater capacity to organize the identification of individuals.*

All kinds of people converge at the airport. By the end of this decade, around half a billion passport holders will pass through national and international airports around seven billion times yearly. Already there is pressure to treat the elite with instant service without queuing. Archaic instruments like the visa cause additional bottlenecks in an already overstretched service infrastructure. Many of the sixty-five million internationally displaced persons also arrive at international airports, many seeking asylum, some in conditions of statelessness. Amidst all this are individuals attempting to travel on one of the over 60 million stolen or lost travel documents, individuals suspected of commercial crime, smuggling, and trafficking, and individuals with a criminal background and intent. Finally, there are the dreaded terrorists, whose detection and interception could prevent untold loss and tragedy. They may arrive disguised across the entire spectrum – from the elite to the asylum seeker. There is no way to tell which persona they will don next.

Airports have the dual objective of maximizing national security and maximizing commerce. This leads to complex layouts alternating wide open spaces with narrow passages and barriers, optimizing for space, speed, and security. Security initially was considered a question of minimizing the time to process. Today the focus is on the outcome. In general, security depends on ID documents, identification and detection devices, CCTV, and data such as no-fly lists. Individually, each has well-understood shortcomings, but together, they do provide a system that seems to hold. Recent years saw the addition of strategies of risk management, more comprehensive post-event assessment, and somewhat controversially, using databases as an instrument of selection, separation, and exclusion. Ideally, passports serve well for external movement. However, the use of ID cards for internal movement opens up many issues of acceptability, standards, and authentication. Similarly, despite constant advancements both in the technology and practice, biometrics as valves that control global flows of humanity might be restricted only to international border crossing.

For the airport, the goal underlying its laws, regulations, procedures, and technologies is to facilitate global mobility and at the same time fortress countries and continents as needed. Smart Borders has become a euphemism for the increasing use of biometrics (mainly face and fingerprints) in this context. Already the mobile phone and biometric payment authentication, between the power of one and the authority of the other, provide even greater capacity to organize the identification of individuals. Newer ID schemes have already breached the conventional distinction between the government and the commercial, domestic and international, and the inside and the outside. However, experts reckon that despite techniques being available, they have not been put together in the most effective way for the identification, classification, and management of individuals and groups sorted by 'level of dangerousness'.

Three specific areas have immediate potential. First, biographic search helps investigators look beyond singular physical identification characteristics. Second, biometric silos need to be turned upside down and provided with connecting passageways. Thus names, locations, faces, and other specifics can be looked at more holistically and intuitively, like a human mind would. Third, there is the hypothesis that identity itself is

not the final frontier of security; it is the knowing that there is intent. One of the important functions of an airport is segregating the streams among the frequent-flying "kinetic elite", the more general classes, the refugees and vagabond immigrants (some needing deportation), and finally those that need a closer look for security reasons. The aim is not only being able to foil their passage at arrival or departure, but also to keep the airport itself out of reach as a target. This gave rise to the current debate between behavior-based and identity-based techniques. Objections abound, and these too need to be addressed, especially those related to privacy, protection, due process, discrimination, and international law and conventions.

Already businesses, airlines and governments are imposing visible and invisible levies that support all means of security at the airport. With annual airport traffic projected to touch seven billion passengers via thirty-five million flights in one hundred and ninety-one countries, the nine thousand-odd airports where they originate and land assume more importance than ever before. Not one of them is known as Checkpoint Delta, but may the specter of Checkpoint Charlie long continue to remind us of the things that change and the things that remain the same. ☒

A longer version of this article was previously published in the Access & Identity Management Handbook 2017.

NEXT *generation* ID *solutions* for HEALTHY and STABLE SOCIETIES

An interview with Ulrich Walter, De La Rue

Silicon Trust is delighted to welcome UK-based ID solution provider De La Rue as a new member. With over 3,500 employees and 10 manufacturing sites globally, De La Rue is the world's largest commercial manufacturer of passports. Established over 200 years ago, the company has been driving innovation in the ID sector since the production of its first passport in 1915. The VAULT caught up with Product Managing Director Ulrich Walter, to get an insight into the company and its philosophy.

☐ *Mr. Walter, what role does identity play for today's society?*

Identity is one of the most important rights in the modern world. It provides protection, peace of mind and freedom for citizens and their governments. It is enshrined in the UN's Sustainable Development Goals – that every person should have a legal identity by 2030. For every individual, identity is a validation of who he or she is. But it also secures that person's rights, ensures their entitlement and access to social insurance benefits and public services and allows them to travel. Still, over a million children a week are born without getting a birth certificate. Fixing issues like this are critical to everyone in society

What does identity mean for the citizen?

In the modern world, our identity needs are many and complex. With an effective identity management system, a single citizen identity can be used across multiple applications, in order to provide an individual with entitlement and access to rights and benefits in their own country and across the globe. They also help to facilitate travel and enable inclusion in many civil and government programmes. Furthermore, an "e-identity" provides citizens with a digital identity, which is the core for online identification solutions in order to use governmental and commercial services – an ever growing important aspect of today's ID world.

A solid, secure identity management system not only provides citizens with more entitlement and more freedom, it also protects them. With the increase of cyber threats, citizens and governments are becoming acutely aware of the need for identities to be secure – across both physical and digital representations. We have spent over 200 years preventing counterfeit – it is in our DNA to stay one step ahead of people who attempt to create fraudulent documents.

How can technology enable a sustainable platform for secure identities?

We believe that flexible identity systems allow for effective governance and a healthy, stable society. Authorities can keep an accurate count of the population, understand who those citizens are and what they're entitled to. This enables governments to plan and provide for social benefits, education, healthcare and policing, and to effectively allocate their country's resources. Today there is a strong shift towards 'digital identity', which provides appropriate access to unique credentials from a single foundation. In addition, a range of highly protected documents can be issued, and a citizen's identity can be managed in a secure, adaptable way. But central to any successful identity management system is a secure and accurate data management system.

How important are developments in the travel industry?

The landscape of international travel has changed dramatically in recent years, due to the ever-expanding global population, increased travel, economic growth and a rise in personal income. Effective identity management facilitates the secure passage of citizens around the world, but also guards against potential abuses.

Terrorist activity brings with it a threat to identity, including the risk of terrorists travelling illegally under a false name. Economic, political and social problems have also led

> *"Today there is a strong shift towards 'digital identity', which provides appropriate access to unique credentials from a single foundation.*

to an increase in illegal immigration and trafficking. De La Rue believes, that these threats can only be tackled by making borders more secure and by keeping the management and protection of citizens' identities at the fore.

There is a lot of talk about digital IDs and mobile platforms. Do secure documents still play a role in identity management?

These are fantastic innovations, and are increasing consumer choice and flexibility. Central to any solution will always be the joint issues of security and durability. Despite the innovations we are seeing, the identity document is still central to managing citizen identity. Being compliant and up-to-date with the latest identity security measures provides nations with credibility and legitimacy on the international stage. The International Civil Aviation Organisation (ICAO) has set compliance deadlines to ensure global standardisation and interoperability of travel documents at borders. Furthermore, free entry to countries is further facilitated by regional agreements in areas such as the European Union and the East Africa Community. Finally we should not neglect the requirement for offline identification, e.g. at remote border posts, at street-side police controls or simply the need to place a stamp in a passport when crossing borders, despite all e-visa and other related initiatitives.

How is De La Rue positioning itself in the identity segment?

De La Rue positions itself as a global specialist in complete, integrated, end-to-end identity management solutions. We draw on our extensive experience and expertise in this field, and our knowledge of the issues facing citizens and governments. In the past few years we have dedicated a considerable amount of our R&D investments in our identity related capabilities. Our products integrate digital systems with the physical document itself. However, we understand that every nation's requirements are unique, so each of our identity protection solutions is completely tailored to your specific needs and challenges. Roughly speaking, we have three main areas of expertise in the secure ID space:

Digital Solutions, where we have created a complete, comprehensive digital identity management solution which simplifies what was previously a series of highly complex work streams, into a single sophisticated but user-friendly system.

Secondly, our range of secure identity documents, which are tailored to each nation's requirements. They are designed to counter specifically identified threats, using a sophisticated, seamless layering of protective features.

And finally, in terms of service solutions, we create fully bespoke packages that provide each country with an on-going support and advice service. This ensures that a country's specific needs and circumstances are addressed before delivery, during the implementation phase and throughout the full operational life of an identity management solution.

"With the increase of cyber threats, citizens and governments are becoming acutely aware of the need for identities to be secure."

We believe it is critical that every customer can be sure they will get the very best solution for their needs, so in addition to our fully integrated service offering, we can also provide some of the key component elements of an end solution – from the secure paper that is used to create Identity documents like birth certificates and passports, to the delivery of polycarbonate bio-data data page solutions.

What made you join the Silicon Trust?

The Silicon Trust is an excellent, well-established platform to exchange knowledge with many expert companies along the secure ID value chain. We are looking forward to being a part of this community, participating in the debates and working together to further educate governments around the globe about the benefits and challenges of introducing identity management programs. ☒

Infineon's security controllers set the new standard for long lasting secure eGovernment

› **Digital Hardware Security**
Integrity Guard with encrypted data processing in the CPU

› **Large Memory & Flexibility**
SOLID FLASH™ security controllers

› **High Performance**
World's fastest ePassport chip technology based on Very High Bit Rates

www.infineon.com/GovID

BRIDGING *the gap between* PHYSICAL and MOBILE CREDENTIALS

By Steve Warne, HID Global

In a world where many of our daily tasks and authentication needs are migrating to mobile applications, the number of physical ID cards distributed by governments continues to grow, despite the emergence of new convenient mobile identity solutions. So why are ID documents still predominantly physical cards? Will this change soon? Will mobile ID adoption see the replacement of physical cards?

☐ Global events such as war, terrorism, refugee relocation, economic migration and political change are driving the need for better identification of individuals. Governments are naturally considering how to securely identify individuals that live and work within their country or cross their borders for work, leisure or migratory purposes.

The instinctive reaction is to deploy physical identity cards that are well established and, in many places, widely accepted by the population. These cards are protected by physical security features, combinations of which, make them difficult to forge, particularly if these features can be further enhanced by personalisation.

For increased protection, many countries have deployed electronic identity cards (eIDs) containing additional security in the embedded chip. These credentials can be used to access governmental services via the chip. In countries like Estonia, it is now commonplace for citizens to identify themselves on Government websites or in Government offices using eIDs.

The challenge for physical identity schemes is how to verify document authenticity. Most cards are verified visually in either official or commercial use. The person verifying the card must be trained in the type and positioning of various card security features. Since only government officials generally have such knowledge, these cards have been a target of fraud in commercial applications. They are either forged or the fraudsters produce "pass-off" copies that resemble the genuine documents but aren't exact replicas. Where eID credentials have been issued, projects often do not realise their full potential due to the cost and complexity of delivering an electronic reader infrastructure that supports all document verification use cases.

Digitisation helps to overcome some of these issues and enhance privacy security and convenience for citizens, while use of third-party verification devices can reduce the need for specialised training when authenticating someone's identification. In fact, new technologies enable identity credentials to be enrolled, provisioned and used on mobile devices. Credentials are securely delivered to citizens' mobile phones, where they can be presented in a way that does not compromise security or privacy. This approach also gives citizens greater control over what identification information they share, in person or remotely, including over the telephone, on websites, or when accessing other digital services. For instance, they need not divulge their name, address or any other identifying information except age to a cashier when purchasing age-restricted goods.

Mobile credentials also lower deployment barriers by eliminating the need to create a reader infrastructure. In many cases, the mobile credential can be verified by another mobile device over a Bluetooth® Low Energy (BLE®) or near-field communication (NFC) connection. This verification process may also take place in an on-line or off-line scenario, with the BLE connection providing additional functionality for verifying at distances up to 30 metres.

As the real benefits of digital IDs are discovered, governments will adapt their single-purpose use into a multi-service model where a variety of functions are enabled through a single device. However, the advent of mobile credentials should not be considered the end for physical documents. Identity and travel documents are defined by numerous standards that ensure commonality of authentication and encryption approaches, and they do not yet exist for digital credentials. It could be several years before these standards are completed and mobile credentials are widely accepted as IDs or proof of privilege. Additionally, the functionality and security of mobile identity relies on the use of smartphones, which are not universally carried by citizens and the distribution of which varies greatly across demographics.

"The advent of mobile credentials should not be considered the end for physical documents. Identity and travel documents are defined by numerous standards that ensure commonality of authentication and encryption approaches, and they do not yet exist for digital credentials."

With these challenges to the adoption of mobile identity, there is a need to bridge the gap between the physical credentials of today and the mobile credentials of the future. New solutions need to evolve which will allow the issuance of a physical or mobile credential, or both, from a single source. These credentials then need to be efficiently authenticated via a single verification infrastructure. Ideally, this infrastructure will be low cost and easily distributed, such as an app on a mobile phone or a simple, low-cost hardware device.

Even when mobile IDs are widely accepted, there is a good case for their co-existence with physical credentials in the long term, primarily to increase security and trust. The physical document could be used as the "trust anchor" for the enrolment of a citizen to a mobile scheme. For example, a multi-factor authentication strategy would then require both a physical and mobile credential to access a secure government website or an individual's health records.

Governments are looking at new approaches to enhance citizen identity schemes. Physical ID cards will continue to be widely used as the primary source of identity documentation – at least for now. At the same time, the use of mobile citizen ID credentials is gathering pace as Governments seek to improve convenience and communication with their citizens. Smart solutions to enable the smooth transition to mobile enabled credentials need to be developed which respect the requirements of citizens and governments, while still delivering a high degree of security and trust.☒

"ARE YOU LOOKING AT ME?"

Face Recognition Technology for Automated Border Control at Venice Airport

By Elke Oberg, Cognitec Systems

☐ Cognitec's automated passport control product FaceVACS-Entry features in eight ABC gates (eGates) at Venice Marco Polo Airport, following the airport's decision to facilitate expedited border control checks at the international terminal. The eGate implementation project was delivered by N-Aitec, an airport IT provider and system integrator.

As the traveler enters the eGate, FaceVACS-Entry detects the person's face, adjusts the position of the cameras according to the person's height and then captures best-quality images that guarantee high verification accuracy. The software instantly verifies the live images against biometric photos stored in passports or other ID documents, and a confident comparison result opens the gate door.

Since the initial rollout in July 2015, more than 600,000 passengers have used the self-service eGates for immigration processes, with four gates serving arrivals, and four gates the departure area. Venice airport sees a growing number of travelers favoring the speed and usability of the automated procedure.

"Our partnership with N-Aitec contributes to further development of face recognition technology for automated border control. We are excited to see such positive eGate user response, and look forward to working on more installations at Venice airport," says Alfredo Herrera, Cognitec CEO.

"We are receiving positive feedback from eGate users," says Corrado Fischer, COO at SAVE, the Venice Airport management company. "We started with two gates in 2015, and now a total of eight is placed in the arrival and departure areas, as we experienced their high reliability and impressive throughput—this is why we are planning to further increase the number of eGates and offer a better journey experience for all our passengers." ☒

FaceVACS-Entry combines smart hardware for facial image acquisition with market-leading software for verification processes, and is ready for integration into electronic gates (eGates) at border control checkpoints.

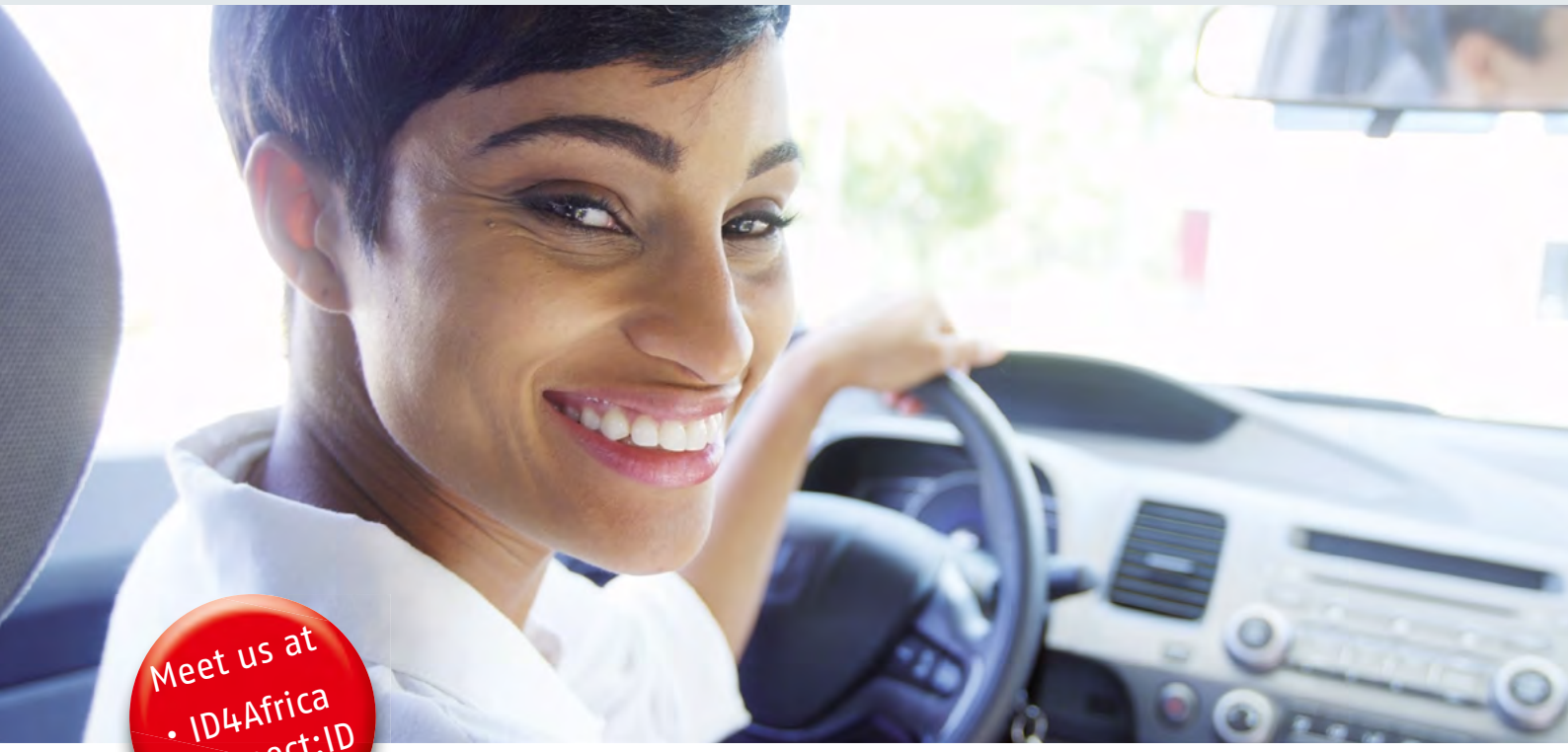
The latest software release, FaceVACS-Entry 5.3, includes Cognitec's current matching algorithm B10 and generates higher accuracy rates for passport images with low resolution and other image quality problems. Cognitec also optimized the performance of FaceVACS-Entry's unique presentation attack detector, which recognizes fraudulent attempts to use photos, videos or masks.

Cognitec also improved various user experience features. Persons entering the gate can overlay the moving contour around their live facial image with a static head silhouette in an optimal position for face recognition measures. The display also alerts users to remove sunglasses. Additional feature upgrades provide system administrators with more streamlined calibration and configuration procedures.

Since the introduction of FaceVACS-Entry in 2014, Cognitec has spent significant development efforts to advance product utilities and respond to increasing demand for accurate, fast and convenient face recognition technologies at borders.

MASKTECH

We make chips intelligent



Meet us at
• ID4Africa
• Connect:ID
• SDW

MTCOS® – ID CHIP SOLUTIONS FOR eGOVERNMENT APPLICATIONS

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

SecurITy made in Germany

Common Criteria

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

A NEW *Encryption Paradigm* for a NEW INDUSTRIAL AGE

By Daniela Previtali, Wibu-Systems

Long before encryption became a commonplace feature of even consumer computers, while computers were still mechanical contraptions and encryption the domain of military cipher clerks, Auguste Kerckhoffs published two articles on the subject in the "Journal des sciences militaires" in 1883. He proposed several principles, one of which remains fundamental for modern cryptography: "The system should not require secrecy, and it must not be a problem if it falls into enemy hands." Put more simply: Let the enemy know the system, as long as they don't know the key!

In essence, the dictum that became known as Kerckhoffs' Principle states that the strength of the encryption system should depend on the key being used, not the secrecy of the system. The system can and should be public knowledge. Even if the enemy, be it a military adversary of yesteryear or a modern software pirate, can access it, he would still lack the key to break it. At the same time, it is also open for researchers to analyze, challenge, and make it stronger.

Even now, more than a century after Kerckhoffs proposed his eponymous principle, most security depends on keeping the systems hidden from the public. "Security by obscurity" is the much-maligned, but still widely followed paradigm in the software industry and beyond. Maintaining secrecy about the technology has its advantages, and even strict adherents of Kerckhoffs do not suggest that all encryption mechanisms needs to be laid bare. Still, an approach that puts all of its trust in secrecy cannot be independently verified: Security by obscurity also means an obscure level of security.

"An approach that puts all of its trust in secrecy cannot be independently verified: Security by obscurity also means an obscure level of security."

What makes a system truly secure?

For us to know whether a system is secure, two factors need to be present: The security property needs to be described precisely, and it must not rely on assuming many restrictions on the attacker. An attacker might not only have access to the encrypted text, but also the plaintext, or he might be able to interfere with either end of the communication, as happened in the famous case of the captured Enigma machine. While the system – the rotors – was a closely guarded secret, the code breakers at Bletchley Park managed to crack it, because they knew part of the plaintext – tiny bits of the message they had guessed correctly.

True security depends on encryption whose strength is mathematically provable, not conjectured by trust in an obscure system. To be demonstrably "hard to solve", it has to become exponentially more difficult as its scale increases. Today's 2048-bit encryption is virtually impossible to crack with the current limits on computational power. Modern encryption systems should be published with demonstrable security properties of this nature, and by fact of being published, they are open to being validated or indeed invalidated. This makes them truly Kerckhoffs-compliant.

Laying open the Blurry Box

For Industry 4.0, strong encryption can have make-or-break impact, opening entire new business models and revenue streams or exposing intellectual property and business-critical data to hackers, pirates, or saboteurs.

"For Industry 4.0, strong encryption can have make-or-break impact, opening entire new business models and revenue streams or exposing intellectual property and business-critical data to hackers, pirates, or saboteurs."

Wibu-Systems has pioneered the Blurry Box technology with this need in mind, fully compliant with Kerckhoffs' Principle and demonstrably hard to solve. The essence of Blurry Box encryption lies in how it handles the function blocks that constitute a piece of software.

Blurry Box splits each function block into several variants, which return the correct output of the original unencrypted function only for a specific input set. A wrapper function maps these

inputs to the variants, which are encrypted with separate keys stored on a dongle. When the software is executed, the system only decrypts those variants that match the given input. Hackers will only ever see that part of the code that matches the previous input.
In traditional encryption, hackers could work their way through the function blocks in what is called a copy-and-paste attack. However, even if a hacker captures individual variants, the principle of inherent complexity demands that the protected program is so complex that no hacker can derive additional variants from a specific subset that may become known to him. In essence, Blurry Box does not depend on making copy-and-paste attacks on individual variants impossible, but on making the attack strategy as a whole unfeasible.
Special traps are included should an attacker attempt to simply force his way through the variants. Once triggered, the trap locks the dongle, which also happens when illegal sequences are detected. This stops hackers from simply retracing a few steps without running the entire process (with the effort and complexity this entails) from the beginning.

Made for Industry 4.0

Blurry Box encryption has great potential for Industry 4.0 environments. The rise of the interconnected industry has created many tempting targets for cyber-attackers wishing to cause damage or steal know-how. The situation is already alarming: According to the Product Piracy Study 2016 published by the German engineering federation VDMA, 9 in 10 industrial machine manufacturers have already fallen prey to pirates.
Preventative measures against these naturally include encryption, as showcased at the demonstration platform SmartFactoryKL, where innovative connected manufacturing technologies are tested with secure communication, using cryptographic keys stored in secure elements. Invaluable data like product designs or machine settings are digitally signed and stored on RFID tags and verified via the cloud. The machines cannot be tampered with and only accept data from authorized sources. The new controls are a boon for sectors of the market heavily affected by product piracy or the revenue-depleting competition of the grey market, like the fashion industry.
Many modern IoT devices are reliant on microcontrollers to deliver their functions. Their makers can include protection mechanisms in their development toolchain and secure their firmware to prevent later tampering or enable such commercially indispensable features as production volume controls, secure updates, or the remote activation of add-on features.
This creates new after-sales potential and allows for completely new business models.
The potential of secure protection and licensing is not limited to the manufacturing industry. Many other sectors are experiencing a shift from hardware-dependent to software-realized functionalities: Innovative medical technology firms are beginning to offer their devices at low entry prices, giving medical professionals in the emerging markets and smaller healthcare facilities everywhere access to cutting-edge therapeutic and diagnostic equipment. They can then offer add-on functions as paid upgrades or with pay-per-use schemes. All this is made possible, secure and fully compliant with the strict standards in the industry, by a sound licensing system.

"Many modern IoT devices are reliant on microcontrollers to deliver their functions. Their makers can include protection mechanisms in their development toolchain and secure their firmware to prevent later tampering or enable such commercially indispensable features as production volume controls, secure updates, or the remote activation of add-on features."

Conclusion

An encryption mechanism that is true to Kerckhoffs' Principle represents a genuine seismic shift away from deceptive "security by obscurity" towards genuinely open, but strong protections. The secure and flexible licensing and encryption capabilities provided by Wibu-Systems are a game changer in the field.☒

Global Hacking Competition

In the true Kerckhoffs' spirit, Blurry Box effectiveness and methodology are being tested in the field. At the opening of the Hannover Messe, Wibu-Systems has called all hackers around the world to crack an application protected with Blurry Box. Results will be made available at www.blurrybox.com.

mikron

Learn more at: **www.mikron.ru/en/**

Microelectronics production since 1964

- Secure microprocessors for smart cards and ID documents
- RFID chips, tags and inlays: brand protection, retail and library labeling, manufacturing and spare parts labeling, medical ID bracelets, event passes, etc.
- Transport applications: tickets and cards, tags, CAMs

MIKRON is an exclusive supplier of microchips and cards for Russia's state infrastructure projects: e-passport program, national payment system (MIR), Moscow public transit system.

Headquaters
Mikron JSC
1-y Zapadny Proezd 12/1,
Zelenograd, Moscow,
124460, Russia
Phone: +7 495 229 74 89
E-mail: globalsales@mikron.ru

Representative offices:
USA
Germany
China
Hong Kong
Taiwan

Citizen Identity Management
A view of the market

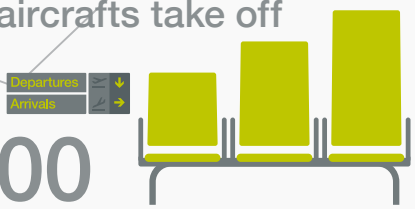
Citizen Identity is a critical issue in the modern world

By 2100, the number of people on Earth will be

11.2 billion

Every 60 seconds,

52 aircrafts take off



5,700 passengers board an aircraft

The rate of births is

4.3 per second
367,200 per day
15,300 per hour
11,383,200 per month

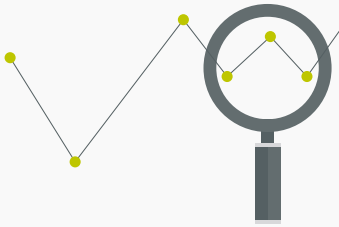
That's an average of

8 million

people travelling every day

There are a number of key challenges to get right

A different approach is required if these challenges are to be solved.



1 Mass migration is the new normal

In the first **7 months** of 2015 the EU received

4 times as many first time asylum seeker applications as it did for the entirety of 2008. But this still represents less than **3%** of the world's displaced population.

A global challenge needs a global response

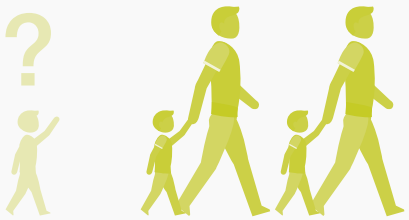
- Global focus on tackling the barriers to realise a legal and secure identity for every person on the planet
- Globally consistent standards for data matching and token security across all regions and travel types
- Specific global approach to identity issues driven by forced migration
- Country-specific roadmaps for enhanced eGovernment services

Sources: Index Mundi, CIA World Fact Book, Plan International, World Bank, United Nations, World Tourism Organisation and World Health Organisation.

The UN estimates that the number of forcibly displaced people is now greater than

60 million

Over **250,000** people per week leave their homes to seek protection



1 in 3 children under five do not officially exist. That's

230 million

children with no identity and who will struggle to access education, health care and social security.

2 The right foundations are essential

Existing infrastructures often hold multiple identities for a single individual.

Ensuring that secure and effective birth registration and death certification in place is essential.

3 Recognise that each country is unique

Countries are facing different challenges driven by their legacy systems and technology infrastructure.

Our Focus

De La Rue are global specialists in citizen identity management, we deliver passports and national identity services, eGovernment and complete identity data management solutions, appropriate to specific needs and individual requirements.

Want to know more? Talk to us. www.delarue.com

UTILIZING the *synergies between* PASSPORTS and eID CARDS

By Veronica Atkins, Silicon Trust

When Infineon's Detlef Houdeau delivered a speech in March 2017 in Baku, Aserbaidschan, he hit a nerve with the delegates of the High Security Printing conference. Representing Eurosmart's Cybersecurity and Digital Identities Committee, Dr. Houdeau made a strong case for recognizing and utilizing the existing synergies between ePassports and eID Cards.

The fast digitization of society continuously brings new challenges to the public sector, its offerings and its service infrastructure. Electronic identification (eID) allows citizens to access online services, using, for example, a secure token in the form of an ID card. During the last two decades, governments all over the globe have defined, specified and started the roll out of eID card schemes, in order to enable their citizens secured access to online services, as well as highly secured documents for personal verification.

Implementing an eID card scheme is a massive investment for any government, especially if eID cards and electronic passports are implemented as separate projects. Thankfully, standardization as well as technology and processes across the value chain allow governments to consider implementing a family concept for both ID1 (card) and ID3 (passport booklet) formats.

ICAO Doc 9303 Machine Readable Travel Documents

ICAO's initiative to develop standard specifications for passports and other travel documents followed the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organisation. ICAO's mandate stems from the Convention on International Civil Aviation (the "Chicago Convention"), which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls.

ICAO Member States have recognized that standardization is a necessity and that the benefits of adopting the Doc 9303 standard

Using the example of the Dutch ePassport datacard and ID card, one can recognise the similar optical design. Integrated within both documents are the same optical security elements (level 1, level 2 and level 3). Both documents carry the same electronic functionality (ICAO 9303 standard) and the same biometric data, stored in the chip (face, since 2006, plus 2 fingerprints since 2009)

formats for passports and other travel documents extend beyond the obvious advantages for states that have the machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer strong defense against alteration, forgery or counterfeit. The adoption of a standardized format for the visual zone of an MRTD (Machine Readable Travel Document) helps airline and government officials with the inspection process.

In terms of protection against tampering and fraud, the optional introduction of biometric data stored on a contactless security chip will provide greater protection and facilitate the use of automatic border control (ABC) systems.

The ICAO 9303 standard has been deployed for travel documents incorporating technology standards such as ISO/IEC 19794 for biometrics and ISO/IEC 14443 for the contactless interface, as well as application standards for travel documents, like passports (ID3 format), Residence Permit cards and Registered Traveller cards.

> *"Implementing an eID card scheme is a massive investment for any government, especially if eID cards and electronic passports are implemented as separate projects."*

Also, since 2006, the ICAO standard has also been applied increasingly for national eID cards (ID1 format). This has political and legislative implications, some application effects as well as an impact on production and of course, it affects the electronic, contactless interface of the card.

Overview on booklets with ID3 format PC holder page – status in 03/2017

Albania, Antilles, Armenia, Azerbaijan, Brunei, Hong Kong, China, Macau, SAR, Colombia, Croatia, Czech Republic, Denmark, Finland, Germany, Hungary, Ireland ,Latvia, Lithuania, Luxembourg, Macedonia, Malaysia, Montenegro, Netherlands, New Zealand, Norway, Panama, Poland, Portugal, Romania, Russia, Serbia, Singapore, Slovakia, Slovenia, Republic South Africa, Sudan, Sweden, Switzerland, Tajikistan, Thailand, Turkmenistan, Ukraine, Venezuela

The following countries start soon:

Brazil, Egypt, Island, Indonesia, Italy, Myanmar, Saudi Arabia, Spain, USA

References on ICAO-MRTD data set in ID1 documents.

The following states use ICAO data sets, biometric, security and interface in ID1 documents in the public domain (alphabetic order):

Albania, 2007	Monaco, 2008
Germany,* 2010	Netherlands, 2006
Hungary, 2016	Sweden, 2005
Italy (2nd Gen), 2017	Turkey, 2016
Lithuania, 2009	Ukraine, 2016

* Note: Germany needs another authentication protocol than ICAO (TA authentication first, followed by CA authentication).

Synergies in production, infrastructure and document security

Synergies between the 2 formats can be found in document production, in equipment procurement, as well as in the process workflow. Both ID1 and ID3 polycarbonate lamination use equipment for both multiple printed panels, the process for lamination applies to both formats with the stacked layers.

When it comes to PC foil printing and finishes, such as hologram and transparent foil, the same equipment and workflow is applicable.

"In terms of protection against tampering and fraud, the optional introduction of biometric data stored on a contactless security chip will provide greater protection and facilitate the use of automatic border control (ABC) systems."

In terms of the key management infrastructure with the purpose of creating and handling keys and certificates, a connected network is required for both formats. In the same way, equipment for capturing the biometric data, such as scanners or cameras, can be used by the registration office also for both document types. Equipment for optical and electronic personalization is available on the market, which can work with ID1 and ID3 documents in mixed mode.

A family concept for both ID cards and passports can be applied when it comes to the optical security concept for a country's documents. All security levels are applicable to both formats, such as rainbow pre-print, UV-mark and special holographic foils.

Synergy in teaching and training of authorized persons

The examples above give a good indication how a cross-format ID family concept can be utilized when it comes to document production and ID infrastructure. However, governments and institutions that opt for a family concept when implementing their national ID document strategy, can utilize synergies beyond the production process.

Take, for example, national ID registration and issuance centers: When rolling out an ePassport project, each center requires a complete solution set – hardware, software, maintenance – even though, on average, only about 30% of the population will ever apply for a passport. If a government decides to use the existing set up also for national ID cards, the efficiency and return on investment is much higher.

Once the documents are issued, also the training and teaching modules of the personnel in charge of border security and immigration, as well as for national eServices, could be offered for both formats: eID card in ID1 & passport holder page in ID3.

"The re-use of this standard into other documents beside ID3 booklets, such as ID1 card and Residence Permit card can reduce cost, effort and time for production, for infrastructure, for training and for the forensic lab."

Use cases for ICAO data set, biometrics, electronic security and interface

Five different document types use the ICAO 9303 Standard:

1. Passport, ID3, eMRP in more than 120 countries worldwide
2. ID-Card, ID1, National eID-Card in more than 9 countries worldwide
3. Residence Permit, ID1 in more than 50 countries worldwide
4. Frequent Traveller Card, ID1, China & Macao; China & Hong Kong
5. Seafarer Card, ID1, Myanmar Pilot, start in 2017; based on the ILO recommendation.

Conclusion and outlook

The ICAO 9303 standard has been well defined since 2004. To date, more than 100 Mio documents, based on this standard, are issued every year. This standard captures a comprehensive data set (LDS1.7), document reading security (e.g. BAC), stored biometric data & quality (ISO/ IEC 19794) and the used interface (ISO/IEC 14443); The re-use of this standard into other documents besides ID3- booklets, such as ID1 card and Residence Permit card can reduce cost, effort and time for production, for infrastructure, for training and for the forensic lab. For the end customer, the benefits are in the application. For example, when entering and leaving states where an additional visa or entry/ exit stamp is not required, the citizen has a choice. He or she can leave the passport behind and use the eID card with the ICAO-standard for travelling and for ABC systems at the border. This means less hassle and more convenience with a standard wallet-friendly ID1 card format. ☒

VIRTUAL TOKEN *– A smart card alternative* that makes SENSE?

By Klaus Schmeh, cryptovision

Why use a smart card, if a secret key can also be stored in a virtual token, i.e. a protected hardware module built into a PC or smart phone? The Trusted Platform Module (TPM) and Intel's Software Guard Extensions (SGX) are two technologies that can be used to build solutions following this approach. Will virtual tokens make smart cards obsolete? Or are they useless, as they miss the point of what smart cards are all about? As will be shown, the truth lies somewhere in between.

The times when a smart card was just a plastic card bearing an integrated chip are long gone. Meanwhile, over a dozen smart card form factors are available, ranging from USB tokens via microSD cards to contactless chips integrated into wristwatches. In addition, it is possible to give up the concept of storing a key on a small item the user can carry with him and, instead, keep this secret information in a protected module inside the end user device (usually, a PC or smart phone). In other words, the key storage place is transferred from the user's pocket to the motherboard. This approach is referred to as "virtual token". A virtual token represents a smart card form factor of its own.

Virtual tokens

A technology that is well suited for implementing virtual tokens is the Trusted Platform Module (TPM). A TPM is a protected hardware module available in most current computers. TPMs are mainly known for supporting software attestation, which is an important countermeasure against malware. In addition, storing secret keys in a protected way is one of the base functions of a TPM. To turn a TPM into a virtual token, a smart card emulation software is necessary that grants access to the keys via a standard card interface. Using a TPM as a virtual token is already common practice and by far the most popular solution for this purpose is Virtual Smart Card (VSC), a technology provided by Microsoft.

Just like a TPM, Intel's Software Guard Extensions (SGX) are suited to realize virtual tokens. SGX is a proprietary set of features supported by many Intel processors. The general purpose of SGX is to provide protected areas (enclaves) to programs running on a PC. Data stored in an enclave are not accessible from outside, not even for the owner of the computer. Typical applications of SGX include malware protection (data stored in an enclave cannot be manipulated by a malicious software) and digital payment with an enclave providing a tamper-resistant environment for handling money transactions.

In addition, SGX supports storing secret keys in a protected environment. If an appropriate emulation software is used, an application program can interact with an SGX-protected area, like with a standard smart card. SGX thus becomes the core

> *“smart cards are indispensable when it comes to implementing electronic identity cards, company cards, digital signature cards, or multi-application cards. On the other hand, a virtual token is the more pragmatic solution – cheaper and more user-friendly.*

part of a virtual token and even has some technical advantages over a TPM in terms of the crypto algorithms supported.

However, SGX-based virtual tokens are still in their infancy, with no market-ready solution being currently available. Ralf König, Product Manager at smart card specialist cryptovision, says: “At cryptovision we have plans to change this situation. We expect to have an SGX-based virtual token ready by 2018.” As a first step in getting familiar with the SGX technology, cryptovision has implemented a credential storage based on SGX together with Intel. It is one of the first SGX applications on the worldwide market.

It goes without saying that a virtual token is not a one-to-one replacement for a conventional smart card. It can even be said that a built-in security module that is not removable contradicts the basic idea of a smart card, which is to separate the key from the device that uses it. It is clear, for instance, that a key stored in a processor register or TPM of one computer cannot be used on another. If a computer is stolen, not only the device, but also the key is compromised. For this reason, a virtual token is considered less secure than a conventional smart card.

On the other hand, storing keys inside a computer device – yet within the borders of a protected module – has a number of clear benefits. Essentially this approach saves money, as it relies on existing hardware, while a smart card solution always requires purchasing one card per user. In addition, virtual tokens are more user-friendly, as a user doesn’t have to bother with a card and he can’t lose it. Finally, although a virtual token is deservedly not considered high security technology, it has some security benefits. For instance, it is a lot more difficult to steal a built-in hardware module than a smart card and as a further benefit, smart card sharing, which is illegally practiced in many organizations, is a non-issue.

Two approaches that don’t compete

A look at these arguments makes it clear that conventional smart cards and virtual tokens should not be regarded as competing technologies. Instead, each variant has its benefits. Smart cards, including form factors like USB tokens or proximity tokens, are to be preferred if a mobile key storage device is desired and if high security standards need to be met. For instance, smart cards are indispensable when it comes to implementing electronic identity cards, company cards, digital signature cards, or multi-application cards. On the other hand, a virtual token is the more pragmatic solution – cheaper and more user-friendly.

cryptovision Product Manager Ralf König states: “Pragmatic solutions have always been successful in the IT security world. We therefore take virtual tokens very seriously.” In spite of these new form factors, Ralf doesn’t see conventional smart cards under threat. “We expect that billions of people worldwide will be equipped with electronic identity cards in the decades to come. For this purpose virtual tokens are not an option.” ☒

AUSTRIACARD

Your Expert for Cards and Beyond

New IoT TECHNOLOGY and *a solid* CHAIN OF TRUST

By and with Andreas Philipp, PrimeKey

How do we realize the benefits of a totally connected world? The paradigm of the IoT focused IT industry is that in the future, everything that can benefit from a connection will be connected. We are only at the beginning of this transformation but even so, Gartner says that by the end of 2017 up to 8 billion devices will be in use worldwide.

☐ The IoT market consists of multiple ecosystems with a high level of complexity. These ecosystems have multi-layer models with hundreds of players - from device vendor and communication service provider, down to the IoT platform software vendor and the IT service provider companies. There is also the collision of Operations Technology (OT) and Information Technology (IT) departments within the enterprises themselves.

But at the end of the day, they all have one common requirement: the demand for trust in the Devices, the Application, and the underlying Infrastructure. In order to create this and to build a bridge between the IT and OT World, there is definitely a need for a solid chain of trust, from the trustworthiness of the Devices and all the way up to Infrastructure.

In the past, it has been sufficient to protect cryptographic key material and its application, but with the new upcoming trends in IoT and Cloud, it becomes increasingly clear that this is not sufficient anymore. Rather, protection must be extended to applications, protection against manipulation, theft, copying or counterfeit. Only with this step will it be possible to build the basic trust foundations on which a stable IoT can be developed and grown.

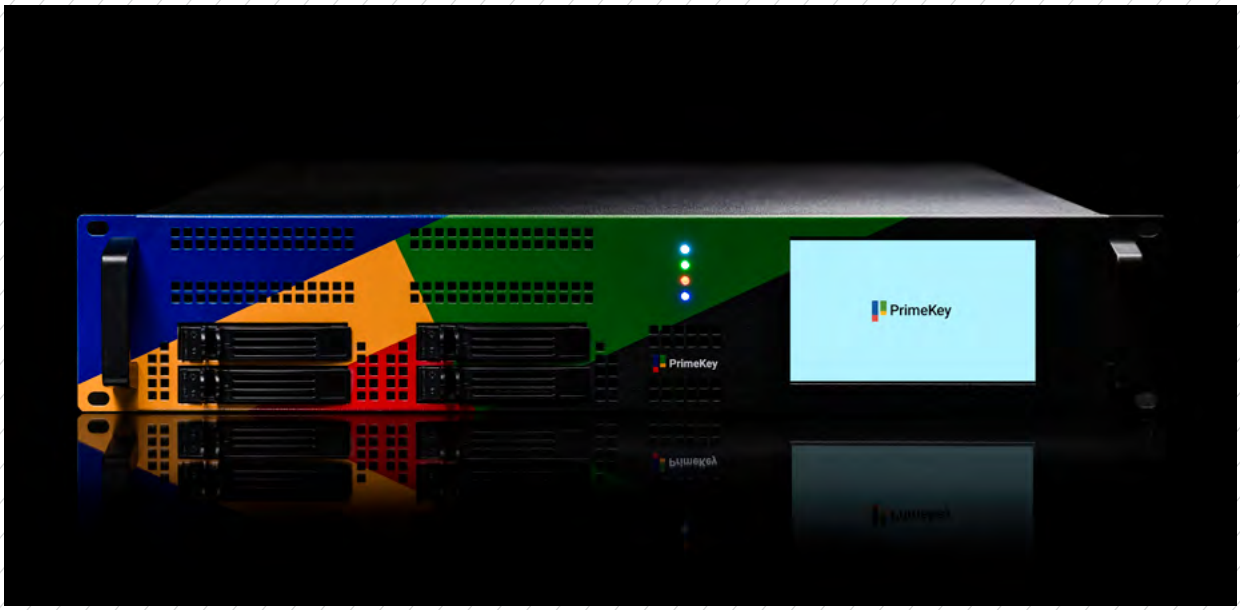
Mr. Philipp, you have just joined PrimeKey. What are your thoughts on their SEE offering?

I have been working with hardware security modules and applied cryptography for more than 20 years and was really excited when I saw the brand new SEE platform by PrimeKey on the RSA show this year. For me, it answers the questions of creating the necessary solid chain of trust urgently needed for IoT. This is ground breaking technology and I wanted to be part of it, which is why I recently decided to join PrimeKey as the Business Developer for the SEE platform.

So how have the first reactions on the SEE been in the market?

Very confirming! I have found that after we've explained the concept of the platform to companies in different sectors and segments, they immediately start discussing ideas for development of application scenarios. This ranges from an extensive authentication solution over personalization platforms, up to the multimedia DRM system.

Knowing the security market well, and having introduced the SEE platform to companies, I am sure that the next success stories can be created by the end of the year. Keep your eyes open and you will see just how the SEE's performance can enable the chain of trust in a growing and everchanging IoT market.☒



Protect your application

The PrimeKey SEE is a full-size rack-mount application server that comes with a patented FIPS protected execution environment for any operating system and application. It ensures that the server runtime environment can only be accessed by an authorized security administrator at all times, making it impossible to access, to extract or to modify by an unauthorized party. By doing so it opens up a new world of possibilities where you can run each mission-critical application in any uncontrolled environment.

Prevent software and data theft

No need to fear that someone will steal or copy your software. You can now deploy your product in places with public access or where you fear that someone would be interested in extracting your software with untoward outcome for your business. With PrimeKey SEE you can place your software wherever it benefits further advances of your business.

Prevent manipulation

If your software controls sensitive information or functionality, you know the consequences that an undetected malicious modification can have. Your IoT device might be hacked, your data compromised or your machines stop working. With SEE you can sleep soundly, as no one can access or modify your software and data.

LINKING the IoT and the DEVELOPING WORLD

By Richard Eyo, Department of Mathematics and Information Security
Royal Holloway, University of London

The Internet of Things (IoT) is here to stay. Therefore, the major focus of this article is to bridge the gap between IoT and the developing world. One of the motivating factors is that most IoT devices have become vulnerable to a series of attacks, thereby threatening safety, security, privacy and even the lives of the end users. We suggest that if governments from the developing world are considering developing IoT frameworks, there is a need for more participatory groups, such as regulatory bodies, professional groups, academia, and civil societies, in order to achieve a safe and smooth implementation. These frameworks, when developed and implemented, will help to "check-mate" inferior products that have been or would be poorly manufactured by the IoT vendors, thereby ensuring no compromise of safety, security, privacy, and interoperability.

☐ Introduction

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. It is a global network that connects physical devices such as household equipment (e.g. refrigerators, kettles, washing machines etc.), buildings, electronic devices, vehicles, medical equipment and manufacturing machines, which are embedded with sensors, network connectivity, software and actuators, which aid in communication and exchanging information to and from devices either through Radio Frequency Identification (RFID) or in more advanced ways (e.g. WiFi). The unique thing about the IoT is that each device will be identified and recognized in the network and could be controlled remotely.

It is expected that 50 billion devices will be connecting together by 2020, although to individual persons or organizations, IoT is seen from a different perspective either as services or technologies etc.. Irrespective of their viewpoints, the primary objective is to make sure that either they provide services or buy services from others by connecting physical objects, sensors, actuators and the Internet together. According to IBM, “every company, every city, every country - every individual - is increasingly interconnected with millions of others; the cost of a bad call can be devastating. But analytics is increasingly helping business and government leaders look beyond their own biases to discern real patterns and anticipate events”.

Supporting ITU - Connect 2020 Agenda in the context of the IoT

ITU - Connect 2020 Agenda has been created to work towards the shared vision of "an information society, empowered by the interconnected world, where telecommunication/ICT enables and accelerates socially, economically and environmentally sustainable growth and development for everyone" and invited all stakeholders to contribute with their initiatives and their experience, qualifications and expertise to the successful implementation of the Connect 2020 Agenda. In order to support ITU Member States in the context of IoT achieving these goals, we will point out some of the challenges that need to be addressed, so as not to hamper the adoption and deployment of IoT in the developing world.

This is achievable if there is trust between the manufacturers of the devices, the users and the IoT devices. By that, I mean the architectural designs, network infrastructures, interfaces for communication, security and safety of the users, standards, policies, and guidelines to regulate the manufacturers and the service providers of IoT should all be in place, otherwise IoT will affect lives negatively.

Challenges of IoT deployment in developing nations

Consider the issue of existing technologies (e.g. electricity, Internet), where many developing countries are still struggling without constant power supply in terms of generation and distribution. Unlike developed countries, where the power sector is fully managed, privatized and regulated through standards and policies, in developing countries, this is more difficult and leads to serious weaknesses. Also, the process of capacity building and establishing adequate regulatory institutions has been a slow and complex one, lagging behind the entry of private operators in the electricity sector, and of course we all know the importance of electricity, as it plays a major role in the smooth operations of IoT.

Again, in most developing countries there is poor and limited internet connectivity, as, for example, in Nigeria. In my own experience, I have seen people subscribe to more than three ISPs. Not that they have so much money to do so, but because they are exposed to the trend of new technologies and are very eager to explore it. It is rather unfortunate and particularly frustrating seeing someone with sophisticated and expensive mobile devices where, due to poor services from the Mobile Network Operators (MNOs), the devices are useless in their hands. This is also because there are no strong standards and policies to keep the service providers on their toes and upgrade their services to a standard comparable with developed countries.

Another important aspect, is that some IoT manufactures are in it for making a profit, but not ready to significantly invest in research. In my own opinion, such manufactures may not have the necessary guidelines - starting from the design, testing, to the implementation phases. There could be a tendency that those devices, which were not initially designed to connect, may be poorly reprogrammed with embedded hardware along the way in order to do so.

Therefore, there should be standardisation and regulatory bodies that regulate and certify the products, to ensure that they meet the relevant standards at all stages, before they are rolled out for use.

> *The architectural designs, network infrastructures, interfaces for communication, security and safety of the users, standards, policies, and guidelines to regulates the manufacturers and the service providers of IoT should all be in place, otherwise IoT will affect lives negatively.*

Safety, security and privacy of the users

Do IoT manufacturers have the safety, security, and the privacy of the users in mind during the design phase, and to what extent? Governments and utility companies are rolling out smart metering in order to improve energy consciousness and efficiency in supply and consumption. Hospitals are introducing wearable devices to monitor the health of their patients, automobile industries are producing vehicles with IoT–enabled sensors and so on.

These devices must connect to one another in order to share services. Therefore, there is a possibility that the devices could be hacked by criminals, where vital information regarding safety, security, and privacy of both the devices and the users is revealed. This could become a matter of life and death, if, for example, an IoT-enabled vehicle is hacked and the location of both the vehicle itself and the driver/owner is revealed to the hackers. Criminals could use the information to track the owner's movements or even manipulate some important components of the vehicle either for fun or for more sinister motives.

What if, in the case of hospitals, IoT drugs dispensary equipment, which is linked to every patient's record and connected to their wearable IoT devices for effective monitoring, is being hacked? This could be devastating to both the patients and the hospital. The life of the patient is at considerable risk, since the hacker has the patient's medical record and therefore knows the timing and dosage of the patient's next treatment. This gives the hacker enough information about the patient and the type of sickness, to enable him to change the type and dosage of the medication, save the record afterwards, and leave the wrong prescription for the next medical practitioner who takes over.

The hacker's intention could be to frustrate the hospital by damaging their reputation, to intentionally kill a patient, or to get the patient's information for the financial benefit of a third party. Of course, seeing the type of drugs dispensed to a patient will inform the hacker the nature of the patient's sickness, and therefore abuses the patient's safety, security and privacy.

Dumping of rejected or banned IoT devices on the developing nations.

In recent times, there have been a series of complaints from developing nations concerning incessant dumping of banned and sub-standard products from manufacturers. In the medical/health sectors, for example, Nigeria and Uganda have raised concern over poorly calibrated, old machines being given to their hospitals as "donations". India has blamed China for exporting sub-standard, low-priced equipment to their country. China has complained to Western and Japanese medical device makers about them selling dialysis kits at exorbitant prices in comparison to indigenous versions. A 2012 report in The Lancet showed that about 40% of healthcare equipment in poor countries is out of service, mainly because of ill-conceived donations. As an example, an oxygen concentrator, donated to a Gambian hospital, worked on a voltage incompatible with the country's power supply.

If proper measures are not being taken, it is obvious that more of these incidences will occur in the very near future as far as IoT is concerned, as the developed nations with strong and standardised bodies will ban or reject sub-standard goods and services from entering their countries. Of course, there are many reasons that could lead to the banning of IoT devices, such as safety, security, privacy, environmental, technological, compatibility concerns etc. And the options for the IoT vendors would be to either ship the sub-standard devices as they are,

or to refurbish them and send them to developing countries, where there is very little or no regulation, in order to not lose out completely. These device shipments could be in the form of a donation, just to create a relationship with a country for subsequent business.

The danger here, is that when such goods and services are banned from the developed world, the manufactures will rush to try and cover up the mess by updating the devices. So, if the updates are not sufficient, they will stop production, since the cost of an update could be more than the cost of producing new devices. And what happens to the hundreds of thousands of devices already in circulation? There will be no updates, as the products would be unsupported or end-of-range. Again, the sub-standard devices could become a back door for hackers to get access and steal the end user's personal information.

On the other hand, the IoT vendors stand greater chances of losing their trust, reputation and integrity, if such flaws are detected. For example, the issue of Samsung Galaxy Note 7 phones that had a high propensity of batteries failing, leading to personal and property damage. Although, Samsung officially stopped Galaxy Note 7 sales globally and urged owners to power down their phones, the banning of said phone first came from a developed nation (USA); even the airlines that banned it, were from the developed world. Does that mean that a Samsung Galaxy Note 7 was not sold in the developing nations? Or that phone owners from developing nations don't travel by air? They do! Kudos to the developed nations that they act together, regulate, and notify their citizens promptly and regularly.

Upgrade of IoT goods and services

The upgradeability of goods and services is very important for the smooth running of IoT; for the manufacturers, service providers, and of course the users. It is clear that millions of IoT users are not IT experts, and there is a tendency for them to choose or purchase as many devices as they can afford, without considering any safety, security and privacy policies. How do IoT users know when new security updates are available in order for them to update to the latest version? Are they allowed to carry out the updates themselves or are the updates set to automatic? What are the assurances that the user will even update the devices? How do they know if the updates are genuine and not a malware from cybercriminals?

Updates are very achievable if the products in their original design were intended to be updated, otherwise, the reverse is the case. Therefore, whenever an update is available, there should be a secure channel of communication between the manufacturers, the service providers and the end users in order to prevent them from installing malicious updates from cybercriminals - allowing their personal information to be accessed by these criminals.

Managing complexity

Imagine over 50 billion devices and sensors communicating with one another in segmented networks, connected to the Internet in order to execute designated tasks. This is a very large system, which is more complex to manage if things are not well designed and implemented. Of course, the systems offer convenience to the users on the one hand, but on the other, the devices have access and connect to the user's personal information, whether they are home or away.

According to Eduard Kovacs, as far as web interfaces are concerned, six out of the ten products listed below are plagued by persistent cross-site scripting (XSS) vulnerabilities, easy-to-guess default credentials, and poor session management. Through flaws in the cloud and mobile apps, 70% of devices can be exploited to determine valid user accounts through the password reset feature or account enumeration. Again, following HP's report, "Internet of Things Security: State of the Union", a total of 250 security holes have been found in the tested IoT devices - on average, 25 per device. The issues are related to privacy, insufficient authorization, lack of transport encryption, inadequate software protection, and insecure web interfaces. The 10 most common IoT devices include TVs, power outlets, webcams, smart hubs, home thermostats, sprinkler controllers, home alarms, scales, garage door openers and door locks.

Should Governments have a say in the design of the IoT?

Governments of the developing world, just as the developed world, have a significant role to play in ensuring that IoT products and services are compliant with their national policies and international standards. This can be achieved through the setting up of committees in line with the usage of devices, since IoT will cut across all facets of life. For example, medical and IT experts should be in charge of regulating medical-related IoT goods and services. The same goes for automotive, smart home etc. The major reason is that if governments do not have a say or clear idea of what IoT products and services are being purchased, in terms of safety, security, privacy, and interoperability, it could be disastrous along the way for both the governments and the individual home users and it may be to too late or very difficult to correct the anomalies, especially in the case of losing human lives.

Espionage

In my own opinion, if governments of the developed and developing nations do not have a say on the designs and specifications of the IoT or have a clear idea of what products are coming into their countries, it may lead to cyber espionage. It means that other countries, certain groups and individuals, for selfish, personal, military, political, economic interests etc. may produce devices that are more susceptible to attacks and use them as back-doors to gain accesses to classified, personal or very sensitive information without formal permission. As it is the government's responsibility to protect the life and property of its citizens, it follows that the government should protect the personal information of its citizens, by knowing how the citizen's data are being managed, and who manages them, in order not to be traded or abused.

Recommendations

Considering the above IoT challenges, such as security, safety, privacy, data management, interoperability etc. governments alone will not be able to tackle the envisaged challenges, hence the following recommendations.

- Governments of the developing world should develop their own IoT framework or adopt one from the developed world if they do not have the necessary resources. Just as Australia did when it embraced the British Hypercat framework, developed initially for IoT deployments in smart cities, in part to address perceived security issues. A framework that would be interoperable with their environments, social, economic, existing or intended technologies.
- There is a need for the governments of the developing world to participate more in groups (e.g. regulatory bodies, professionals, academia, and civil societies) to help review IoT products and services for the benefit of all. In the developed world, there are good examples of such groups which include; the US Federal Communications Commission Technological Advisory Council (FCC TAC) Internet of Things Working Group, European Commission, Expert Group on the Internet of Things (IoT-EG).
- As the IoT is here to stay, there should be some routine meetings with academia, researchers, IoT vendors, service providers etc. in order to get feedback from different areas in which IoT is deployed and to plan for the future.

"If governments of the developed and developing nations do not have a say on the designs and speci cations of the IoT or have a clear idea of what products are coming into their countries, it may lead to cyber espionage."

Conclusion

The advantages of IoT for developing nations are enormous when smoothly adopted and deployed, as it will positively affect lives in areas such as drought/environmental monitoring, agriculture, health care, home/office automation, transportation, education, research etc. With users and machines exchanging data easily over the Internet, IoT has the capability of boosting the economy positively by saving money and time.☒

Due to layout restrictions, the sources and references of this text are not listed here. Contact the editor if you want the full version, including source references.

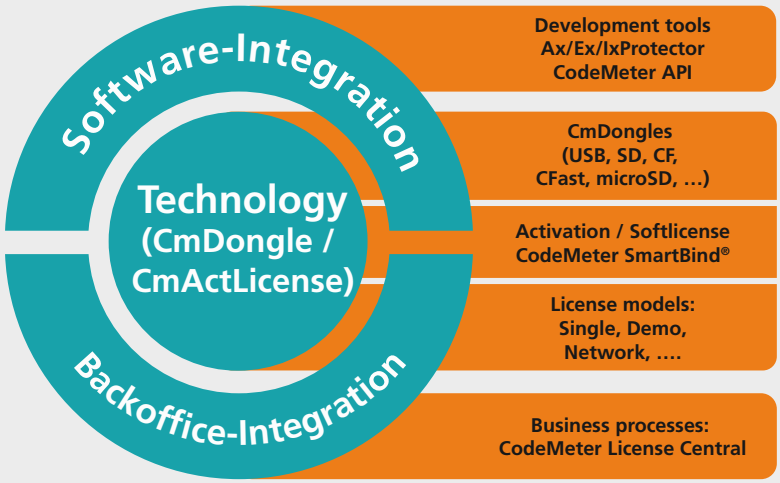
CodeMeter
Securing the Industrial Internet

WIBU SYSTEMS

- Industrie 4.0
- Smart Factories
- Embedded World

CodeMeter Security – Watch the full Video – www.wibu.com/cms

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.

5. Deutscher IT-Sicherheitspreis 2014

SECURITY
LICENSING
PERFECTION IN PROTECTION

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

DATA CAPTURE *when* you want and *where YOU WANT IT*

By Chimezie Emewulu, Seamfix

The need to collect and store customer information may differ from industry to industry but at the core, a platform must be able to meet the customer's requirements and add value to their business or help achieve their objectives. In both the public and in the private sector data capture, data storage and data access are crucial.

☐ KYC Innovation

In order to be able to react to the strong demand in the market, Seamfix has developed BioRegistraTM , a proprietary, innovative and state of the art KYC AS A SERVICE online platform. The platform enables the customer to capture and store any form of information (textual, pictorial and fingerprint). The platform is developed for various sectors and industries across the globe, with the aim of ensuring that the customer can capture data, store this data, and have access to the data in order to validate, verify, export and even update the captured data sets.

Enrolment Use Case

This use case is strictly used for enrolment of fresh records into the BioRegistra system. The information captured during enrolment is based on the configuration (textual, fingerprint, and picture) done during project setup.

Re-Enrolment Use Case

This use case enables a re-enrolment/update of the already registered record: the previously captured data is retrieved using the unique ID and the agent/user can then update the record. To record the updated data, there are different modes of validation;

Fingerprint validation – this applies to strictly captures that have fingerprints. A match of the new fingerprint is done against the previously captured fingerprint. Once the match is successful, the record is retrieved to the client and user can proceed with the update.

OTP validation – an OTP is sent to the mobile number tied to the previously captured data. Once the valid OTP is submitted into the client and there is a match, the captured information can then be successfully updated.

No validation – this mode implies that there is no need for validation before updating captured data, the data is retrieved to the client directly and a user can proceed with the update.

Verification Use Case

Biometric Verification – a one-to-one (1:1) fingerprint matching between the previously captured fingerprint and the newly supplied fingerprint. The system handles this process and returns an output to the end user – match found or match not found.

Textual Data Verification - two sets of textual information are supplied, the primary identifier and any other parameter. The system does a check to confirm whether the values passed exist as a pair (together) on the system.

Identification Use Case

This use case is a one-to-many (1: N) match, where the system does a match of the fingerprint provided against all records enrolled within the customer's project. This BioRegistra system has an extremely high processing capacity, which enables the very high speed core computing. ☒

The officer's best friend.

Thanks to the KINEGRAM®, the authenticity of banknotes and government documents can be checked by the naked eye.

For banknotes: LEONHARD KURZ Stiftung & Co. KG
Schwabacher Straße 482 | D-90763 Fuerth | www.kurz.de | sales@kurz.de

For government documents: OVD Kinegram AG | Member of the KURZ Group
Zaehlerweg 12 | CH-6301 Zug | Switzerland | www.kinegram.com | mail@kinegram.com

KINEGRAM®

SILICON TRUST DIRECTORY 2017

THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

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

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

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

EXECUTIVE COUNCIL

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

INFINEON TECHNOLOGIES

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

ADVISORY BOARD

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

BSI

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

FRAUNHOFER AISEC

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

cryptovision

July 11th – 12th 2017
Wissenschaftspark
Gelsenkirchen

Mindshare 2017

presented by VERIDOS Identity Solutions by Giesecke+Devrient and Bundesdruckerei

- meet experts
- enjoy keynotes
- share knowledge

Free admission, register now!
www.cryptovision.com/mindshare

#cvmindshare @cryptovision

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 lifetime 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

Austria Card 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.

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, prelaminates, 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 protect- ed. 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.identive-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 microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.de

MELZER

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 protect government documents and banknotes. More than 100 countries have placed their trust in the KINEGRAM® security device to protect their high security documents. OVD Kinegram is a Swiss company and a member of the German Kurz group. The company has accumulated over three decades of experience in the protec- tion against counterfeiting and maintains close contacts with police forces, customs authorities and internationally reputed security specialists. OVD Kinegram offers a full range of services: consulting, design, engineering, in-house production, application machines and support as well as after-sales service.

www.kinegram.com

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

PrimeKey

How about a full blown PKI **in a turn-key solution?**

PrimeKey PKI Appliance delivers a turn-key approach to deploy an enterprise PKI (Public Key Infrastructure), without the hassles of complex installation and integration procedures. You get the complete feature set needed to operate a full blown, highly available PKI.

By combining the EJBCA Enterprise PKI software with high performance hardware and a FIPS certified HSM, PrimeKey PKI Appliance provides you with enterprise level security and easy administration.

Want to know more?
sales@primekey.com
www.primekey.com

Upcoming Event!
PrimeKey Tech Days

During previous years, tickets to PrimeKey Tech Days have sold out quickly and over 90 % of the attendees have said that they want to attend the event again. A high quality hard core tech event in PKI is rare to find and we are proud to once again invite you to what is probably the best one: PrimeKey Tech Days.

We have had many exciting speakers during the years and the 2017 edition is no different. Once again, we are honoured to have researchers and leading experts present at PrimeKey Tech Days.

Date: 25 – 26 of September
Place: Stockholm, Sweden
Ticket fee: 380 Euro + VAT.

www.primekey.com/tech-days

PRECISE BIOMETRICS

Precise Biometrics is an innovative company offering technology and expertise for easy, secure, and accurate authentication using smart cards and fingerprint recognition. Founded in 1997, Precise Biometrics today has solutions used by U.S. government agencies, national ID card programs, global enterprises, and other organizations requiring multi-factor strong authentication. Precise Biometrics offers the Tactivo™ solution, a smart card and fingerprint reader for mobile devices.

www.precisebiometrics.com

PRIMEKEY

One of the world's leading companies for PKI solutions, PrimeKey Solutions AB has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

www.primekey.com

PWPW

PWPW is a commercial company, entirely owned by the Polish Treasury, with a long tradition and extensive experience in providing security printing solutions. The company offers modern, secure-products and solutions as well as highest quality services which 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.

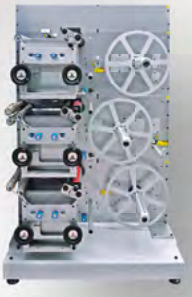
www.teletrust.de

Revolutionary Inline Production Equipment for **MRTD Products**

Punch + Test

- Highest automation level for maximum accuracy, security and yield rates
- Shortest lamination times
- Minimum demand of operators, floor space and energy
- Inline efficiency and flexibility

Lamination



Multiple Unwind

Collation

INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER®

Please visit us at: RFID Journal LIVE! · Phoenix, Arizona, USA | **SDW** · London, UK · Booth L25
Watermark Conference · Yekaterinburg, Russia | **Labelexpo Europe** · Brussels, Belgium · Booth 6C10

www.melzergmbh.com

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

De La Rue is a leading provider of sophisticated products, services and solutions that help keep the world's nations, economies and populations secure.

At De La Rue, we provide governments and commercial organisations with the products and services that enable countries to trade, companies to sell, economies to grow and people to move securely around an ever-more connected world. With a 200 year heritage, we work to the highest ethical standards and stand firm in the fight against counterfeit and fraud.

www.delarue.com

DeLaRue

BECAUSE PEOPLE ALREADY IDENTIFY WITH THEIR PHONES.

As demand grows for more intelligent and secure mobile identification solutions, HID Global is driving innovation through best-in-class technology and convenience. Our HID goID™ platform for government-issued mobile IDs is the most advanced solution of its kind — allowing control over how much personal information is shared — so a citizen's identity is always protected, whether online or off. And because it's powered by secure Seos® technology, you can invest with confidence.

You'll call it customizable convenience. We call it, "your security connected."

YOUR SECURITY. **CONNECTED** | Visit us at hidglobal.com