NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2020 | SPECIAL EDITION

The VAULT

A SILICON TRUST APPLICATION BRIEFING

THE NEXT BIG QUESTION

What could the new 'normal' be for travel, border crossings and payment, post-andemic?

Accelerate your eID project with SECORA™ ID

When time is tight and you need a customized solution …

SECORA™ ID is our new ready-to-go Java Card™ solution optimized for electronic identification (eID) applications. It accelerates your time-to-market through ready-to-use applets supporting rapid project migration. Combined with our free development tool, the SECORA™ ID platform gives you maximum freedom to develop your individual eID or multi-application solutions.

Highlights:

- Ready-to-go solution for fast time-to-market
- Easy and rapid migration of individual projects
- Open platform for highest flexibility
- Best-in-class security controllers and wide choice of packages
- Targeting the highest international security standards for eID applications

Find out more:
www.infineon.com/secora-id

Contents

Imprint

THE VAULT ISSUE 28

Published by Krowne Communications GmbH, Berlin.

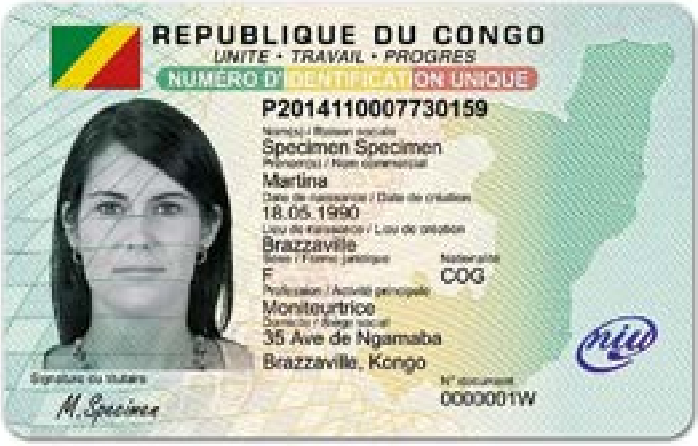
PUBLISHER: Krowne Communications GmbH, Steve Atkins, Kurfürstendamm 194, 10707 Berlin
EDITOR-IN-CHIEF: Steve Atkins
ART DIRECTOR: Lana Petersen
PARTNER DIRECTOR: Yvonne Runge

EDITORIAL CONTRIBUTIONS: Rainer Bergmann, Ursula Schilling, Stephan D. Hofstetter, Guenther Fischer, Lara Schmaus
PHOTOS: INFINEON TECHNOLOGIES, ISTOCKPHOTO, KROWNE COMMUNICATIONS, SCHREINER PRINTRUST, MÜHLBAUER ID SERVICES GMBH
PRINTING: DRUCKEREI HÄUSER KG, COLOGNE
EDITION: November 2020.

World Innovation:

REPUBLIC of the CONGO *Launches* *BIOMETRIC* Tax ID CARD *SOLUTION*

By Lara Schmaus, Mühlbauer ID Services GmbH



REPUBLIQUE DU CONGO
UNITE • TRAVAIL • PROGRES
NUMERO D'IDENTIFICATION UNIQUE
P2014110007730159
Nom(s) / Raison sociale
Specimen Specimen
Prénom(s) / Nom commercial
Martina
Date de naissance / Date de création
18.05.1990
Lieu de naissance / Lieu de création
Brazzaville
Sexe / Forme juridique
F
Nationalité
COG
Profession / Activité principale
Moniteurtrice
Domicile / Siège social
35 Ave de Ngamaba
Brazzaville, Kongo
N° document
0000001W
Signature du titulaire
M. Specimen

□ Following the successful cooperation in the issuance of the Congolese national ID card and the ePassport, the Republic of Congo extended its trust in Mühlbauer. In 2018, the German high-tech company was awarded another prestigious project: the implementation of an unprecedented biometric tax ID issuance system, that reliably supports the registration and identification of all taxpayers, as well as the data life cycle management.

In close cooperation with the Congolese Ministry of Finance and Budget, Mühlbauer developed a modern solution for the issuance of biometric tax identification cards for all Congolese citizens and legal entities. The Information Systems Department (DSI) of the Ministry of Finance and Budget has reliably taken care of the new Tax ID Card system's set-up.

The grand launch of the world's first biometric tax identification system L; The Congolese Director of Identification: Mr. Henri Jacques Kienaka, M: Minister of Finance and Budget: Mr. Calixthe Nganongo, R: Minister of Small and Medium-Sized Enterprises, Handicrafts and the Informal Sector: Mrs. Adélaide Mougany

In ten enrollment offices across the country, private individuals and legal entities can be enrollment for the Tax ID Card via a dedicated, web-based enrolment system. Enrolled applications are forwarded to the Main Data Center, where a Unique Identification Number (NUI) is generated. Within 48 hours – as required by international standards – the applicant receives an electronic document with a NIU (Unique Identification Number) via email or SMS. In two personalization sites in the capital Brazzaville and in Pointe-Noire, the Tax ID Cards are personalized by means of four personalization machines equipped with laser-engraving and highly-secure chip-encoding technologies. As a second step, the personalized Tax ID Card is handed over to the applicant.

During every registration request, the applicant's demographical and biometric data secure the identification process and guarantee the uniqueness of the Tax ID. A sophisticated combination of the software components MB SDM and MB ABIS reliably supports the detection of multiple registration attempts and other inconsistencies. The biometric Tax ID Card ensures the integrity and security of the Congolese national tax system: It offers multiple advantages for administrators and operators in state or private institutions to securely identify and verify taxpayers in the field. By means of a third-party access interface, the biometric Tax ID Card solution enables the secure exchange of data with external entities, such as tax or customs authorities or financial institutions.

The grand launch of the world's first biometric tax identification system took place on August 10, 2020 under the patronage of the Minister of Finance and Budget. The introduction of the Tax ID Card marks another milestone in the Congolese eGovernment initiative: It is a valuable contribution to the modernization of the country's administrative infrastructure and to the securing of state revenues. ☒

WHY do we NEED *biometric* contactless *PAYMENT* cards NOW?

By Ursula Schilling, Infineon Technologies

Biometric payment cards offer stronger, more convenient customer authentication capabilities, while ensuring strict compliance with PSD2 regulations. Regulatory requirements for secure customer authentication are becoming more stringent for specific applications and in specific regions around the world. The introduction of regulations such as PSD2 (Payment Services Directive 2) and GDPR (General Data Protection Regulation) in Europe clearly illustrate this growing trend.

□ In a study published in February 2020, ABI Research predicted that nearly 1 million biometric payment cards will be shipped to the market by the end of 2020. This figure will rise to 65 million by 2024, with key markets developing in Europe and China.[1]

Multi-factor authentication

On-card biometrics enable highly convenient, innovative multi-factor authentication for point of sale (POS) purchases. The card holder ("what you have") can easily validate their identity ("who you are") at the POS by presenting a fingerprint that matches the biometric print on the card. As such, payment cards with integrated biometric sensors are an extremely convenient, innovative means of complying with strong customer authentication (SCA) requirements. In markets that rely on offline PIN mechanisms or chip-and-signature infrastructures, biometric payment cards are a great way to harmonize authentication processes and comply with SCA regulations without costly and complex changes to the POS infrastructure.

Greater choice

In addition to this, some market players want a broader choice of authentication methods tailored to different user groups, such as disabled or older people, early adopters and forward-looking millennials interested in innovative solutions. Some of these user groups still have reservations about card and contactless payments. Biometric payment cards simply offer greater privacy, as the card always stays in the user's hand. The buyer does not have to hand it over to a cashier or push any buttons on a pin pad. As such, this technology fosters consumer trust by reassuring users that their personal data will remain private.

Better, more hygienic user experience

Biometric contactless technology also improves the overall customer experience by making transactions quick and easy to complete, as there is no need for users to touch a pin pad or interact with a cashier. This "no-touch" approach also has a vital role to play in today's global pandemic: it protects users' health and well-being by allowing them to make hygienic, contactless payment transactions without touching potentially contaminated pin pads. This also applies for high-value payments above a certain limit for a cardholder verification method (CVM) stipulated by networks and issuers. Thus, for both low and high value payments, no PIN entry will be required anymore when using a biometric sensor-enabled payment card. Biometric authentication, when implemented in a security controller (SC) on card, fulfills the highest certification standards.

Put simply, biometric payment cards strike the right balance between security, convenience and speed, while increasing efficiency at the POS. At the same time, however, biometric cards are a new concept for many consumers and so card issuers will have to educate their customers on this new payment technology and its usage. Enabling users to easily sign up from home without having to visit a bank branch is one approach that could support the rapid adoption of biometric payment cards.

Advantages of biometric contactless payment cards for different market players in the payment ecosystem

Overall, biometric contactless cards will bring huge benefits to all players in the payment ecosystem. These far outweigh the hurdles and drawbacks connected with this new technology.

a. For network and infrastructure providers

Looking at the existing POS infrastructure, the cost and effort involved in rolling out biometric payment cards will be minor, since infrastructure updates will not typically be required on the POS side. Over 90 percent of POS terminals have already received the requisite firmware updates and so only a small number of POS terminals will still have to download these. Transactions will be based on well-known ISO 14443 standards. The only investments required will be on the part of card manufacturers, who will have to embed biometric sensors and inlays into cards to ensure they can source sufficient power from contactless fields.

[1] *ABI Research, Payment and Banking Card Technologies Report, Feb. 2020, updated May 2020*

> “ *Put simply, biometric payment cards strike the right balance between security, convenience and speed, while increasing efficiency at the POS*

The cost of the new cards will be slightly higher. However, upcoming security controller (SC) innovations from companies such as Infineon Technologies – the market leader in payment ICs – will bring the cost of card production down, as SC external silicon components become obsolete and the card production process, as a whole, becomes less complex.

New state-of-the-art security controller platforms delivered by chip vendors such as Infineon Technologies meet all requirements regarding contactless performance, power efficiency and security.

The majority of contactless security controller (SC) can be implemented into any kind of form factor. Similar SC implementations can be built into contactless cards (a yearly market shipment of >2 bn pieces), contactless tokens for secure second-factor authentication for remote payment (yearly market shipment of 40 m) and smart payment wearables (approximately 80 m pieces per year).

b. For banks and issuers

Card payments based on biometric authentication are expected to increase, while costly cash handling processes are expected to decrease. The current level of Card Present (CP) fraud at POS will drop, as biometric authentication is known to be more secure, making it more difficult for criminals to skim personal information stored on cards.

This technology will boost consumer trust and increase the number of contactless transactions.

Incorporating these technology innovations into cards will act as a draw for consumers and make it more likely that these cards become “top of wallet” for users.

Biometric cards will also reduce costly chargebacks, as users will no longer have to enter a PIN and so the likelihood of making a mistake or fraud, together with skimmed card details will be minimal.

c. For retailers

Higher customer throughput is to be expected as biometric authentication is quicker than entering a PIN for high-value transactions. At the same time, this increased customer throughput may translate into higher revenue for retailers.

Generally, it is perceived that payments at points of sale in shops will become easier and less confusing as there is no CVM (cardholder verification method) limit for biometric card payments. This would mean that consumers will no longer need to enter a PIN, thereby making payment transactions more efficient and streamlined.

Ultimately, retailers can expect to see more customers, more revenue and fewer costly cash handling processes.

Payment networks and issuers can expect an overall reduction in fraud rates for lost and stolen cards as the only person who can make a transaction with a biometric payment card is the individual who matches the biometric data.

d. For consumers

When a consumer pays in person for a high-value transaction, they do not have to insert their card into the payment terminal. All they have to do is hold a card over the terminal. A second factor such as a PIN, signature or biometric authentication is required for payments above any nationally defined spending limits to prevent fraud through the skimming of card details or to ensure the user is not paying with a lost or stolen card. This makes contactless payments more secure for consumers.

Networks and issuers have all recently increased spending limits for low-value payments to increase the number of contactless transactions without CVM. In Germany for example, customers can make contactless payments up to a limit of EUR 50. In the UK, the limit is GBP 45. Similar measures have been taken in a further 27 countries. Already for a high number of contactless transactions a 2nd factor authentication has been waived. This situation is unlikely to change until biometric cards have been rolled out on a wider scale with secure cardholder authentication for all payment transactions.

This new biometric technology can also make remote payment transactions more secure. If a user has to confirm their identity for a remote payment using a second authentication step, all they will need is their card and an NFC-enabled mobile phone – they will not have to use another potentially less secure device for two-factor authentication.

It is expected that consumers will appreciate the convenience of making payment transactions without having to remember a PIN. This should be particularly welcome among the elderly. Overall, it is expected that biometric card payments will become the secure method of choice.

Finally, the high speed of transactions (less than one second for low and high-value payments), together with a seamless user experience and the hygiene factor outlined in the next chapter, are all expected to make biometric contactless cards the number one choice among customers.

More security for consumers and retailers during the COVID-19 pandemic

Faced with continued uncertainty surrounding the COVID-19 pandemic, customers and retailers across the globe are switching to contactless payments over concerns about contact-based transmission of the coronavirus. Standards of security and convenience are rising and biometric contactless cards are expected to increase hygienic security standards even further.

The contactless biometric card system is the only card-based payment method that allows users to make touch-free and virus-free high-value payment transactions at the POS, without having to come into contact with surfaces potentially contaminated with the COVID-19 virus. Presently, for all high-value transactions, users must enter a PIN, which comes with the risk of contracting the potentially deadly COVID-19 virus that may found in germs on the POS touchpad.

Even in cash-driven Germany, more than half of everyday payments are currently being made with contactless cards

> “Faced with continued uncertainty surrounding the COVID-19 pandemic, customers and retailers across the globe are switching to contactless payments over concerns about contact-based transmission of the coronavirus.

today, compared with only 35 percent of payments being made with contactless cards before the coronavirus crisis began (Deutsche Kreditwirtschaft). The situation has changed even more dramatically in the US. According to Visa, the volume of contactless transactions has increased by >2000 percent since the start of the pandemic.

While contactless technology makes payment transactions faster, more hygienic and more convenient, only a combination of contactless payment and biometric solutions is considered robust enough to provide all-round protection against viruses and diseases. The way we pay has already changed radically and will continue do so, even more with biometric contactless cards around the corner.

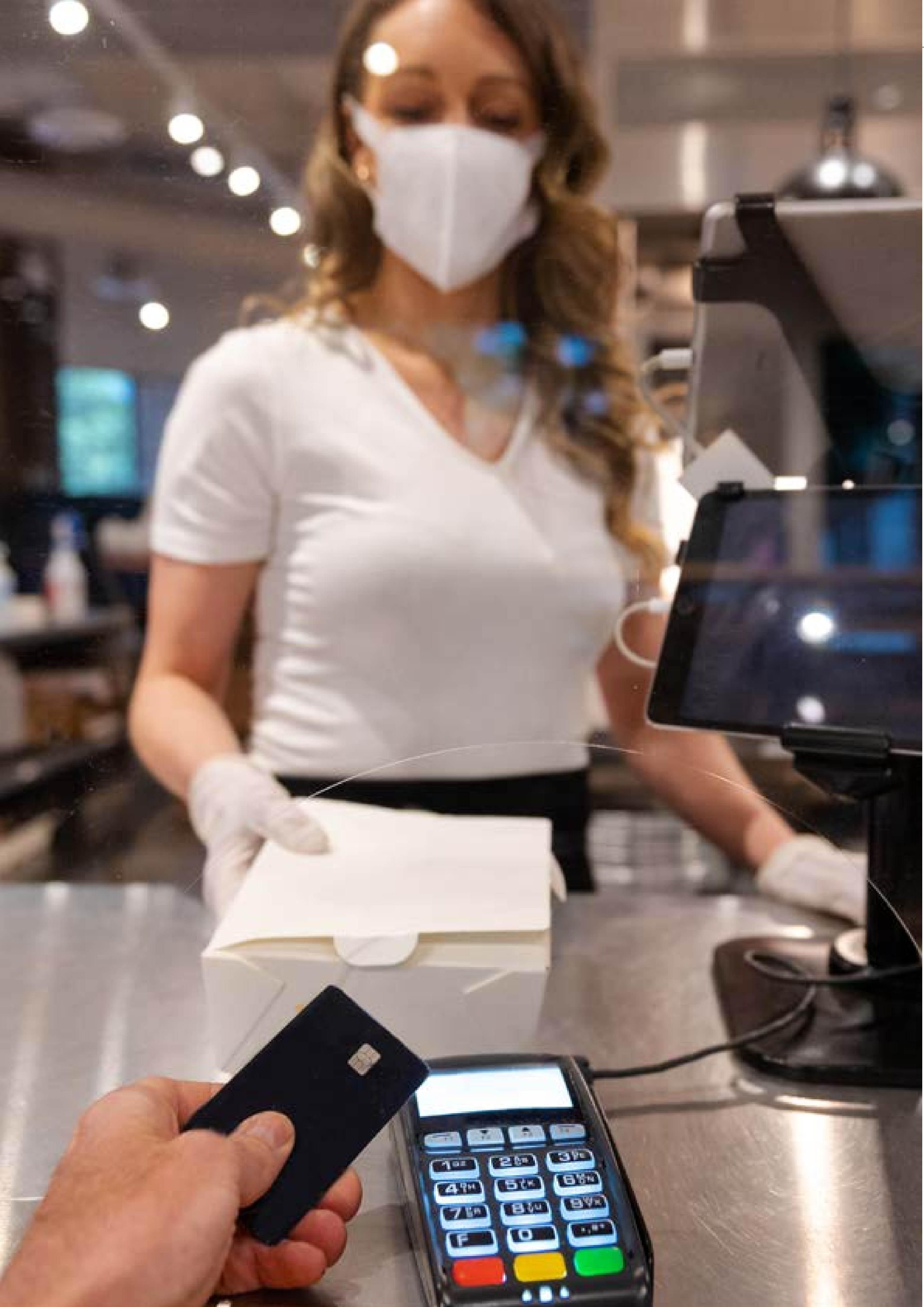
What can Security Controller providers contribute to the payment and biometric card market?

Infineon is the global market leader in the area of payment security chips. Worldwide, every second chip in a payment card is an Infineon chip inside. The company is also playing a key role in the development of biometric payment cards and has supplied chip solutions for all major pilot schemes and biometric card projects in the first half of 2020.

Infineon’s sophisticated security controller (SC) for contactless payment cards offer a range of benefits, including extremely low power consumption and a unique feature set that enables manufacturers to easily and flexibly integrate elements into card bodies with minimum effort.

Leveraging its experience in security and contactless design, Infineon is committed to supporting the widespread adoption of biometric payment cards by integrating additional functions into security controller that enable manufacturers to efficiently produce scalable biometric systems for cards.

Infineon’s contactless payment chips have an optimized power profile for non-battery-supported contactless systems and deliver outstanding contactless transaction performance, enabling contactless payment transaction times of below 200 milliseconds, even in scenarios with low reader field strengths and when used in combination with small antenna designs. These factors are a decisive benefit for biometric card solutions with seamless card implementation further enhanced by various industry partnerships


1
2
3
4
5
6
7
8
9
F
0

Partnering for biometrics

In order to seamlessly manage the different cards components, Infineon cooperates with various partners in the field of biometrics:

Infineon partners with biometric company Zwipe to deploy Infineon's chip solutions in pilot projects featuring Zwipe's biometric payment platform. In other words, Infineon is supporting multiple leading payment networks run by twelve major banks in various countries across Europe and the Middle East.

Infineon has teamed up with Fingerprints Card (FPC) and IDEX Biometrics to provide secure, cost-efficient platform solutions that will enable the mass deployment of biometric cards from 2022 onwards.

This is how Bjoern Scharfen (Head of the product line Payment & Ticketing Solutions at Infineon) perceives Infineon's engagement into contactless biometric cards, "Infineon is committed to enabling a secure, convenient payment experience enhanced by fingerprint authentication. Our turnkey solutions will drive biometric innovations in the smart card industry and help make digital transactions easier and safer. Biometrics are the next innovation step for contactless payment cards, providing additional security and convenience to banks and consumers, while protecting customers and merchants from infectious viruses."

Market data and pilot projects

Currently more than 20 world-wide pilots and biometric card volume projects have already been launched by different issuers supported by different networks and key players backed by interesting market information issued by various channels:

- Mastercard is working with Crédit Agricole Payment Services on a biometric card pilot for 200 customers in Touraine and Poitou. The pilot will trial payment cards with integrated fingerprint sensors.

- Mastercard has certified its first contactless biometric payment card from Thales based on the SLE78 family, enabling the company to move from the pilot phase to commercial deployment.

- Biometric technology company Zwipe has entered into a partnership with global smart card manufacturer XH Smart. The partners are focusing on commercializing end-to-end biometric payment offerings for XH Smart customers in China and beyond.

- Biometric technology company Zwipe has entered a milestone partnership with China's largest secure payment solution provider Goldpac to launch biometric payment cards. The two partners are working together to launch biometric payment cards, enrolment offerings and related services to Goldpac's extensive customer network, which includes some of the largest financial organizations in the world.

- IDEX Biometrics has been granted a patent by the UK Intellectual Property Office for unconnected on-card enrollment on biometric smart cards. IDEX biometrics has extended its on-card enrollment patent to the United States and Germany and is looking to extend its influence and reach across further key regions.

- Swiss Corner Bank has launched Switzerland's first commercial biometric credit card through a partnership between Fingerprint Cards (FPC), Thales and Visa. According to an announcement from FPC, this is the first limited commercial launch of its kind.

- Fingerprint Cards (FPC) has announced that its sensor module has passed accuracy and security testing with BCTC and is targeted at the Chinese market. https://www.fingerprints.com/2020/04/15/contactless-comes-of-age-how-biometrics-is-taking-cards-to-the-next-level ☒

Facilitating RESPONSIBLE *travel* in TIMES of *PANDEMICS*

By Stephan D. Hofstetter, Managing Partner SECOIA Executive Consultants Ltd

Both domestic and international travels have been heavily limited in the fight to combat the spread of COVID-19 and break the curve. What follows is a highly edited article based on a 5-part series that looks into the question of how to facilitate future travel in the mid to long term while the world deals with the effects of COVID-19. Details on how to read the complete article series can be found at the end of this article*.

□General assumptions and boundaries, reflections on risk management and commercial impacts

For this article, we will be focussing on mid-term international travel. We still lack broad understanding of how the virus can be fought or cured, and indicators about immunity are mixed, with some reports debating it remaining for longer than 12 months. With this in mind, we will make some assumptions:

Hypotheses

- The first hypothesis is that a continued, general lockdown of borders on international and intercontinental travel is not an economically viable solution for the mid- and long-term.

- The second hypothesis is that processes all along the travel continuum need to be facilitated. The slowed down processes, and the enormous space requirements for pre- and off-boarding is a serious burden for the airport and airline operators, let alone for the passengers.

- The third hypothesis for this article is that generally placing all or the majority of persons under quarantine for 10 or 14 days is not viable, neither for tourists nor for business.

Risk-Management

Accepting the need for facilitated, reasonable international travel, the next question should not be focused on the tools, but on the acceptable risks. The discussion will not only be focused on the epidemiological aspects, but has the potential of being discriminating for various reasons. The outcome of ethical and legal discussions of these questions will highly depend on the society reviewing them. Among the many parameters, a couple of exemplary questions will lead the discussion:

- Should a person with elevated COVID-exposure risk be permitted to travel? And if so, should he be subject to a different process than the average persons? This question has an impact on persons living in countries, or having visited countries, with high infection numbers. Many countries have locked their borders to specific countries, or have imposed quarantine procedures for persons travelling from countries of elevated risks.

- A special and highly intrusive aspect is this one: Is voluntary behavioural exposure risk to be treated differently from ‘normal’ behaviour? This concerns people not aware of, or voluntarily ignoring the impact of COVID-19 on a persons health and global economy. It could specifically affect a younger population who is attracted to a lively nightlife or major sporting events.

- Which risks is the destination country willing to accept as the price for ramping up the local economy with leisure and/or business travel? A very liberal practice is bound to have a negative impact on the infection rates. A too strict practice would not meet above assumptions. In absence of sufficient evidence-based data and procedures, a restrictive approach is bound to lead to closed borders.

- Who is to set the benchmark on the risk parameters? While a certain diligence can be expected by the countries of origin, it is more likely to be for one of the air carrier operators who would be concerned upon emigration. However, and in any case, the authorities at the destination will consider themselves most concerned. As a consequence, the traveller will have arrived already at the border and must now be handled on their own territory. This is a burden for the authorities of the destination country, but equally for the traveller. For the latter the predictability of immigration is lost. Unless, a pre-departure process can be established.

- Which sources of data will be trusted by the competent risk assessment authority? This question becomes an integral part of the above evaluation for pre-departure processes. On which sources of data will the destination country be willing to ground their "clearance-to-travel" processes?

The economic, risk management and commercial liability aspects cannot be separated. The only way to solve this in the medium term, in our view, is to achieve a multilaterally agreed procedure and risk management approach, combined with transparent and verifiable communication, leaving a margin for internationally varying privacy legislation.

Tools and processes

International travel for both business and private in times of a pandemic must be made easier in the medium term. The challenges lie in risk management and in finding appropriate policies, standard operating procedures and tools to facilitate and enforce responsible travel. Therefore, it is necessary to look at the system of instruments and processes to be considered.

Risk factors and sources of data

To determine the risk parameters of individuals based on current knowledge about the spread of the virus, we can consider five data clusters. The first four are preventive, the last is reactive:

- Demographic data
- Exposure behaviour
- Self-protective behaviour
- Health
- Track and Isolate

Demographic data considers where the centre of your life is located (country or region of residence), your age, gender, occupation, ethnicity, and perhaps some other elements that we will discuss below. Based on developing statistical evidence[1], there may be relevant indicators that can be extracted from these data. Some of this data can be collected from the Advanced Passenger Information Records (API)[2] for air travel, an advanced e-Visa application and travel registration forms. Many of these factors can be checked for evidence based on existing processes and tools already established in the travel ecosystem. Also, most of the factors will not change on a regular basis, which provides long-term stability and a source of cross-reference. The challenge is rather that science must be able to create meaningful and fair profiles and limit both false negative and false positive outcomes.

The factors based on **exposure behaviour** are more profound when it comes to determining the probability of being exposed to the virus:

- Does the person avoid gatherings of people (e.g. nightlife) and/or does he/she restrict his/her geographical area of movement etc.?
- And, what is the exposure of people living in the same household? This could be an important factor in the assessment: For example, while the person himself might be very careful and even live in quarantine, his family members might be at increased risk working as healthcare professionals.

The generation of this data is a challenge within the limits of data protection regulations. It is also a challenge within the system, as the country of destination must rely on foreign information and tools and comply with the various local laws. For exposure measurement, authorities could consider using the different national COVID tracking apps. However, extensions are needed to provide a meaningful interface and data set for such an evaluation. The national tracking apps must integrate a universal interface that respects privacy and provides international authorities with a clear understanding of:

1. How long has the app been in continuous operation (app running, Bluetooth active)
2. Link the app to a person (i.e. passport/ID number; photo; name)
3. Evidence that the app has actually been with the person (e.g. use of accelerometers, screen time or activity monitoring).
4. Unified output interface of exposure risk

Some governments decided to use GPS data or QR Code based check-in processes at various locations of interest, such as shops. Other countries, including most European countries, use the Google/Apple Tracking interface, excluding the use of GPS. For this reason, a universal model based on the movement of the individual is not realistic. It could be possible to use anonymised mobility data[3]: Either by use of GPS-data, or mobile phones connect their users to telecommunications and Internet networks via cell phone towers.

The current **health assessment** can be structured in four layers:

- The first is the self-declaration of symptoms. Some countries ask general questions about the well-being of passengers. Others ask specific questions about symptoms, such as fever, respiratory issues, impaired taste and smell sensation, body aches, etc. If the forms are submitted online, the answers cannot be validated by the authorities as they may change within an hour. Therefore, a risk assessment that exonerates the person has less value than one that comes to a negative conclusion based on the data provided.

[1] Factors associated with COVID-19-related death using OpenSAFELY https://www.nature.com/articles/s41586-020-2521-4

[2] Advanced Passenger Information Records (API) https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx

[3] Apple makes mobility data available to aid COVID-19 efforts https://www.apple.com/uk/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts/

> *International travel for both business and private in times of a pandemic must be made easier in the medium term. The challenges lie in risk management and in finding appropriate policies, standard operating procedures and tools to facilitate and enforce responsible travel.*

- The second element is the request for a current COVID-19 PCR test report. The time frame ranges from 48 hours before travel (Equatorial Guinea) to 10 days (Bahamas), with a 72-hour limit in most countries. Several countries, including China, will perform a COVID 19 PCR test upon arrival. This approach serves the national need for protection. However, it does not give travellers sufficient certainty that they can reach the objective of their travels.

- The third is to examine people at the airport and place them in waiting rooms or quarantine until the results are available for further processing.

- The fourth is the popular but controversial temperature scanning, which is carried out as border screening. With detection rates below 50% and many false positive results, the opportunity costs are considerable.

Finally, the reactive measures of **track and isolate**. On arrival in a country, the centre of focus shifts. The emphasis shifts to the tracking of persons who themselves represent a risk or have been exposed to risks. IATA and the airlines make use of the well-known instruments of the **Passenger Locator Forms** (PLF)[4]. The aim of these forms is to determine the risk exposure during the stay in the aircraft - based on the seat number - and to be able to contact the persons in case of need after arrival at the destination. Since the forms are filled out on paper in the aircraft, the contact details cannot be verified. A detour via the **Passenger Name Records** (PNR)[5]and above-mentioned API data could eliminate some of the sources of error.

Selected countries require the use of their local tracking apps, which goes beyond the mere registration of contacts. They provide a communication channel or even localization.

Further considerations on the use of tools

On one hand, approaching the subject from an industrialized and IT-affine world doesn't go far enough and is even discriminating. On the other hand, the wealth of the privileged society bears additional risks to be considered, when making use of tracking devices and apps:

- *One person - One device:* Many people own several devices, suitable for running the governmental tracking apps. As such there is a threat for cheating the sensors, especially for people able to travel by air.

- *One device - one person:* In vast regions the availability of suitable devices is not given on a personal basis, but perhaps per family or clan. Enforcing technical tracking and sensors on a personal basis causes risk of exclusion for economic, gender or cultural discrimination.

[4] *Passenger Locator Forms (PLF) https://www.iata.org/en/programs/safety/health/locator-form/*

[5] *Passenger Name Records (PNR) https://www.iata.org/en/publications/api-pnr-toolkit/*

- "A device is not necessarily a *suitable* device". This again can pause a risk of exclusion of poorer or elderly, less technology affine societies.

- Network coverage is not complete, and not necessarily affordable. Primarily, this does not impact the tracking devices. However, it does have consequences for filling in online-forms or receiving travel certificates.

- Output devices / printers are not generally available: As above for network coverage, devices and printers are not always available, or suitable to print usable certificates with QR-codes.

Science, legal framework, technical feasibility and coordinated agreements are important factors. However, orchestrating them effectively is a major challenge in view of the many unknowns. A look at reference projects and the resulting findings is a resource that needs to be investigated.

Case-Studies

In this section we will take a practical approach and look at some specific national implementations. What is being done and what are the lessons to be learned, from the positive and from the weaknesses.

We will discuss three basic scenarios: The restrictive suspension or severely restricted freedom to travel, the liberal freedom to travel within so called "travel bubbles" and the managed screening programmes before boarding. The focus will be on the latter.

Restricted or no travel (Lock-down)

The list of countries with absolute travel bans for foreigners is long and ranges from Japan to most African countries. More often, countries have closed their borders to certain countries with poor pandemic indicators or established a small exception window for entry, supplemented by 14-day quarantines.

Travel within bubbles

Travel bubbles, also known as travel corridors and corona corridors, are essentially an exclusive partnership between neighbouring or nearby countries that have had considerable success in containing and combating the COVID-19 pandemic within their respective borders. These countries then restore the links between them by opening the borders and allowing people to move freely within the zone without having to undergo quarantine upon arrival. A caveat; the following examples were in place at the time this article was written (September 2020) but it may be necessary to check if these examples are still in place post-publishing (November 2020) to establish the level of current ‘travel bubbles’.

The spread of the concept was promoted by the three Baltic States, namely Estonia, Latvia and Lithuania, when they established a trilateral partnership which allowed citizens of these countries to enter the territories of the Member States. This free passage was eventually to be called the 'travel bubble'.

- There are several travel bubbles in Europe. Two examples are the travel bubbles between Austria, Germany, Switzerland, Liechtenstein and neighbouring eastern European countries. A second bubble exists between the two Scandinavian countries of Denmark and Norway. Sweden was excluded because of the still very negative development of its COVID case numbers.

- In the Asia-Pacific region there are many bubbles that already exist or are developing. Intensive talks are currently taking place between Australia and New Zealand on the creation of a Trans-Tasman travel bubble. Another example is between China and South Korea, which have implemented a corona bridge since May 2020. This bubble connects only selected cities, including the economic centres of Seoul and Shanghai. It could be extended to the special administrative zones of Taiwan, Hong Kong and Macau.

- Intensive talks are taking place on the American continent. Colombia is seeking agreements with its neighbours. However, the freedom of travel between the USA and Canada has experienced some restrictions that only allow authorized persons to travel.

- No travel bubble arrangements have been made in Africa.

Setting up safe travel corridors are a welcome manner to facilitate commerce and freedom to travel. However, they are complex to be managed by the various stakeholders including the airline operators. They are subject to rapid changes as the case-numbers develop. And they are not suitable to contain the pandemic.

> “ *Knowledge of best practice is still limited. However, the various schemes provide an invaluable source of inspiration for assessing more effective ways to facilitate responsible international travel.*

Screening prior to boarding

This solution concept is based on the Passenger Location Form (PLF), the Health Declaration Form (HDF) and the Advanced Passenger Information (API) concept, which aims at a prepared risk assessment before the passenger arrives at the border.

These implementations have the advantage that they can be implemented quickly. However, the actual value is not clear due to the non-transparent algorithms. They also lack actual validation of the data: No validation of contact data (challenge-response from email / phone), to link to API data (i.e. non-existing flights, wrong dates and ports of entry could be entered), deadlines for providing the information were sometimes not enforced, and the health screening questions might serve liability requirements, but not actual management of the pandemics.

Assessment of pre-boarding screening

The biggest weaknesses of the current implementations of the pre-boarding screenings are:

- The initiatives are not harmonized, lacking guidance and common policy rules. The international organizations such as CAPSCA, ICAO or IATA are yet to provide guidance on best practice.

- The captured data is not standardized and not validated, making it difficult or even not practical to actually run machine-based assessment for an actual pre-travel screening.

- Digital contact data is mostly unvalidated, although it would be a simple step to be improved: Challenge-response eMails or SMS-Validation of mobile phone numbers are standard services.

- Being able to make use of existing risk assessment procedures would be of great value, preventing isolated patchworking. Many countries have existing API/PNR-review mechanisms, allowing sometimes even recent travel pattern validation. In order to make this work, there is a need of acquiring the according keys: Passport Number is one of them, linking the application to a travel document. The other would be the request of booking reference, allowing to populate or validate Flight information, place of embarking, place of arrival, time, and perhaps even hinting on the days of remaining in the country.

- The questions related to the COVID-risk exposure are in many cases very generic, and appear rather random. While most of the above referenced countries do ask about individual symptoms, they often fail to ask for all of the currently known major indicators, such as loss of taste. Also, they might ask about having tested COVID-19 anytime in the past.

Knowledge of best practice is still limited. However, the various schemes provide an invaluable source of inspiration for assessing more effective ways to facilitate responsible international international travel[6]. Many measures appear to have been implemented in a short time and with few resources. Finally, some of the implementations, such as in Jamaica, are ground-breaking in terms of what could be done, although it would not be possible for several countries for data protection reasons.

[6] *A comparison table can be found by using the link; https://thevault.secoia.ltd*

The travel industry in change

We are still at a stage with many assumptions, little stable knowledge and understanding of interdependencies. The global system of travel and its impact on the local society is very complex. Companies and with them the lives of individuals depend on finding a solution. However, the emphasis is on "returning to what we had before".

The VUCA approach

The leadership theories of Warren Bennis and Burt Nanus, summarized under the acronym VUCA, can be helpful. VUCA stands for "volatility - uncertainty - complexity - ambiguity". This summarizes the fragile status we are in. The solution-oriented, agile approach applies VUCA with new meanings: "vision - understanding - clarity - agility".

Volatility can be countered with vision. What is "the new normality"? The authors would describe it as "managed risk", where absolute security is biologically, financially and ethically unattainable or desirable. It could be a situation in which at least the travelling population is no more infectious or contaminated than in the destination country. This threshold seems to be in line with the travellers' willingness to take risks. Much attention is being paid to various contactless service points in airports, such as biometric border control or boarding. Given the sheer endless number of contact points throughout the journey, we doubt that the introduction of contactless checkpoints is part of the strategy to contain the pandemic, and will not have a really serious impact on overall air safety. However, it is rightfully part of the oneID strategy[7], contributing to user-friendliness. Also, it addresses expressed needs of airport and aircraft operating staff for their safety and it carves out any pretext and concerns of passengers that might refuse to interact with contact-based operations.

From the vision comes the opportunity to transform uncertainty into understanding by bringing all stakeholders to a common mindset and understanding of how they can contribute to success, along with key working principles that promote active communication and widespread participation practices. Never before have public authorities, industries and interested groups been so willing to listen, develop understanding and even actively contribute to a broad audience as they are today. Despite the challenges associated with network connectivity and technology in general, this could be even more inclusive as costs and travel restrictions are no longer a considerable issue.

Complexity can be countered by clarity, which is the result of constantly reinforcing real priorities. The change brought about by the current pandemic brings enormous complexity - therefore, the organisations and industries involved must be careful not to create and maintain internal complexity and must share a common commitment to simplicity. A great opportunity to reduce complexity and increase clarity lies in data integrity and a shared view of its reliability and impact.

As the last part of the acronym, ambiguity can be met with agility. The term agility has found its renaissance in IT project management as a response to a strict waterfall approach. It is based on a clear mission, clear boundaries and role models, without going into the details at an early stage. This leaves room for growing insights and lessons.

Unified approach

On April 8, 2020 IATA / APCS conducted a virtual Think Tank meeting focused on two main topics: a) How can passenger confidence be restored and b) What new standards, best practices or processes will have to be considered post crisis? From the report can be taken, that emphasis was on information / situation awareness. The rapid changes on a national level, sometimes even airport / border crossing level on one hand, and evolving knowledge on the virus itself on the other hand, make this kind of intelligence key for implementing effective processes. Within this situation of a highly fragmented regulatory landscape, Joseph Suidan, Head Ground Operations IATA mentioned during an IATA Webinar 15.07.2020 a noteworthy assessment: "It is not the time for customized processes. The passengers want a simple and harmonized process."

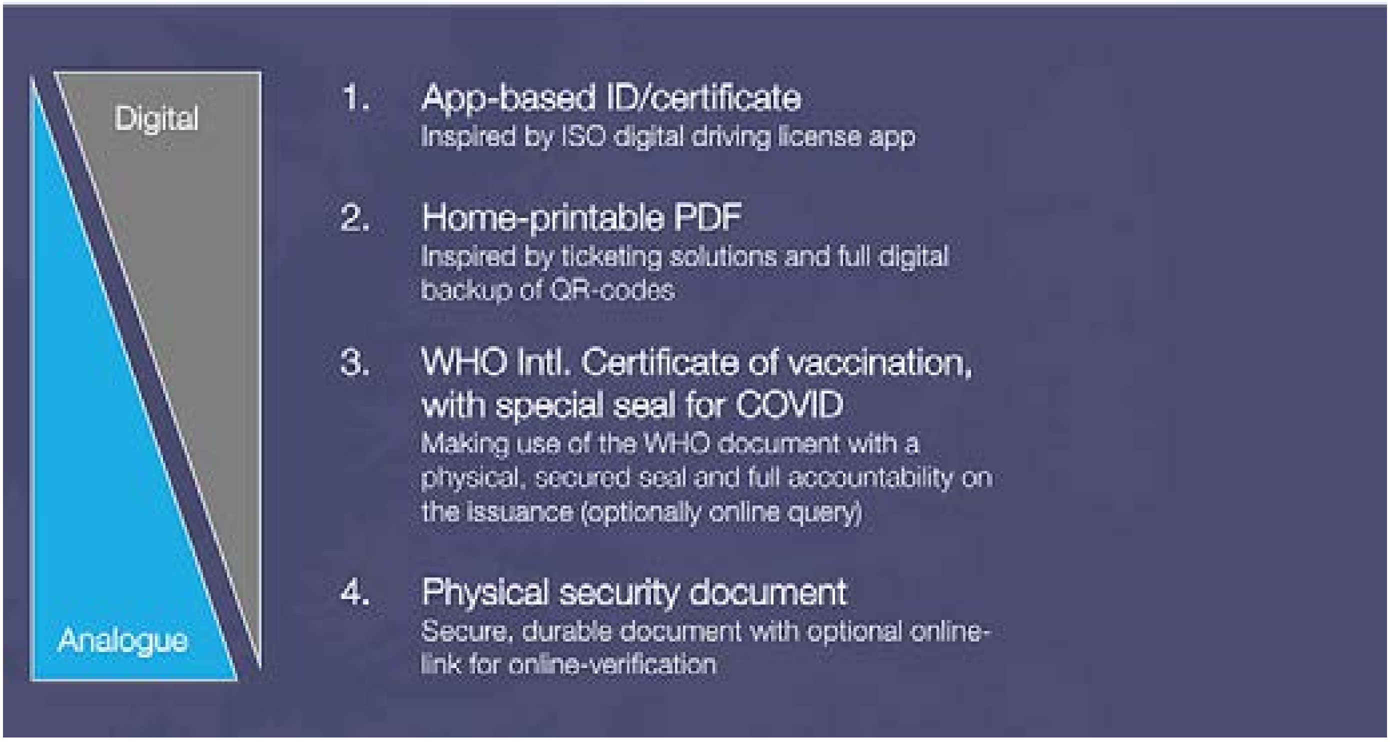
And it is safe to say: It is not only the passengers seeking clarity and simplicity. The airline operators are facing immense challenges with nearly daily changing rules applicable between any two countries.

In view of health-related credentials for travelling, the above mentioned Think-tank produced these ideas (selective listing):

- Health Certificate: safe to fly status (like ready for carriage on cargo) / health certificate / Electronic System for Travel Authorization (ESTA) equivalent via web portal

- Technology for Health Certificates: Use of general ledger (Blockchain) for Health certificate to enable flying.

[7] *the oneID strategy https://www.iata.org/en/programs/passenger/one-id/*



1. **App-based ID/certificate**
   Inspired by ISO digital driving license app
2. **Home-printable PDF**
   Inspired by ticketing solutions and full digital backup of QR-codes
3. **WHO Intl. Certificate of vaccination, with special seal for COVID**
   Making use of the WHO document with a physical, secured seal and full accountability on the issuance (optionally online query)
4. **Physical security document**
   Secure, durable document with optional online-link for online-verification

Each of these categories contains characteristic advantages:

- Legal Implications of Health Certificates: Carriers not responsible to verify health / provide guarantees/ just to verify. Also: Self-declaration versus authority-based health “credentials”

- OneID: some standards exist but are not yet all connected. The key element is that we as airlines have to establish your identity based on your Passport. One ID will bring this closer and so COVID accelerates the OneID principles

Solution components in context

When discussing solution components, three scenarios must be taken into consideration: The first is the regular scenario for a free movement certificate, as required, for example, to be able to move around with restricted local or national freedom of movement. The second develops the first scenario further and facilitates international travel. The emphasis is on supporting a more predictable, internationally regulated travel policy, however short-term such a certificate may be. It is linked to cases where the visa waiver has been suspended and a medical risk profile must now be established before being allowed to travel. Finally, the third scenario combines the first two, applied to the specific requirements of refugee management.

Categories of technical responses

The technical responses to these scenarios are clustered by the authors into four main segments that are evolving from purely digital to purely analogue system designs. The first are purely digital, app-based ID cards or certificates, perhaps comparable to digital ISO driving licence systems. The second includes home electronics that converts digital information into analogue certificates produced at the individual's home. A representative of this category could be flight or train tickets printed at home.

The extension of existing ePassport technology or Logical Data Structure (LDS) with health-related information could also be a representative of this category in the medium term. The third method uses (existing) physical documents and adds digital certificates or links containing the last health status recorded. The yellow WHO International Vaccination Certificate, with a special dated seal for COVID testing or vaccination, could serve as a model. The fourth category is a purely physical security document, which may have a long-life span and is enriched with data encrypted on the document.

App-based ID/certificates are likely to be very flexible, require little perceived logistics, could be combined with other COVID apps and can be designed to respect privacy. Home-printable

MASKTECH

We make chips intelligent

MTCOS®

Independent – High Secure **Chip Operating System**

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

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

SecurITy made in Germany

Common Criteria

PDFs are based on home infrastructure and pragmatic workflows. These are advantages when the average resident has access to such infrastructure and networks, and a practical advantage in other cases. The ePassport infrastructure option would use the existing infrastructure and even increase its use.

Given that most countries still lag behind basic implementations in terms of border control, adding this feature as a fast-deployment solution would require a detailed assessment. The use of the international vaccination certificate uses existing processes, is low cost and scalable, with processes supported by databases. However, in the digital economy, this would be seen by many as a very old-school approach. Finally, the use of dedicated physical security documents can be very versatile in difficult environments and can offer high credibility, even when used offline. It offers flexible form factors such as a card or archive document. Furthermore, the scheme is scalable and is proposed for various humanitarian use cases.

ISO certified digital driving license as a technology model

The concept is to carry a digital COVID-19 ID in a single digital wallet to track pandemic risks and travel authorizations. The implementation is based on an interoperable ISO standard certificate that can be used both online and offline. The data is managed centrally and can be updated at any time when the device is online. This means that the fragile COVID check or potential immunity status itself may expire or be frequently updated.

BlockChain

CovidPass[8] uses block chain technology to store encrypted data from individual blood tests, so that users can prove that they have tested negative for COVID-19. Using block chain technology, it provides an encrypted record of the test results. The developers say it could allow healthy travellers to avoid quarantine. The app could also enable the safe re-opening of sports and entertainment venues and the global conference and exhibition industry.

CovidPass is the idea of Mustapha Mokass, one of the Young Global Leaders of the World Economic Forum.

Home-Printable PDF

After testing negative to COVID-19 or a positive antibody/immunity test, the patient receives a downloadable document that he can print out at home. It can be reprinted several times. The link with the actual identity is ensured by recording an official identification document when the test sample is taken at the doctor's office or at the test site. The data is protected by visual and digital coding that can be verified by smartphone apps or, in some cases, by lenses of simple, well-trained visual controls. In addition, the document and data can be verified online in special databases.

Upgraded ePassports

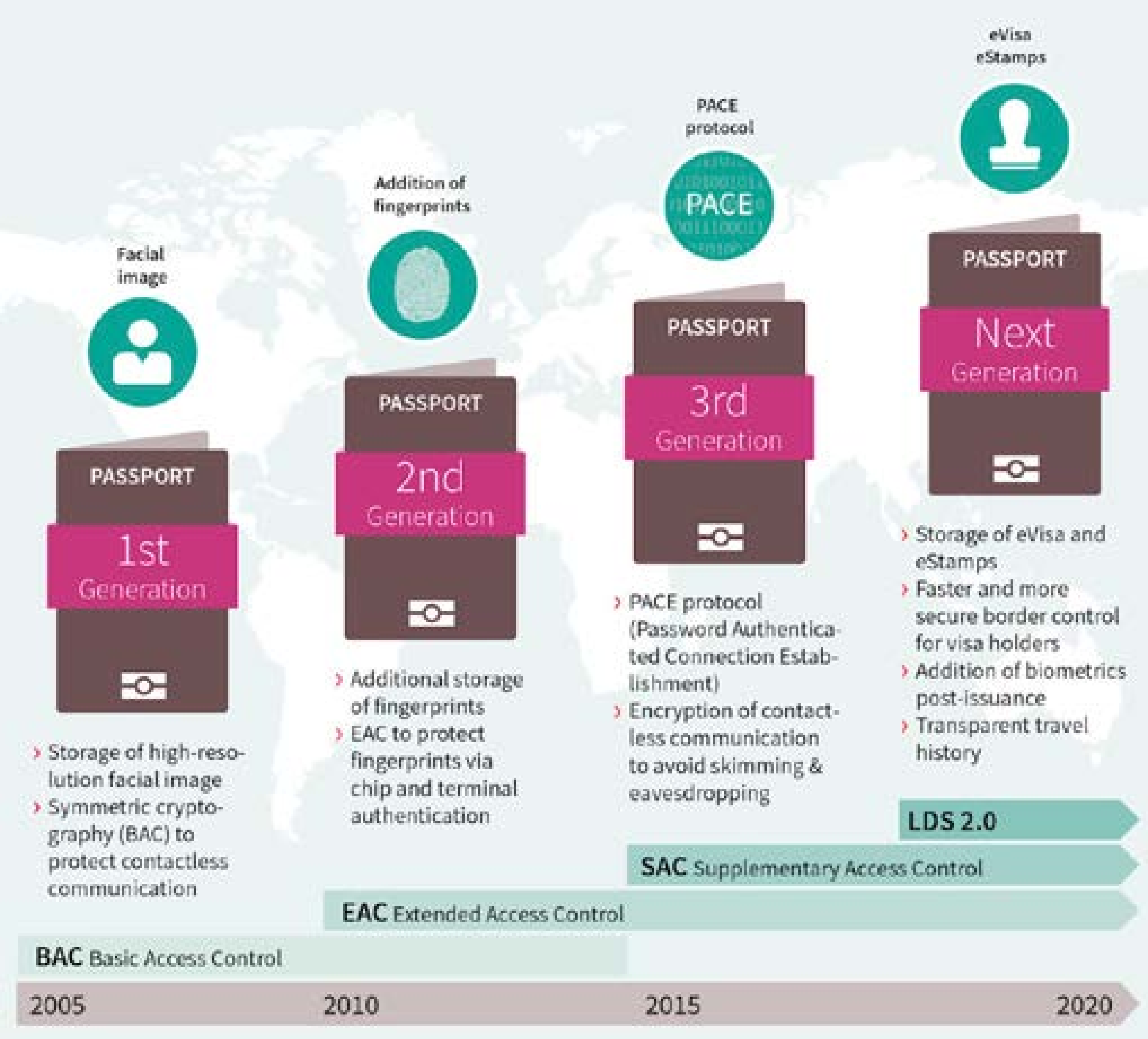
The ePassports standards have evolved over the years to allow for improved facilitation without compromising security. Notable developments are the Optional Logical Data Structure (AKA LDS2), Visible Digital Seal (VDS) and Digital Travel Credentials (DTCs). All of these innovations happened before the onset of this pandemic and could possibly be extended to dealing with the pandemic situation.

The driver for LDS2 was the desire to store travel related information like visas and travel stamps in the chip instead of being attached to the blank pages of the passport booklet. This was intended to facilitate easier reading at the various touchpoints of the travel continuum. Extending it to store additional health related information would be easy. However, the adoption and implementation of LDS2 itself is not trivial and reaching the minimum threshold required for it to be useful for health-related information is going to take some time and may not be of benefit in the near term.

The Visible Digital Seal was designed to extend cryptographic protection to paper documents that do not have an embedded chip in them. They are currently defined for two use cases. One, to protect the integrity of Visa Stickers and two, for Emergency Travel Documents. Extending it to include the use case for health information is trivial and could be used in both the app-based model and the Home-Printable PDF model. This is the most likely candidate for the current situation.

The Digital Travel Credential was designed to improve the possibility of touchless interaction for a seamless travel journey. It seems to be the most appropriate option for the current situation. The ICAO TAG/TRIP has just endorsed the first part of the specifications written by ISO and the next part is expected by middle of 2021. Once these specifications are in place, the deployment and use of DTCs could be the long-term solution for the current and future crises situations.

[8] *Could this COVID-19 'health passport' be the future of travel and events? https://www.weforum.org/agenda/2020/07/covid-19-passport-app-health-travel-covidpass-quarantine-event/*


Facial image
PASSPORT
1st Generation
› Storage of high-resolution facial image
› Symmetric cryptography (BAC) to protect contactless communication
Addition of fingerprints
PASSPORT
2nd Generation
› Additional storage of fingerprints
› EAC to protect fingerprints via chip and terminal authentication
PACE protocol
PACE
PASSPORT
3rd Generation
› PACE protocol (Password Authenticated Connection Establishment)
› Encryption of contactless communication to avoid skimming & eavesdropping
eVisa eStamps
PASSPORT
Next Generation
› Storage of eVisa and eStamps
› Faster and more secure border control for visa holders
› Addition of biometrics post-issuance
› Transparent travel history
LDS 2.0
SAC Supplementary Access Control
EAC Extended Access Control
BAC Basic Access Control
2005
2010
2015
2020

Roadmap of the LDS and Access Security of ePassports © Image: Infineon

WHO Intl. Vaccination Certificate

After a negative COVID test or positive antibody/immunity test, the patient receives an entry in his international vaccination card from his medical practitioner. The entry is made with a security seal. The doctor MUST confirm with a permanent pen that the exact passport or identity card is noted on the document. The document is tracked by a registered seal linked to the test report and possibly reported to the national database. Such security seals can integrate numerous physical and logical security features, which are very different from the traditional vaccination entries in the current document. This allows both offline and online validation of the status, which can be used internationally even in low-tech areas.

Other options are security solutions where the physical protection of the certificate is combined with the digital protection of the personalised data. For such approaches, Diffractive Optically Variable Image Devices (DOVIDs) can be used, where a key pair of a hashed public key in the form of an optically protected, metallised QR code is used in combination with a printed, signed 2D barcode. This enables the authentication of the certificate's carrier material and additionally ensures that the personalised data of the document has not been manipulated or altered.

INFORMATION FOR PHYSICIANS

RENSEIGNEMENTS DESTINÉS AUX MÉDECINS

World Health Organization

International Certificate of Vaccination or Prophylaxis

International Health Regulations (2005)

Organisation mondiale de la Santé

Certificat international de

INTERNATIONAL CERTIFICATE OF VACCINATION OR PROPHYLAXIS

Certificat international de vaccination ou de prophylaxie

© Image of seal by courtesy of Schreiner Printrust

Physical security documents

The issuance of physical documents poses some logistical and infrastructural challenges: there is a need to distribute a normalised set of system components to numerous places of registration or output. The adopted processes are divided into two subgroups: centralised issuance and decentralised issuance:

A) Initiation of process

1. A person who thinks they are immune to COVID goes to the doctor, or the person has tested positive and has a double negative test status, or the patient is treated directly in hospital.

2. Staff take the biographical data from a government document (ID/passport) and record it.

3. The medical staff guarantees the correct identification

4. The doctor sends the probe with the random unique identity (RUID) to the laboratory to validate the immune status.

B1) Central issuance

1. The biographical data will be sent along with the test-sample, including the postal address

2. Laboratory confirms a positive immune status

3. Central issuance prints certificate with joined RUID and personal data and sends document to patient and feedback to doctor

B2) Decentral issuance

1. Laboratory confirms a positive immune-status

2. The status is returned to the doctor, together with the RUID

3. The doctor issues the document and provides it to patient

The centralised issuing procedure has the advantage of a less decentralised, specialised technology. Decentralised output better protects the privacy of individuals, such as avoiding genetic fingerprinting.

> “ *At the time of writing, COVID-19 is still prevalent worldwide. Its’ impact upon both domestic and international travel cannot be underestimated in the mid to long term.*

The technology components for such documents are based on substrates and printers and on some appropriate track-and-trace IT systems.

When considering that documents have a long-life span, are subject to wear and tear or should be placed in a wallet with little effort and cost, synthetic security papers can be the first choice. They offer a high level of security, can be security printed and have the same features as those mentioned above. They can also be complemented by digital security technologies.

The use of encrypted QR codes and patterns, as well as physical security inks for personalised UV features (or others) is a considerable value that needs to be evaluated in decentralised, non-networked environments.

Conclusion

At the time of writing, COVID-19 is still prevalent worldwide. Its impact upon both domestic and international travel cannot be underestimated in the mid to long term. Airlines and the airport industry are assuming change will come, but ultimately it is down to government and perhaps organizations such as ICAO, CAPSCA or IATA to bring change forward that is both easy, understandable and manageable. The idea that we could return to ‘what we had before’ is probably unrealistic.

Very few of the countries currently impacted required medical reports for short-term travelers prior to the emergence of COVID-19. It is fair to presume that, moving forward, these countries may demand medical test results to be submitted (COVID-19 or other tests) to ensure that the travelers are free from any communicable disease in order to safeguard countries’ borders, independent of ‘travel bubbles’ and in addition to visas and other travel documents. At present, the viability of on-site pre-flight instant tests is being debated.

Additional health documents either in a physical or digital format are now a very real probability and the ability for organizations to ‘track and trace’ travellers is something that may be around for a long time. A consensus on the format of the document and the technology to enable their implementation has yet to be reached. There are pilot projects out there, such as the Digital Travel Credential, but full endorsement of the specification is not expected for at least another 12 months. Until that time, expectations are that individual countries will continue their ‘ad-hoc’ approaches in the short term, but the likelihood of a standardised health document for travelers is a certainty mid to long term – as is the expectation that there is no such thing as a ‘return to the way things used to be’. However, there is a need to create a best-practice, evidence-based, verifiable health declaration form with standardised evaluation procedures. From this, travelers shall have a higher certainty on what to expect during their travels. The use of sensors to provide such evidence, or to enforce adherence to governmentally imposed restrictions can be considered, and are a factor to be considered for health factor enhanced travel documents.☒

**You can read all 5 complete sections of this series by visiting www.secoia.ltd*

Digital *Certificates* – A *MATTER* of TRUST

By Guenther Fischer, Senior Consultant, Licensing and Protection at Wibu-Systems AG

The network specialist Cisco predicted a 26 percent increase in IP traffic year on year for the foreseeable future in its white paper "Cisco Visual Networking Index: Forecast and Trends 2017-2022".[1] By 2020, machine communication (M2M) has accounted for more than 14.6 billion connections or the majority of all digital communication, a steep rise from its share of 34 percent in 2017. With the rapid proliferation of Industry 4.0-ready machines, secure, unique, and tamperproof identities are becoming indispensable for all devices engaged in this unceasing and universal digital conversation.

> “ *Whether a certificate is valid and genuine can be ascertained quite easily by checking its expiry date and the public key of the relevant certificate chain.*

□ Certificates as Digital Proofs of Identity

All Internet users encounter them every day, at work or in private – but very few people are aware of what they are and why they are so important. We are talking about digital certificates. They are the backbone of all secure transactions over the web. Digital certificates contain the electronic ID of people, organizations, devices, or any other object, and they are protected against tampering and manipulation by cryptographic means. One particularly common type is the public key certificate: These include not only an ID, but also a related public key. Its counterpart, the private key, is stored in some secure place away from the certificate. With the public key contained in them, these certificates are used to prove digital identities beyond all doubt or to encrypt and sign data.

Certification Authorities: Neutral Arbiters

Official certificates are given out by known and recognized certificate authorities (CAs) or trust centers, acting as independent and trustworthy arbiters like public notaries in the physical world. For a person, organization, or object / device to get an official certificate, they need to bring proof of their identity to the CA, which can be a valid identity card, a copy of the company register, or a device's serial number. Their identity is checked, and if it is genuine, the CA creates a key pair and a certificate that contains all of the essential ID information – the public key, the expiry date, and the CA's name and digital signature. CAs act as essential roots of trust, which is why many CAs are household names in the field, like Symantec, Comodo, and GlobalSign. There are also alternative providers, set up to create certificates for free, such as Let's Encrypt (https://letsencrypt.org). Some companies have begun to host their own CAs to create and manage so-called self-signed certificates. Their trustworthiness is, in that case, limited to the specific organization they hail from.

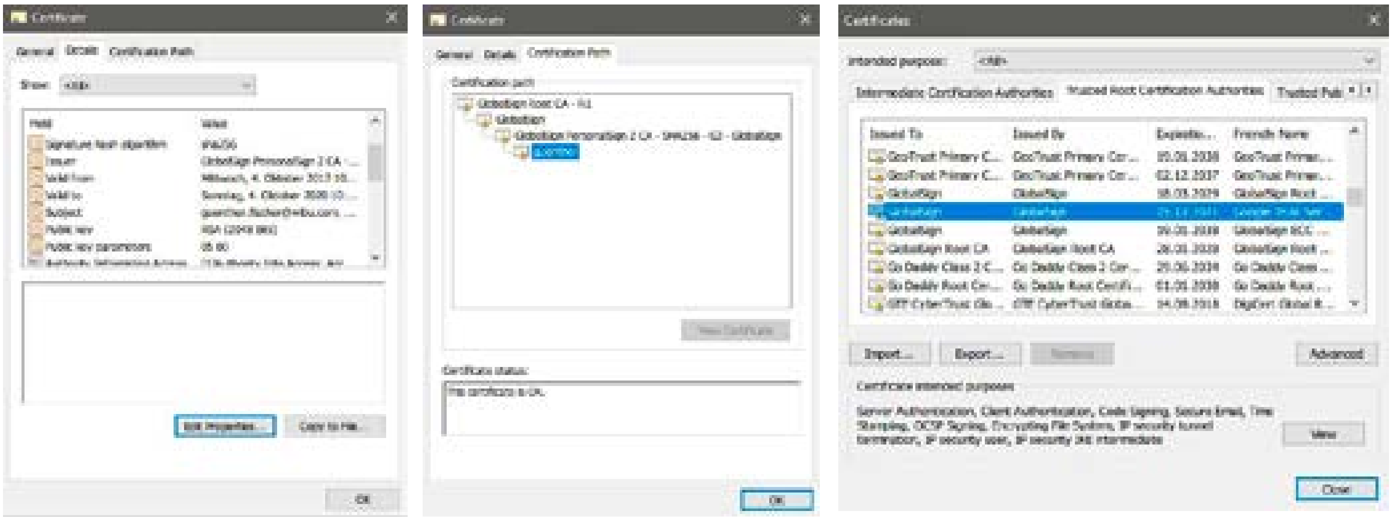
Validity of Certificates

Whether a certificate is valid and genuine can be ascertained quite easily by checking its expiry date and the public key of the relevant certificate chain. Every certificate should come with such an expiry date and only stay valid for that defined period – which depends on systems actually checking the expiry dates. The validity of a certificate can be checked by looking at the at the public key of its certificate chain: Every certificate is signed with the private key of its CA, which can be verified with the certificate assigned by the CA. The process checks the entire chain of certificates back to their root to establish their authenticity, since the genuineness of the root certificate cannot, by definition, be doubted.

Certificate Management and Distribution

Certificates come with one major challenge: Managing and distributing the certificates and private keys. Doing so manually, which is still the norm, can be a recipe for disaster, with catastrophic consequences if the private keys fall into the wrong hands. One prominent example is the eDellRoot certificate preinstalled by DELL – and distributed alongside the private key (https://securesense.ca/sayhello-edellroot).

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html



Field	Value
Signature hash algorithm	sha256
Issuer	GlobalSign PersonalSign 2 CA ...
Valid from	Mittwoch, 4. Oktober 2017 10...
Valid to	Sonntag, 4. Oktober 2020 10:...
Subject	guenther.fischer@wibu.com, ...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Information Access	[illegible]

Certification path:

GlobalSign Root CA - R1
GlobalSign
GlobalSign PersonalSign 2 CA - SHA256 - G2 - GlobalSign
guenther

Certificate status:
This certificate is OK.

Issued To	Issued By	Expiratio...	Friendly Name
GeoTrust Primary C...	GeoTrust Primary Cer...	16.01.2036	GeoTrust Primar...
GeoTrust Primary C...	GeoTrust Primary Cer...	02.12.2037	GeoTrust Primar...
GlobalSign	GlobalSign	18.03.2029	GlobalSign Root ...
GlobalSign	GlobalSign	15.12.2021	Google Trust Ser...
GlobalSign	GlobalSign	19.01.2038	GlobalSign ECC ...
GlobalSign Root CA	GlobalSign Root CA	28.01.2028	GlobalSign Root ...
Go Daddy Class 2 C...	Go Daddy Class 2 Cer...	29.06.2034	Go Daddy Class ...
Go Daddy Root Cer...	Go Daddy Root Certifi...	01.01.2038	Go Daddy Root ...
GTE CyberTrust Glo...	GTE CyberTrust Globa...	14.08.2018	DigiCert Global R...

Certificate intended purposes

Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, OCSP Signing, Encrypting File System, IP security tunnel termination, IP security user, IP security IKE intermediate

X.509 certificate with expiry date, certificate chain, and root certificate

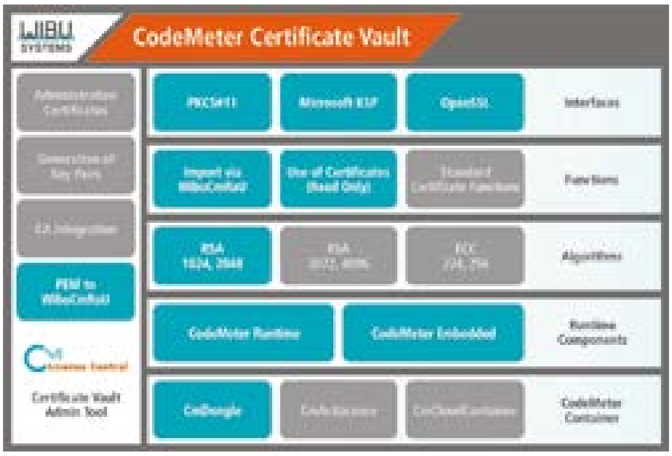
Straightforward and Secure: CodeMeter Certificate Vault and CodeMeter License Central

Wibu-Systems, the innovator of software protection, licensing, and security solutions, takes all of the fuss out of using certificates, without compromising on their security. This is made possible by CodeMeter Certificate Vault, based on the award-winning CodeMeter technology, and Wibu-Systems' CmDongles as special secure elements with integrated smart card chips to serve as protected key storage and cryptographic engines. CmDongles are sold in a choice of form factors ranging from USB, SD, microSD, or CF to directly integrated ASIC options, with industrial grade versions for use even in extreme environments available for each variant. CmDongles can also come fitted with MSD flash memory storage e.g. for signed logs. CodeMeter Certificate Vault stores all certificates in the safe harbor of the smart card chip. On top of CodeMeter's own API, it works with other standard interfaces like PKCS#11, KSP, and OpenSSL to make the solution a perfect fit for any existing application and every client's needs. The PKCS#11-compliant token provider was designed to work with Microsoft's Cryptographic API Next Generation (CNG) and the OpenSSL API to empower users with easier access to secure identities, digital signatures, emails, or VPNs with robust authentication systems.

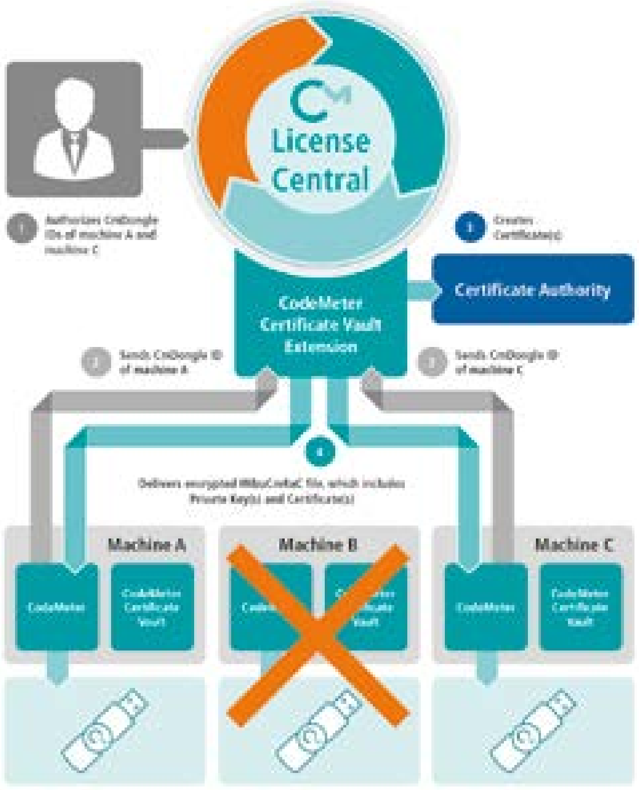
CodeMeter License Central, the popular backend system for creating, managing, and distributing licenses, can now also be used to distribute certificates and keys securely via CmDongles. Certificates can be created and rolled out automatically and with minimum effort, and the private keys and certificates are safe from being read, shared, duplicated, or otherwise compromised. Whenever a certificate is used, a cryptographic operation using the private key is executed.

> *Certificates can be created and rolled out automatically and with minimum effort, and the private keys and certificates are safe from being read, shared, duplicated, or otherwise compromised.*

CodeMeter License Central streamlines the formerly circuitous process of requesting, updating, or installing signed certificates. The entire administration and certificate creation process happens in one central place, with the option of including a higher certificate authority, such as a company's own CA. This CA could act as a trust center to verify that the public key is indeed valid and assigned to the machine or device in question.



Features of CodeMeter Certificate Vault Felder highlighted in turquoise


License Central
Authorizes CmDongle IDs of machine A and machine C
Creates Certificate(s)
Certificate Authority
CodeMeter Certificate Vault Extension
Sends CmDongle ID of machine A
Sends CmDongle ID of machine C
4
Delivers encrypted WibuCmRaU file, which includes Private Key(s) and Certificate(s)
Machine A
Machine B
Machine C
CodeMeter
CodeMeter Certificate Vault

CodeMeter Certificate Vault

Public key certificates are indispensable for authenticating the identity of individuals, organizations, or other entities, like machines or hardware devices.

Keys and certificates created in a central and secure environment are taken by the CodeMeter Certificate Vault Admin Tool or CodeMeter License Central and repackaged in an encrypted update file (WibuCmRaU) that moves them for exclusive use on a dedicated CmDongle. Updating the dongles happens in a sophisticated sequence of steps using a request (WibuCmRaC) and response file (WibuCmRaU), which makes for a far simpler, but highly secure process. It also allows the additional security features of CodeMeter to be used, like time limits for certificates, since CodeMeter has an internal and tamperproof UTC clock.

Conclusion

Public key certificates are indispensable for authenticating the identity of individuals, organizations, or other entities, like machines or hardware devices. They are proof that data is genuine and has not been tampered with. The combination of public and private keys can be used to establish a secure channel of communication, as long as the private key is safely stored away in a separate and impenetrable secure element, like a CmDongle. This also goes for the storage of certificates if they are to be trusted as standard and their authenticity not checked separately. To enable all of this, Wibu-Systems provides its powerful CodeMeter License Central as the backend system for the central management and distribution of certificates and private keys. It fulfills all the requirements for truly secure machine / device identities, facilitating the type of reliable machine communication that underlies the vision of Industry 4.0.☒

SILICON TRUST DIRECTORY 2020

THE SILICON TRUST

THE INDUSTRY'S PREMIER SILICON BASED SECURITY PARTNER PROGRAM

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

THE SILICON TRUST PROGRAM FOCUSES PRIMARILY ON:

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

EXECUTIVE COUNCIL

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

INFINEON TECHNOLOGIES

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

www.infineon.com

ADVISORY BOARD

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

BSI

Bundesamt für Sicherheit in der Informationstechnik – The German Federal Office for Information Security (BSI) is an independent and neutral authority for IT security. It has been established in 1991 as a high level federal public agency within the area of responsibility of the Ministry of the Interior. The BSI's ultimate ambition is the protection of information and communication.

Especially in the area of smart card technology, BSI is responsible for the design and definition of secure solution requirements for governmental identification documents. The German ePassport has been introduced in 2005, the second ePassport generation followed 2007, and starting in 2010 the all-new German eID card has opened a new trustworthy approach to Internet authentication for all German citizens. Security of all these documents is based on BSI specifications, developed in close collaboration with European/international standardization bodies and leading industry partners.

www.bsi.bund.de

FRAUNHOFER AISEC

Fraunhofer AISEC supports firms from all industries and service sectors in securing their systems, infrastructures, products and offerings. The institution develops qualitatively high-value security technologies, which increase the reliability, trustworthiness and tamper-resistance of IT-based systems and products. The approximately 80 members of the Fraunhofer AISEC scientific and technical staff balance economic needs, user-friendliness, and security requirements to develop optimally tailored concepts and solutions.

The security test labs are equipped with state-of-the-art equipment, and highly qualified security experts evaluate and analyze the security of products and hardware components as well as software products and applications. In our laboratories, functionality, interoperability and compliance are tested to give clients targeted, effective advice. Strategic partnerships with global corporations as well as with internationally recognized universities guarantee scientific excellence as well as its market-driven implementation.

www.aisec.fraunhofer.de

ULTIMATE ID CARD

SILICON TRUST PARTNERS

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

AdvanIDe

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

ATOS

Atos SE is an international information technology services company with 2014 annual revenue of € 9 billion and 86,000 employees in 66 countries. Serving a global client base, it delivers IT services through Consulting & Systems Integration, Managed Operations, and transactional services through Worldline, the European leader and a global player in the payments services industry. It works with clients across different business sectors: Manufacturing, Retail & Transportation; Public & Health; Financial Services; Telcos, Media & Utilities.
www.atos.net

AUSTRIACARD

AUSTRIACARD AG is a holding company of businesses providing end-to-end solutions and products in the field of Digital Security and Information Management. The Group brings together the century-long heritage in printing services and state-of-the-art digital data solutions (Information Management division) with the well-established production and personalization of smart cards and the offer of cutting-edge digital payment solutions (Digital Security division). The combination of well-established industrial roots with an expanding services portfolio that meets the needs of the increasingly digital and mobile economy is at the very core of the Group's confidence in its future.
www.austriacardag.com

AVATOR

AVTOR LLC is an integrator of cybersecurity solutions and the leading Ukrainian developer in the field of cryptographic protection of confidential information. The AVTOR's hardware secure tokens and HSMs are based on smartcard technology and own smartcard operating system "UkrCOS" are compliant for operations with qualified digital signatures and classified information.

AVTOR provides services for development and integration of complex cybersecurity systems for automated systems for different purposes and any level of complexity and predominantly deals with: protection of data transfer (IP-traffic); secure electronic document management; developing corporate and public certifying authorities (CA) in public key infrastructure (PKI); integration of complex information security systems; development of special secure communications systems.
http://www.avtor.ua/

CARDPLUS

CardPlus is a consulting firm with a focus on customized, enterprise level, Identity and Security Management Solutions. We offer a full range of Professional services to build, transform, implement and manage our customized enterprise level security and identity solutions. Due to our vast hands-on experience in designing and implementing secure travel and identification systems for governments and large public sector customers, we are uniquely positioned to understand your highly complex security requirements and translate the same into practical, workable solutions.
www.cardplus.de

COGNITEC

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

CRYPTOVISION

cryptovision is a leading supplier of innovative cryptography & public key infrastructure (PKI) products. The lean and intelligent design of the complete product range makes it possible to integrate the most modern cryptography and PKI application into any IT system. cryptovision PKI products secure the IT infrastructures of diverse sectors, from private enterprise to government agencies. The consultancy service spectrum ranges from the risk analysis of subsystems or standalone systems to the design of complete cross-platform cryptographic architectures.
www.cryptovision.com

DE LA RUE

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

DIGITAL IDENTIFICATION SOLUTIONS

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

www.digital-identification.com

GEMALTO

Gemalto, a Thales company, is a global leader in digital security, bringing trust to an increasingly connected world. We design and deliver a wide range of products, software and services based on two core technologies: digital identification and data protection.Our solutions are used by more than 30,000 businesses and governments in 180 countries enabling them to deliver secure digital services for billions of individuals and things. Our technology is at the heart of modern life, from payment to enterprise security and the Internet of Things.We have built a unique portfolio of technology and expertise including physical and digital identity credentials, multiple methods of authentication – including biometrics – and IoT connectivity as well as data encryption and cloud service protection. Together, these technologies help organizations protect the entire digital service lifecycle from sign-up to sign-in and account deletion with data privacy managed throughout.Gemalto is part of the Thales group, a €19bn international organization with more than 80,000 employees in 68 countries worldwide.

HBPC

Pénzjegynyomda Zrt. (Hungarian Banknote Printing Shareholding Company) is the exclusive producer of 'Forint' banknotes, and is one of the leading security printers in Hungary, specializing in the production of documents and other products for protection against counterfeiting. Currently, HBPC produces passports, visa, ID documents, driving licenses, securities, duty and post stamps, tax stamps and banderols, paper- and plastic-based cards, with or without chip, and is aiming to provide complex system solutions.

www.penzjegynyomda.hu

HID GLOBAL

HID Global Government ID Solutions is dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide. HID Global Government ID Solutions offers government customers an end-to-end source for their most demanding state and national ID projects. With Genuine HID™, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Government ID Solutions offerings include expert consulting services, data capture, credential management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelaminates, LaserCard® optical security media technology, and FARGO® card printers.

www.hidglobal.com

MASKTECH

MaskTech is the leading independent provider of high secure system on chip designs, embedded ROM masked products, security middleware, certification and integration services focused on human credential applications. MTCOS – MaskTech Chip Operating System – is a high performance and high security operating system, especially designed for secure semiconductors with powerful crypto co-processor and RFID, dual interface or contact interface. MTCOS is available on a unique variety of microcontrollers of different silicon vendors. MTCOS is a fully open standard (ISO/IEC) compliant multiapplications OS, used in more than 40 eID projects worldwide.

www.masktech.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

MK SMART

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

With production capacity of over 300 mio. card per annum and more than 700 employees, MK Smart (a member of MK Group) is ranked under the Top 10 largest card manufacturers globally. The companies production facilities and products are security certified by GSMA, Visa, Mastercard, Unionpay, ISO 9001 and FIDO. Our system and solutions business unit offers advanced issuance solutions and software for integrators and operators in all targeted industries.

MÜHLBAUER ID SERVICES GMBH

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

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

http://www.muehlbauer.de

OVD KINEGRAM

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

www.kinegram.com

PARAGON ID

Paragon ID is a leader in identification solutions, in the e-ID, transport, smart cities, traceability, brand protection and payment sectors. The company, which employs more than 600 staff, designs and provides innovative identification solutions based on the latest technologies such as RFID and NFC to serve a wide range of clients worldwide in diverse markets.Paragon ID launched its eID activity in 2005. Since then, we have delivered 100 million RFID inlays and covers for ePassports. 24 countries have already chosen to rely on the silver ink technology developed and patented by Paragon ID for the deployment of their biometric electronic passport programs.Today, Paragon ID delivers nearly 1 million inlays each month to the world's leading digital security companies and national printing houses, including some of the most prestigious references in the industry. Through 3 secure and certified manufacturing sites located in France (Argent sur Sauldre), USA (Burlington, Vermont) and Romania (Bucharest), Paragon ID ensures a continuous supply to its local and global clients. Visit our website for more information and our latest news.

www.paragon-id.com

PAV

PAV Card is a German, family-run business and one of the leading manufacturers for smart cards and RFID solutions. PAV products are used in many applications, ranging from hotel access, airport and stadium technology to the use in retail outlets and smart card applications, such as payment and health insurance. PAV's product range includes special heat resistant and tamper-proof ID cards as well as smart cards using the latest contactless technology for secure access solutions suitable for corporate buildings or sensitive access areas, such as airports.

www. pav.de

POLYGRAPH COMBINE UKRAINA

State Enterprise "Polygraph Combine "Ukraina" for securities' production" is a state company that has more than 40 years of experience in providing printing solutions. Polygraph Combine "Ukraina" has built up its reputation in developing unique and customized solutions that exceed the expectations of customers and partners. Moreover, the enterprise offers the full cycle of production: from prepress (design) processes to shipment of the finished products to customers.It offers the wide range of products: passports, ID documents, bank cards, all types of stamps (including excise duty and postage stamps), diplomas, certificates and other security documents. Find more information at:

www.pk-ukraina.gov.ua

PRECISE BIOMETRICS

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

www.precisebiometrics.com

PRIMEKEY

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

www.primekey.com

PWPW

PWPW is a commercial company, entirely owned by the Polish Treasury, with a long tradition and extensive experience in providing security printing solutions. The company offers modern, secure products and solutions as well as highest quality services which ensure the reliability of transactions and identification processes. It is also a supplier of state-of-the-art IT solutions.
www.pwpw.pl

SECOIA EXECUTIVE CONSULTANTS

SECOIA Executive Consultants is an independent consultancy practice, supported by an extensive global network of experts with highly specialized knowledge and skill set. We work internationally with senior leaders from government, intergovernmental organizations and industry to inspire new thinking, drive change and transform operations in border, aviation, transportation and homeland security. SECOIA provides review and analysis services for governments in the field of Civil Registry, Evidence of Identity, Security Document issuance and border management. Also, SECOIA specialises in forming and grouping companies for sustainable, ethical sales success. Adding to the consulting and coaching activities, SECOIA offers Bidmanagement-Coaching and RFP preparation / Procurement assistance for Government offices and NGOs. Try us, and join the growing family of customers.
www.secoia.ltd

SIPUA CONSULTING

SIPUA CONSULTING® is a leading and well-established consultancy company, focusing on customized e-ID solutions for government agencies and institutions around the world. Based on detailed market intelligence and long-lasting relationships within the e-ID ecosystem, SIPUA CONSULTING is in the strategic position to conceptionalize, promote and implement various projects along the value chain.
www.sipua-consulting.com

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, a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market. Wibu-Systems' comprehensive and award-winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and intelligent device manufacturers who distribute their applications through computers, PLC, embedded-, mobile- and cloud-based models. .
www.wibu.com

X INFOTECH

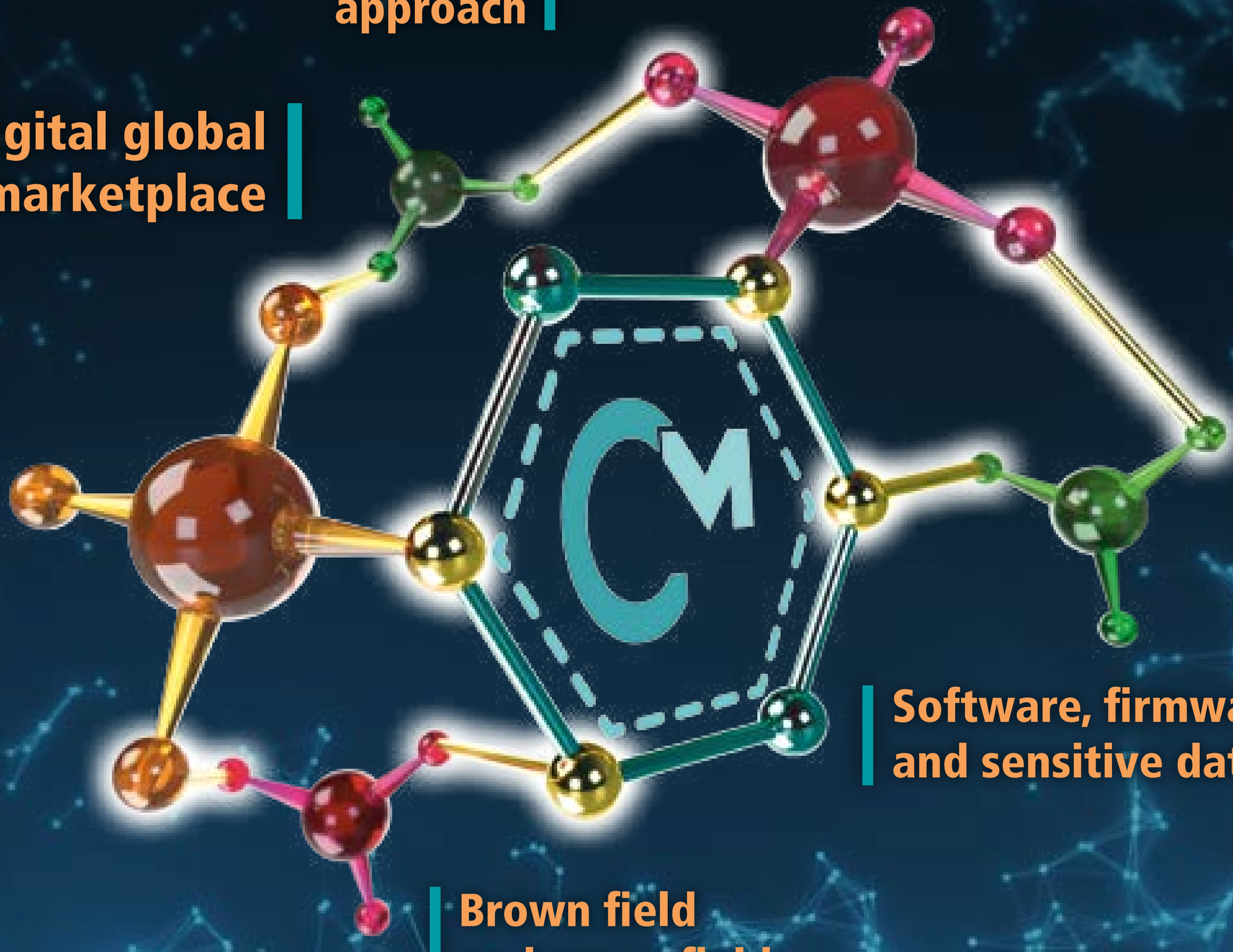
X INFOTECH, a leading systems integrator and a developer of software suite Smarteo, delivers premium solutions for issuing, managing and verification of electronic ID documents and smart cards. The company's turnkey solutions are fully independent and flexible, and in combination with unrivalled team expertise, allow smart card and eID programs to be implemented easily, adapting to any environment by supporting any equipment and chip type. With successfully implemented projects in 45 countries already, X INFOTECH is now a trusted business partner and preferred solutions and services provider for hundreds of customers.
www.x-infotech.com

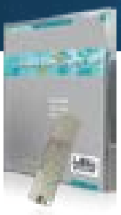
WIBU SYSTEMS

CodeMeter – the Catalyst of the IoT driven Economy

Let CodeMeter inspire you with new license-driven business models

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


Customer centric approach
From the cloud down to FPGAs
Digital global marketplace
Software, firmware, and sensitive data
Brown field and green field



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

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

SECURITY
LICENSING
PERFECTION IN PROTECTION