YEAR 23 OCTOBER 2020/ **ISSUE 85**

INFOSECURA

A magazine for the security printing industry worldwide, published four times a year by Intergraf in Brussels and mailed to named members of the security printing community, such as security printers, their suppliers, banknote issuing, government and postal authorities as well as police forces in more than 150 countries.

Contents

InfoSecura is published four times a year by Intergraf in Brussels. Information is accepted from industry contributors on a bona fide basis. Signed articles imply the personal opinion of the author and do not necessarily reflect the policy of Intergraf. Information and articles may be submitted to the publisher, who is free to accept or reject any item for publication. The publisher reserves the right to edit all submissions including reader's letters.

Editor-in-chief: Beatrice Klose
Editor: Manfred Goretzki
Editorial office and publisher:
Intergraf, 130 A, Avenue Louise
B-1050 Bruxelles
T. + 32 2 230 86 46
F. +32 2 231 14 64
securityprinters@ intergraf.eu
Advertising inquiries: Manfred Goretzki

Virtuality is real

The main focus of this issue of Infosecura is on matters of identity. At least that was the original idea. But then, as so often in these Covid 19 days, reality intervened. The plan was to publish two more issues before the coming conference in Lyon, as back in March 2020 we had been confident that the pandemic would be noting but a bad memory by the time the date for the next Intergraf conference came around. Over the late summer, the confidence of the Committee of Experts and Intergraf's leadership dipped and finally in the last days of September we had to face reality: It will not be safe to hold a physical conference in March 2021 in Lyon, not for the delegates, nor for the speakers, the exhibitors or for the staff. The alternatives were to cancel that date and announce a new date one year later or to hold a virtual conference instead of the physical one. In the end, the committee decided to do both. You will see the reasoning and the decision in detail on the next page. This decision also meant that speakers and exhibitors, that had already planned for the conference in March 2021, had to be notified first, hence the publication of Infosecura, with the announcement to the wider security printing community, had to be delayed by some weeks.

Meanwhile, the main subject of this issue has lost nothing of its urgency. Track and trace has moved from the ability of follow a parcel or a commercial shipment from sender to receiver to the ability to trace the movements of any person and find the other people that person had contact with. This scenario is close to the worst nightmares of any privacy-conscientious citizen. And yet, to know who may have infected you, or who you may have infected is vital for overcoming the pandemic. It takes extraordinary sensitivity on the part of the authorities and also assurances that any surveillance measures are temporary to gain the acceptance and cooperation of the population.

Meanwhile many occupations have become quite solitary, even writing and editing a magazine like this one. Not that long ago, before a completed issue was sent to the printer, the editor would meet with a trusted friend and former colleague on the Committee of Experts to go through the issue to be published to ensure that it was factually correct and reflected the thinking in the industry. That friend was Jacques van Droogenbroeck, the former head of the National Bank of Belgium printing works and later, of Sicpa. Although he was retired, he still had an excellent and up to date knowledge of security printing and an active and extensive network of serving and former heads of the industry. He also was a gentleman of the 'old school' and as a true 'Bruxelloise', a connoisseur of wine and food. Our 'post-editorial' meetings in one of the restaurants around the fish market in Brussels were a pleasure as well as an education. Jacques died, aged 81 on September 19, 2020. He will be much missed.

The Editor

Intergraf Currency+Identity Conference and Exhibition will be a virtual event on the planned date, March 24 to 26, 2021

Dear Colleagues

We were looking forward to staging Intergraf in March next year to meet you at our conference and exhibition, as we did every year. Intergraf Currency+Identity in Lyon was to be something special. The town at just about any time of the year is a delight and in spring especially so. The conference programme was ready and looked great and the exhibition, judging by the stand bookings received, was bound to be a success. We were ready and we believe, so were you.

Intergraf has been running events for the currency and identity industry for over four decades. Some of you may be relatively new to these. But many among you have been with us quite some time. Year after year, you return to fill the seats of our conference rooms, not only to listen, but to feel and to participate in the way the industry moves. And to forge new partnerships on our exhibition floor. In doing so, you have made Intergraf Currency+Identity what it is. So the first thing I want to do is to thank you.

I would like to share with you our plans for the immediate future. The COVID-19 pandemic has affected nearly every aspect of our daily lives. It has changed the way in which we connect. And it has transformed our work. Our community is no exception. Like many, we wrestle with the uncertainty and scale of all that is happening just now. So I want to share our plans with you openly and honestly.

This is to formally announce that we're postponing the event we planned to stage in Lyon, France in March 2021. The well-being and safety of our attendees, speakers and exhibitors is our highest priority. Our next in-person event will take place in France, in Lyon, on 6-8 April 2022.

2022 is a long way away. We recognise that. And we also believe, now more than ever, that it is critical for our community to unite. Business leaders, decision-makers and innovators like you need a shared space and moment to reconnect. It has always been Intergraf's mission to provide that platform. So that you can collaborate and make a positive impact on our society.

We had long discussions with our Committee of Experts - per video link of course. We considered what action to take. And with all this in mind, we made the choice to adjust our strategy and go virtual. To develop a new, online event that will enable you to fully engage in the challenges at hand in the world of currency and identity. It will take place on the same days: 24, 25 and 26 March 2021.

The virtual Intergraf Currency+Identity will go the extra mile to bring you what you need most. There will be livestreamed and on demand content from an exclusive line-up of experts at the forefront of their fields. There will be an exhibition showcasing emerging solutions and technologies. And there will be real interaction. Tools to let you to network in a secure environment, strictly restricted to attendes vetted by Intergraf.

Of course, we remain committed to Intergraf's in-person future on the other side of this crisis. But, for now, we're excited to invite you to be part of the virtual Intergraf Currency+Identity. With travel costs eliminated, you'll be able to join that global conversation no matter where you are. The virtual environment offers new possibilities. We'll be publishing more details on our website soon and look forward to seeing you online in 5 months. Until it is safe to welcome you again, face-to-face, in Lyon in 2022.

Beatrice Klose
Secretary General

TOMORROW'S ID IS ALREADY THERE

In many countries the Coronavirus lockdowns exposed flaws in national ID systems, which may have hampered efforts to track and trace any Covid 19 virus infections and to provide services to citizens. It seems that what was needed was a strong link between the electronic capabilities of modern ID cards and secure official and civil electronic systems, without endangering the privacy of citizens. It looks as if that goal has already been reached in some countries.

The Covid pandemic has strengthened the case for a digital ID ideally linked to a physical card. During the lockdowns, a huge range of human activities have moved online far more smoothly than almost anyone expected. Yet as they migrate to the virtual world, many people are discovering that they do not have the right documents to prove their identity. In dealing with officialdom this is crucial, as rather than simply exchanging goods for money, governments give money away and issue commands, so they need to know more about their "customers" than, say, a supermarket does.

In countries without a system of secure digital identities, the closure of bricks-and-mortar government offices and the shift of public services online have caused havoc. Italy's system for doling out emergency payments crashed and then demanded paperwork that applicants could not obtain because government offices were shut. In America, Washington state paid $650m in unemployment insurance to fraudsters who made applications using stolen identities, The Economist writes.

No such havoc occurred in Estonia, where every citizen has an electronic identity. More than just an identity card, it links every Estonian's records together. So when the government created a furlough system for workers affected by the pandemic, it already knew where they worked and how to pay them. Nobody in Estonia had to join a queue on a pavement to claim benefits, as people in other places did. Digital ID does not only make it quicker and easier to access government services remotely. It would also make track-and-trace systems more effective. If, in an emergency such as the pandemic, health data were linked to work data, governments could quickly spot when a cluster of covid patients all happened to work at the same factory.

Using the argument of efficiency may convince many people, but those that fear the overweening power of the state of constant surveillance of the population may turn just as many people off.

FROM IDEA TO REALITY

"A universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them." This sentence appeared in the European Commission's Communication entitled "Shaping Europe's digital Future", which sets out the three key objectives in the EU's digital strategy: Technology that works for people, a fair and competitive economy and lastly, an open, democratic and sustainable society. It is also a dig at the overwhelming presence of platforms such as Facebook, Google, etc. granting them access to a wide array of personal data about that consumer.

It is the first of these objectives that leads to the question; if the technology works for the people, will the people be able and want to work with the technology? The fact that the Covid pandemic forced thousands to work remotely from home, which necessarily involves technology, shows that many people are able to use technology in their daily lives. However, the 'universally accepted' part of the first sentence does not only mean that the eID is to be accepted everywhere, but also accepted - and used - by everyone. And in this, in spite of the Covid-forced uptick in the use of technology, there are some problems.

In France, 13 million people, or close to 20 per cent of the population, have difficulties with digital applications, an article in the press said. In Germany, which was one of the early adopters of eID, even before the EU Regulation on ID cards, about 63 million Germans, out of a population of around 81.4 million, already have the new version of the national ID card, which contains extensive electronic capabilities in its eID function. Until 2017 there was a choice to activate this or not, but since 2017 the eID function has been activated in every new ID card. However, before that date, figures show that only 25 million had activated this function. Later figures, after the automatic activation, indicating use, are not available.

In June 2019, the Council of the EU adopted a regulation, which introduced tighter security for ID cards in order to reduce identity fraud. Under the new rules, identity cards will have to be produced in a uniform, credit card format (ID-1), include a machine-readable zone, and follow the minimum security standards set out by ICAO (International

Civil Aviation Organisation). They will also need to include a photo and two fingerprints of the cardholder, stored in a digital format, on a contactless chip, making them eID cards. There are also rules on the length of validity of eID cards. Until the new regulation came into effect, ID cards varied greatly across the EU in every respect. They now will be much more uniform but they are still not obligatory for member countries. Among EU member countries, Denmark and Ireland do not issue ID cards, nor do Iceland, Norway and the UK outside the EU. In Austria, an ID card is not mandatory. In this context, it is remarkable that the 10-year validity period of French ID cards issued after 1/1/2014, which do not have any electronic function and do not adhere to the ID-1 format, has just been extended by another 5 years.

The new regulation will prompt the French government to add an electronic capability to all newly issued French ID cards (see article on page 6). Depending on how it is implemented, it may also make the planned, but not yet introduced, Alicem electronic platform that is to enable trusted online identification and interaction between French citizens and the state, as well as with economic entities, superfluous. Alicem ran into difficulties because it proposed to use facial recognition technology in the enrolment process, which was opposed by the government's own data regulator CNIL. The link between user data and the Alicem platform will be provided by the chip in the French ePassport, not by the ID card. Passports are not mandatory in France.

The latest version of the German ID card

DIFFERENT WAYS TO REACH A GOAL

That facial recognition is not the only route to verifiable identification online is demonstrated by the German ID card.

The German ID card contains a chip, which enables it to be used online and which offers secure identification on the Internet and on government or civil websites. During identification all personal data are protected and are transmitted in completely encrypted form. The identification process starts by an online service demanding identification. The user then creates a connection between ID card and smartphone or/and card reader and he sees who requests which data. If the user agrees to the request, he submits his six figure PIN code. The chip in the ID card checks if the owner of the online service had the official authority (given by the state) to request the data and only if that authority is established, the data is transmitted in encoded form. The basis of this process is that the ID card is deemed secure and the two-factor verification is given by the presence of the ID card and the PIN number.

If the German eID model seems advanced, the Estonian model is much more so. In that country, electronic identity (eID) is a cornerstone of the Estonian digital ecosystem. Here the ID-card is an identification card that can be used also in the digital world. It has a chip containing a microprocessor and some memory, supporting two secret keys, one used for authentication and a key for digital signatures. All operations are done inside the microprocessor and the secret keys never leave the chip. However, to use the ID-card the computer needs software in order to communicate with the chip. Therefore, one has to install the ID-card software before the card can be used.

The ID-card, in its physical manifestation, is a means of authentication and electronic signing for about 5,000 public and private sector services. Over 98 per cent of Estonians have an ID-card and 67 per cent of the population use it on a regular basis. Here are some examples of how the eID is regularly used in Estonia: to prove identity when logging into bank accounts, to sign documents digitally, to vote using the I-Voting system, to check medical records or use an e-Prescription service and to establish a company or submit tax declarations. And in spite of all these electronic functions, the Estonia ID card is still a physical card. ■

The Estonian ID card version 2019. It supports near field communication technology (NFC), but it does not incorporate the changes called for in the latest EU regulation, which require a colour photograph and the three letter code of the country on a blue background surrounded by the EU stars.

FRANCE: SECURE ID AND THE PERILS OF FACIAL RECOGNITION

In June this year the French government introduced plans for a digital national ID card. This followed an announcement in autumn last year to create a new digital identification service to give citizens highly secure access to sensitive online services such as banking and tax sites. The latter got stuck in parliament, because it uses facial recognition in the enrolment process. The former is still on course but details of what the new digital ID card will look like are scarce.

An article in *France Culture* of 11 June reported that France is planning to introduce a national digital identity card sometimes in 2021. The Assemblée Nationale, the French parliament, is due to publish a report about digital identity and make around forty recommendations for this project. The aim of this future digital identity device is to enable citizens to identify themselves securely on the Internet just like they do now with the national identity card in the 'real' world, especially when they want to access any of the 500-plus services available via FranceConnect, a government-backed online services gateway used by government agencies and private sector companies including banks.

This means that the state will need to create a digital identity platform and in June, the Secretary of State for Digitalisation declared that the project this time had to succeed and become a reality in the lives of French citizens. The project had been continuously pushed back because of fears linked to general surveillance of the population. Last year, the application Alicem, which was to allow access to public services online, was temporarily halted because it used facial recognition technology. Alicem is supposed to be finally operational as of the next 'rentrée' in September.

The article said that in order to follow European regulations, beginning in summer 2021, France will propose a digital national identity card that will eventually replace the identity card as used today. In parallel, a solution for a digital identity will be put in place. An information campaign, supported by an online consultation will publish 43 recommendations for this digital future.

A DIGITAL IDENTITY: WHAT FOR?

In our daily use of the Internet we use digital identity extensively, but that identity does not have to be complete, nor accurate. In some application even pseudonyms will do. We leave traces of our identity and of our use of the Internet every time we go online. This data is collected and used by the big players of the Internet, the American GAFAMI (Google, Apple, Facebook, Amazon, Microsoft, IBM) and the Chinese BATX (Baidu, Alibaba, Tencent, Xiaomi), often to target ads at specific audiences, but sometimes for more nefarious reasons. A secondary aim of the digital ID project is to lessen the power of these companies to collect data.

Increasingly, however, we also use the Internet to access online banking and administrative or official functions of the state, which require a far higher level of security than that used for private access. This is an evolution that is seen as necessary in the coming years especially as it is also mandated in the European regulation. For national ID, we need "a document that remains physical, with a chip but to which we want to add a purely digital identity that allows us to face our exchanges in the digital world ", said Jean-Michel Mis, the parliamentary co-rapporteur of the project.

One of the problems the project faces is that of the 'digital divide', as an estimated 13 million French have difficulties with digital applications. The remedy, the report will suggest, is the broadest possible use of training but, to assure all, the information report insists that digital identity remains optional.

ALICEM

The digital identity project is not the first foray of the French government into matters digital. In October last year it announced a new digital identification service, Alicem ("Authentification en LIgne CErtifiée sur Mobile" - Certified online authentication on mobile phones), which was to give those that use it and who have and know how to use an Android phone (not an iPhone), highly secure access to around 500 government websites and to banks. That was the plan, but because the technology uses facial recognition in the enrolment process, the plan hit a snag.

The French technology publication 01net explains that the one-time enrolment works like this: "Just as with contactless payment, you will need to scan the biometric chip of your electronic title (passport or ID card) using the phone. The system then has access to the data stored therein — except fingerprints — which will then be checked. This step verifies the authenticity and integrity of the document as well as its current validity. The final step is to perform biometric identity verification by making a selfie-video on the app that will capture expressions, movements and angles. That video is sent to a government server together with data, Alicem has collected from the chip. The server compares the video with the passport photo, checks the document hasn't been stolen and sends the user a code

with which he can set up an online identity. Then, the video is erased from the server. Finally, at the end of this process, the 'digital identity' is generated though a code the applicant is sent.

The new service was announced in May 2019 and has been undergoing testing by the French Ministry of the Interior since June 2019. The app was due to go live by the end of 2019 or early in 2020. The mention of facial recognition technology was sure to lead to public criticism, but even CNIL (Commission Nationale de l'Informatique et des Libertés - National Commission on Informatics and Liberty), France's own data regulator, was concerned that program violates the European rule of consent, guaranteed by the European Union's General Data Protection Regulation (GDPR), which forbids the collection of any biometric data without a user's free consent. At the same time, a French privacy group is fighting the initiative in an administrative court.

As mentioned, Alicem was to go live in September this year (or later). It is not certain that all legal hurdles have been cleared, but the government seems to be confident. The timing of such a move seems a little difficult. The Coronavirus lock-down and the attempts by France and many other countries at contact tracing have stoked fears of general surveillance. The French may not like electronic surveillance in any form or for any purpose. A newly introduced contact-tracing app "StopCovid" was downloaded 1.9 million times but only 68 users entered a positive COVID-19 test result and just 14 were notified of an at-risk encounter. France has a population of 67 million.

However, the criticism of facial recognition seems, in this case, a little 'thin-skinned' as facial recognition is only used once in the enrolment process to verify that the holder of the ID card or passport, as identified by the data on the chip, is the same person as the one on the video applying for online registration. If the French state does as it says and the video is erased, there is no possibility of using this example of facial recognition for any further surveillance. Additionally, the use of Alicem is to remain 'optional'. ■

WHAT IS HAPPENING IN THE AREA OF IDENTITY DOCUMENTS?

In a meeting of the Frontex Expert Group on Document Control in February, Dr Uwe Seidel gave a comprehensive overview of the changes and developments in European identity documents and the work that is being done on the world stage to make travel documents safer and more efficient.

Not only the international organisations of the airline industries, such as IATA and ICAO, meticulously follow any development in travel documents, the EU's Frontex, the European border and coast-guard agency, is doing the same. At a meeting of the Frontex Expert Group on Document Control in February, Dr Uwe Seidel, of the Forensic Science Institute of the Bundeskriminalamt, Germany's federal criminal police and member of Intergraf's Committee of Experts that is responsible for the contents of Intergraf's Security Printers conferences, gave an overview of the recent developments in the European document domain.

Dr Seidel looked at developments that are, or have been, happening in two areas, in the work of the ICAO New Technologies Working Group (NTWG) and in the regulatory environment of the European Union. In the EU it was the change to the 'Schengen visa' and the EU residence permit that mattered most.

The Schengen visa: the new (top) and the old

THE NEW EU SCHENGEN VISA

Before the current EU visa, which grants short-stay entry to 26 European countries, 22 of them members of the EU, was first used in a EU member country, Germany, in July 2018, its predecessor had been in use for 20 years. As Dr Seidel showed in his presentation, over the years the visa sticker had been compromised by high quality forgeries in almost every aspect, even by some especially good ones for the DOVID. In 2017, amendments to the relevant regulation Regulation (EU) 2017/1370 of 04 July 2017 had been proposed, which came

into force on 17/08/ 2017. It regulates also a transition period – but after 21/12/2019 only new visa were allowed to be issued. Currently, travellers from 104 countries and entities need to obtain a visa to enter the EU for stays up to three-months within the Schengen Zone.

The new Schengen visa had been a complex project, which was led by Germany and financed by the EU's Internal Security Fund (ISF), a EU financing scheme set up for the period of 2014 to 2020. As the Schengen visa is used by and produced by all Schengen countries, to be cost efficient, the specifications had to be suitable for the production capabilities of all participating countries, leading to necessary compromises. The main differences between the old visa and the new version is the layout, the addition of new sophisticated guilloches, a new DOVID vignette and the proposal for an new digital seal in the form of a two-dimensional barcode. The UV image on the visa was also changed.

Although highly complex and sophisticated, it did not take long for the first good counterfeits to appear. Although already discussed during the introduction of the new visa, one of the countermeasures taken to tackle the new counterfeits was the introduction of the mentioned digital seal, which contains the text of the MRZ and a digital signature as well as the passport number and the issuing date. It enables a comparison of the MRZ in the seal and that printed on the visa. It protects against forgery of data and stolen blanks, but not against photo substitution.

THE NEW EU RESIDENCE PERMIT

A similarly complex project, also funded by the EU's ISF was the new EU residence permit, which was led by Spain. As the residence permit is a standalone card, produced and issued by the member countries, efficient production in every issuing country required even more co-ordination and compromise than the visa sticker. Germany has issued the new card since November 2019 and, following EU regulation 2017/1954, as of 10 January 2021 it will be issued by all member states.

IDENTITY CARDS IN THE EU

Apart from not being compulsory in all EU member countries, the format, content and design of identity cards, unlike passports, was until now not regulated, which lead to considerable differences in security levels. Although often regarded as domestic ID documents, within the EU Schengen area, ID cards enable citizens to enter the Union coming from abroad and also function as ID document within and between the Schengen countries. Less secure ID cards have become the most frequently detected false documents used for intra-Schengen travel.

In June 2019, the EU introduced tighter security for ID cards in order to reduce identity fraud. The new rules, laid down in EU regulation 2019/1157 will improve the security by introducing minimum standards both for the information contained in them and for security features common to all member states that issue such documents. They do not require member states to introduce identity cards if they are not foreseen under national law.

Under the new rules, identity cards will have to be produced in a uniform, credit card format (ID-1), include a machine-readable zone, and follow the minimum security standards set out by ICAO. They will also need to include a photo and two fingerprints of the cardholder, stored in a digital format, on a contactless chip. ID cards will indicate the country code of the member state issuing them, inside a EU flag.

Identity cards will have a minimum period of validity of 5 years and a maximum period of validity of 10 years. Member states may issue ID cards with a longer validity for persons aged 70 and above. If issued, ID cards for minors may have a period of validity of less than 5 years. The new rules include strong data protection safeguards to ensure the information collected does not fall into the wrong hands. In particular, national authorities will have to ensure the security of the contactless chip and the data stored in it, so that it cannot be hacked or accessed without permission.

In general, existing identity cards which do not meet the requirements will stop being valid 10 years after the date of application of the new rules or at their expiry, whichever is earlier. The least secure cards, which do not meet the minimum security standards or do not have a machine-readable zone, will expire within five years.

RECENT DEVELOPMENTS IN THE ICAO NEW TECHNOLOGIES WORKING GROUP

As it does every three years, ICAO's New Technologies Working Group (NTWG) issued a request for information (RFI) to the international vendor community to report on progress, solutions and products in selected technology categories.

Among the main areas of interest that were selected are a strengthening of the electronic Machine Readable Travel Document (eMRTD), optimisation of the use of existing eMRTD capabilities, as well as future forms of eMRTDs. Also very high on the agenda of the NTWG is the development of guidelines and technical specifications for the ICAO Digital Travel Credential, which is the subject of a separate article in this issue.■

HOW WILL WE TRAVEL IN THE FUTURE?

Answering this question means looking in to a future we are very unsure about. Up until about March 2020, international bodies such as IATA or ICAO started their papers about the future of travel, by which they meant air-travel, like this: Increasing international traffic volumes are placing pressure on airport passenger facilitation, and the need for secure and trusted traveller identification remains ever present in the face of global turmoil.

That was then. In expecting global turmoil, many papers had been certainly correct, but their expectations centred usually on terrorism. What came changed everything. By April, airports had emptied out and even when travelling started again slowly in June and July, passenger numbers were a fraction of what they had been before the pandemic. Air travel between the US and the European Union had been closed down completely. But still, governments, industries and individuals must think about travel after the Coronavirus. A look back at an ICAO suggestion of February 2019, gives useful pointers.

That year, ICAO's New Technologies Working Group (NTWG) established a specialized sub-group to begin work on standardizing a digital travel credential (DTC), for which it used the ePassport as the benchmark, given that it offers a secure, portable, verifiable and unclonable token.

In digitizing the travellers' biographic and biometric data, ePassports have been very successful. Until 2019, over one billion had been issued by 139 states. The advantages they offer for e.g. improving security for border management and the authentication of travel documents are considerable. However, an article by Louise Cole at www.unitingaviation.com, claims that the ePassport until now has not been used to its full potential for changing the way travellers clear checkpoints during departure and arrival. She said that the DTC envisioned by the NTWG uses the technology available in the ePassport to create a credential that can bring additional benefits, while maintaining a balance between security and facilitation.

E PASSPORTS PLUS

As a recap, here are the attributes of the existing ePassport: It allows verifying entities to authenticate the credential supplied, it includes a means to protect against cloning, it accepts and stores pertinent holder and/or travel data, protects the privacy of the user and is has a secure verification process.

A DTC serves the same functions as an ePassport, it reliably confirms the identity of the traveller. In addition it can improve passenger flows by allowing travellers to give their data in advance and use more self-service options. It also allows the airport and airlines to link additional data, such as boarding passes, to the DTC and forward data to relevant authorities to support biometric matching through controlled checkpoints, to allow biometric boarding and can improve pre-arrival security and/or risk assessment. Of course, to achieve these advantages, globally-interoperable features have to be widely accepted, and an issuer needs to be able to control the credential.

THE TECHNOLOGY PLATFORM

The digital travel credential has to be based on a technology platform that offers a balance between security, ease of use and interoperability. The ICAO NTWG subgroup looked at technologies, or 'form factors', such as smart devices, closed servers, remote servers, and distributed ledgers. The criteria, which formed the basis of its examinations were that it could be produced by a travel document issuing authority, that it was globally interoperable so that it could be used in different environments and that it was capable of being adopted by travellers. The latter means that the traveller has to trust that the DTC is as, or more, secure than an ePassport and that his/her biographic and biometric data and privacy is protected.

Although each of the technologies, or 'form factors', had a number of positives, they all turned out to be less secure than an ePassport. The failings were mainly in the area of interoperability and security and would be unacceptable for most, if not all, border authorities.

A HYBRID SOLUTION

The subgroup thought that the problems could be solved by using one or more of the form factors together with the existing technology already used in the ePassport, to create a hybrid credential that would meet all the basic criteria and key attributes. This would be a combination of a virtual token (credential) that is linked to one or more physical tokens (authenticators). The credential could be stored in a remote system, such as a database or webserver, and the authenticator could be an ePassport, smart card, or mobile phone. The

virtual credentials would have to include many of the same security elements of the current ePassport, including authentication, when required by inspection authorities.

A border authority authenticates an ePassport by reading - validating - the chip, which verifies the digital signature in it and that shows the digital certificate was used by a bonafide authority when the data in the chip was sealed and confirms that the biometric and biographic data has not been altered. The authority can then confidently rely on the information in the chip to compare against the information printed in the physical passport book, and if need be, against the traveller themselves. To create a similar level of confidence is not easy but the subgroup thinks it can be done.

By linking the virtual travel credential to one or more physical tokens, the border agent can additionally actively authenticate the credential for increased security. The physical token can be used to retrieve the data from the remote system by authenticating the holder of the virtual credential to that system.

This is the model preferred by the ICAO NTWG, because the credential is already securely linked to the issuing authority. The physical token allows the verifier to select the correct virtual credential, including when it was provided in advance. It also gives the verifying entity the flexibility to decide whether the virtual credential is sufficient for the traveller to pass through controlled checkpoints without having to physically present their passport.

One of the advantages of the DTC is that it offers several options for creation and form, without losing the benefits of interoperability. The DTC itself could be derived from an existing ePassport by the holder. Or the issuing authority could create the DTC with the option to store the virtual component on a remote system or securely on a smart device.

When booking or checking in, travellers could send their virtual component in advance to the border authority, in an 'electronic system for travel authorization' (ESTA) process or using API/PNR etc. When they arrive at the airport, they could use their token, whether it is a physical token such as their phone, or purely virtual token, such as their facial biometric, to pass through the different check points in the airport journey. If it is not sent in advance, the virtual component must be able to be read in a standardized method using passive authentication.

The working group aimed to have the DTC technical specifications presented for endorsement by the ICAO TAG/TRIP in 2020. Whether that will even take place is not certain. ■

A SHARP EYE ON THE BORDER

Countries that have an external border, and that includes international airports, have sole responsibility for border control. But Frontex can provide additional technical support for EU countries facing severe migratory pressure, by coordinating the deployment of additional technical equipment and specially-trained border staff. It also assistes in the detection of fraudulent ID documents.

Fraudulent documents, especially ID documents, can be detected in a variety of places including banks, local administrations etc. Most frequently they are, however, detected at borders. Within the EU Schengen area this means the external EU borders and airports which are controlled by the national police of the country they are situated in. They are also the concern of Frontex, the European Border and Coast Guard Agency, which acts together with national border police forces. One of their tasks is to reduce illegal border crossings involving fraudulent documents, which are often used to commit other crimes, such as smuggling of drugs, firearms, stolen vehicles, trafficking in human beings and migrant smuggling.

Since the revision of the Schengen Borders Code in 2017, everyone crossing the external borders is being checked against national and European databases containing information on stolen, lost or invalid travel documents, and on persons suspected of cross-border crime.

CENTRE OF EXCELLENCE FOR COMBATTING DOCUMENT FRAUD

For years, Frontex document fraud experts have helped in joint operations at the EU external borders to identify and register migrants in hotspots and there hundreds of fraudulent documents are detected every year. In 2018, Frontex expanded its role in combatting cross-border crime and established the Centre of Excellence for Combatting Document Fraud.

Frontex developed a reference manual for border guards with images of passports, identity cards,

and visas, to help them determine whether the document in front of them is genuine.

The Centre of Excellence for Combatting Document Fraud also contributes to the work of other Frontex units, including risk analysis, training, as well as research and innovation. The Centre has a core staff working at the agency and over a dozen document experts from member states who can be sent quickly to a member state in emergencies related to document fraud. It also manages a document expert group of 85 experts in document fraud and forensics from member states, who participate in all document fraud related-projects and activities coordinated by Frontex.

SITUATION AT EU EXTERNAL BORDERS

In the first half of this year, the number of illegal border crossings at Europe's external borders fell by nearly one-fifth from a year ago to 36 400, mainly because of the effects of the COVID pandemic. The drop was largest on the Western and Eastern Mediterranean migratory routes. These two, with the Western Balkans and Central Mediterranean, are the four main illegal immigration routes into the EU.

The Western Balkans became the most active migratory route in June with 2 050 detections of illegal border crossings, 70 per cent more than in May and nearly three-times the figure from a year ago. This increase is mainly due to higher numbers of people who had originally landed in Greece and the easing of COVID measures by the national authorities in the region. The total for the first half of this year was 9 300, 73 per cent more than in the same period in 2019. Two of every three migrants detected in the region so far this year were Syrian, while Afghans accounted for 17 per cent of the border crossings.

In the Eastern Mediterranean, 200 illegal crossings were reported in June, the lowest recorded on this route since 2009. In the first six months of 2020, the total number of detections fell by nearly half to 11 900. Nationals of Afghanistan and Syria accounted for the largest number of detected migrants.

Although in June the number of migrants using the Central Mediterranean route fell by nearly 50 per cent to around 900, in the first half of this year, the total for the region was close to 7 200, double that from the same period of 2019. This is mainly due to the higher numbers from early 2020 compared to very low figures in 2019. Tunisians and Bangladeshis made up the largest portion of the detections in this area.

There were around 750 detections of illegal border crossings in the Western Mediterranean in June, 8 per cent more than in the previous month. The total for the first six months of 2020 halved to 4 500, with Algerians beeing one out of every two arrivals, followed by Moroccans.

FRAUDULENT DOCUMENT USE

In its Risk Analysis for 2020, Frontex wrote that in 2019, there were over 7 000 attempts to use fraudulent documents at the EU's external borders (entry/exit/transit), 5 per cent fewer than in 2018. Of this total number, some 5 700 detections were made on entry to the EU/Schengen area from third countries, 13 per cent less than in 2018. The most significant decrease was reported by Poland and Hungary and the 40 per cent decrease reported by Spain. The latter related to migrants from Morocco, while the former mostly to Ukrainian nationals arriving on fraudulent travel documents from Ukraine.

As in previous years, most fraudulent documents - seven out of ten - were detected on air routes. The number of document fraud cases from Morocco's Casablanca airport increased by 114 per cent in 2019 compared to 2018, making it top departure airport for detections of fraudulent documents from third countries. Many of the false document holders headed to Italy. The majority of them came from sub-Saharan countries, e.g. Ghana, Mali, Nigeria, the Democratic Republic of Congo, Senegal and Guinea. The second highest number of false documents were found in 2019 at the new international "Yeni Havalimani" airport in Istanbul. An increase in detection of fraudulent documents was also found on flights arriving from Brazil, Tunisia and the Emirates. In many cases, users of false documents pretended to use EU and Schengen countries only as a transition point on the way to another destination outside Europe. Instead they applied for asylum at the transit airport.

As in 2018, in 2019 the border between Hungary and Serbia saw the most cases of document fraud, mainly involving nationals from the Western Balkan region. The number of Kosovar fraudulent document users doubled and the largest increase was in the use of fraudulent Turkish, Serbian and Romanian documents, but reported detections at Eastern land borders with Russia and Belarus decreased.

INTRA EU/SCHENGEN MOVEMENTS

While detections of fraudulent documents on entry from third countries decreased, those on secondary movements inside the EU/Schengen area increased for the third year in a row, by 33 per cent to its highest level ever. Ireland became the most popular route for irregular migrants using fraudulent documents and several Greek airports saw an increase in the number of attempts to travel within the EU/Schengen area using fraudulent documents. Many Italian airports also found similar increases. Italian documents continue to be the favourites used by fraudulent document users on secondary movements. ■

Proving "I exist"

The Coronavirus pandemic exposed the need for functioning ID documents exactly at the moment when efforts to close the gap in ID registrations, especially in the developing world, were halted. They will start again, hopefully soon, and with greater vigor and perhaps with slightly altered aims.

There are 1.1 billion people without an official identity. About 50 per cent of them live in Sub-Saharan Africa and 47 per cent are below the national ID age of their country, which means they have no birth certificate.

Many are refugees or belong to ethnic minorities who struggle to achieve recognition by a federal government. Without an identity, access to vital services such as healthcare, social protection, education and banking can be out of reach. They have no way of proving "I exist." Poverty is another characteristic that accompanies ID-less status in Sub-Saharan Africa and the proportion of women among this group is also disproportionally high. These are not only sad statistics, they are a call to do something to alleviate the problems and fortunately, there are people and organisations that try to do just that. Some organisations aim for digital only identities, which for many underdeveloped countries seems a little reckless.

IDENTIFICATION FOR DEVELOPMENT

The World Bank Group has been running an initiative called ID4D or Identity for Development that aims to provide these 1.1 billion people with a functioning identity. A subset of the initiative is ID4Africa, which is aimed at Sub-Saharan Africa but also includes North African states.

ID4D developed a set of guidelines and suggestions to help countries start or advance their work towards giving all of their citizens an identity. The first is to eliminate barriers: Identity should be delinked from other rights or entitlements and distances should be reduced by using mobile registration, an important point in thinly populated large countries. Additional requirements for women should be removed, e.g. the need to provide a marriage certificate and all-female registration points should be available, especially in very traditional countries. The process should be as simple as possible, and a minimum of data should be collected, e.g. only 4 to 5 data fields. Documentation requirements need to be flexible and there should be alternative pathways for those without documentation. And lastly, there should be positive incentives for registration, even including cash transfers and the first ID registration and issuance should be free.

Inclusivity is a problem in some countries, especially for minority groups. Coverage and accessibility from birth to death need to be universal and no group, religion or ethnicity should be excluded. Barriers to access and usage and disparities in the availability of information and technology need to be removed.

The design of new identity programmes should be robust, secure, responsive and sustainable. This needs platforms that are interoperable and responsive to the needs of the various users, employing open standards and ensuring vendor and technology neutrality while protecting user privacy and control through system design. And considering the economies of many of the states that need to build such systems, financial and operational sustainability without compromising accessibility should be guaranteed.

To build trust in such projects, a comprehensive legal and regulatory framework needs to be in place to protect privacy and rights. There need to be clear institutional mandates and accountability, independent oversight and adjudication of grievances.

Before even embarking on a comprehensive ID project, an initial review of legal frameworks needs to be done to identify risks, gaps and weaknesses, and assess whether the legal and regulatory framework requires incremental improvements, substantial reforms or needs to be built from scratch

So much for the roadmap. There are quite a number of countries in Africa, Asia and the Americas that have started to implement "identity-for-all" programmes in its various steps, but on the whole, the Coronavirus pandemic has put a stop to efforts on the ground, such as enrolment and registration drives.

THE VIEW OF ID4AFRICA

One particular platform in the ID4D community, ID4Africa, has been forced by the pandemic to use the webinar format and blog posts to continue discussing its aims and practices instead of AGMs. In a blog post, Dr Joseph Atick, Executive Chairman

of ID4Africa writes that COVID has totally disrupted birth and death registrations due to closure of civil registration bureaus and the confinement measures. The disruption of such fundamental function could have been less dramatic, had governments put in place digital declaration and registration protocols which use mobile platforms for civil registration functions. Unfortunately, no country in Africa has done so. Dr Atick emphasizes digital identity throughout, which for national registers is certaily corrrect, but in the context of the developing world, ID without a physical document seems impossible.

Dr Atick points out that the pandemic has also uncovered the fault line between those with and without access to the digital world. Those who have access to digital tools and were able to shelter in place are not suffering that much during this pandemic. But those who lacked access—the poor or those without adequate infrastructure, digital credentials, etc., or simply little to no opportunities because of the nature of how they earn a living - have suffered and will continue to suffer significantly. Governments need to help those who are on the other side of the digital divide (the digitally poor), along with the economically poor and vulnerable.

Dr Atick does not fear a great negative impact on funding, which will remain strong because of of the increased demand that Covid has generated for digital identity, although there will be revisions in roadmaps for identity projects in order to respond faster to shifting priorities, such as public health, social safety nets and digital service delivery.

The scale of the challenge is making it clear that governments cannot meet it alone. They need to mobilize the private sector within Public Private Partnership frameworks, and they need to work together with the global community. Covid is a global pandemic and requires internationally coordinated response.

NOT PERFECT BUT USABLE

The situation has also opened the doors to the acceptance of alternative types of identity systems, which are fast and easy to use, even if they do not meet the same level of trust as that for government ID systems. It is clear what the world needs now is not legal identity by 2030, but a useful and safe identity-for-all, NOW. There are many possible identities that could compliment and even coexist with official national identity systems, such as community identity, self-sovereign identity, commercial identity schemes and social media identity. While before, governments were suspicious of non-official identity schemes, the need for immediate identification means and platforms is leading to fundamental changes in their view of the potential of non-official identity schemes to improve the identification ecosystems in their country.

Covid has made the enrollment process, which was already challenged, significantly more difficult, and this may persist even post Covid. The situation calls for alternative ways for enroling and screening. Self-enrollment is one method, where applicants can use an official mobile app to capture biographic data, scan supporting documents and include biometric data in the form of a selfie image and a photo of their fingerprints. The data would be encrypted and sent to the national authority's central database, where it would be remotely vetted and, if all is well, a unique digital identity number would be issued almost in real time. This number could be kept valid for a limited period of time, during which the applicant is expected to present him or herself in person to an authorized enrollment center, in order to validate their enrollment.

The digital identity number could be used to demand services from other agencies, or banks and insurance companies, or to conduct limited value transactions. The challenge with this type of unattended process is the vetting and screening of individuals to make sure that no robots, synthetic or stolen identities are allowed to penetrate the national identity registers. The use of social media footprints and video interviews with the applicants could help combat identity fraud and maintain the needed trust in the identity systems.

This is a paradigm shift for identity authorities, who are used to classic in-person models, where applicants are interviewed and vetted by a trained agent and only then issued an identity which can include physical and dematerialized credentials. In addition, no best practices, within the government, as opposed to commercial sector, exist that identity authorities can follow for a totally digital and risk-free enroment process. ID4Africa expects this to be a hot area for innovation, and many of the development agencies are looking to motivate the industry to advance in this regard.

The need for digital enrolment is not just a matter of convenience, it is an urgent necessity in order to avoid exclusion in digital service delivery. Countries have to identify their populations and their needs so they can deliver aid to them in a timely manner. The fact that a digital identity could be obtained in a very short time, almost real-time, adds an important value as it allows quick access to the world of benefits that digital identity is designed to unlock. But if access is limited to those who do not need it, this would be a recipe for failure from the start - that is why emphasis on inclusion should remain high on the development agenda. ■

THE RESILIENCE OF CASH

When the Covid-19 pandemic struck in Europe, many banknote printers, both public and private, rightly saw the safety of their employees as the priority. But once that was secured, thoughts about the future of the market and the place of companies within it, soon came to the fore. Infosecura talked to Bernd Kümmerle, Member of the Management Board of G+D Currency Technology, about how cash will ride out the current situation.

The covid-19 pandemic has accelerated digitalization across all societal domains, including payment. Many non-cash payment providers used covid-19 and the momentum toward digital it generated to campaign against cash with the aim to push their own non-cash products, even though scientific evidence clearly proved that cash was safe to use.

Cash demand has spiked during the crisis. End of March, the European Central Bank saw a "huge increase in cash demand" and "the largest weekly jump of cash in circulation since October 2008". Other countries and regions, as for example Mexico, reported a similar development: between December 31, 2019 and April 30, 2020 "the amount of banknotes and coins in circulation increased 5 per cent, representing the first increase since 1989." Generally, as the Financial Times in an article in July suggested, people seemed to find "comfort in the security of cash during the crisis." While people turned to cash as a store of value, the anti-cash campaigns had an impact in that cash usage took a hit in some countries during the pandemic.

Bernd Kümmerle, Member of the Management Board of G+D Currency Technology

At the same time, the virus and the ensuing discussions about hygiene and digital payments pushed Central Bank Digital Currency, CBDC. While many factors contributed to central banks contemplating the issuance of a CBDC, among them private ventures such as Bitcoin or Facebook's Libra, covid-19 certainly accelerated research and pilot projects. In April this year for example, China announced its Blockchain Service Network to be followed by the E-Yuan, a CBDC. Sweden has been pioneering an E-Krona for a couple of years and is now in the process of evaluating the corresponding technology for the roll-out. And last year, the ECB established a task force to look into CBDC.

In light of these developments, Infosecura asked Bernd Kümmerle, Member of the Management Board of G+D Currency Technology, a private provider of end-to-end solutions for the currency cycle, how G+D Currency Technology has been coping with the crisis and what the future holds.

Infosecura: Mr. Kümmerle, if one were to believe the pundits, the demise of cash has been imminent for at least 40 years. Now, with covid-19 still in full swing, cash usage has indeed declined in some parts of the world and CBDC is a hot topic. Is this the end of cash as we know it?

BK: *laughs*, I would say the opposite is true. Cash has developed quite a momentum, not only during the crisis but also now, in its aftermath. I think it is the unique characteristics of cash – tangibility, familiarity, security, resilience, universal availability – that makes people turn to cash in times of uncertainty. It is the most trusted form of payment and will be for a long time to come. Cash in circulation is growing at ~3 per cent per year, and over 80 per cent of all transaction worldwide are made in cash. Central banks have been reporting increasing demand across the globe, and all print works, whether private or state-owned, have been rather busy. That said, it is true that in some parts of the world people use cash increasingly as a store of value while cash usage has gone down during the pandemic.

Infosecura: Covid-19 then did not paralyse the industry? What did the printers do to be fully operational in the crisis?

BK: Naturally, all printers did their best to keep up with the demand. Crisis response teams established new procedures to keep the employees safe from the virus, even if that meant a loss of productivity for some time. We were able to continue operations throughout the crisis. As a partner in crisis we also supported some of the central banks that usually are supplied by their national print works. The measures to keep the virus contained are still in place, naturally, and will be for a long time to come. At our sites, for our service technicians, for everyone at G+D, a strict hygiene concept tailored to covid-19 applies, which includes a mandatory distance of 1,5 meters from each other, regular hand washing and

use of disinfectant and virtual meetings and home office where possible. All measures are being monitored and tracked. We shared our concepts with our customers, with cash center operators and with suppliers with whom we have also been in continuous communication and alignment in order to maintain an uninterrupted supply chain.

Infosecura: Even though the world demand for banknotes is relatively stable at around 160 billion banknotes per year, experts believe that the amount of cash in circulation will decrease mid- to long-term and be replaced by CBDC. One main driver will be China with its boundless appetite for the data of its citizens and its desire to make large financial transactions within its "Road and Belt" scheme easier. How can the industry react to the increasing likelihood of CBDC being issued?

BK: Behaving like rabbits caught in the headlights is not an option. CBDC will not displace cash, it will complement it. The risk of doing nothing is higher than to engage into that journey and maintain control. Central banks have been looking into CBDC much more actively since covid-19 started, and we have been offering central banks support for this transformational journey from the start. A fair, democratic, inclusive and secure government-issued payment system, currency as a public good, is an important element of the future. It is our responsibility to design it in a way that all groups in a society feel at home in it.

Infosecura: Not every player in the industry is equipped to participate in this development. Do you expect a market consolidation once CBDCs have become the norm?

BK: This was not my point at all, and nobody knows what will happen in ten years. Even though I think the industry should join the debate in order to shape it we strongly believe that cash will continue to be an integral part of the payment landscape now and in future. It is up to us to keep cash attractive – by making it appealing, by making it secure and by making the cash cycle ever more efficient. Intelligent automation and digital solutions in the cash cycle are great tools when it comes to optimizing the cash cycle and to making it more secure and more cost-efficient. They are also very helpful with regard to managing cash centers for example in times of covid-19. Innovation and digitalization are at the heart of our efforts to keep cash attractive.

Infosecura: Do you then think that the future of banknote printing and design lies in a boutigue approach, i.e print rather small volumes of beautiful and technically very accomplished banknotes, often from small and exotic countries?

BK: Even though we all love these notes, they cannot substitute our volume business. Commemorative notes, sample notes and small-scale showcase notes are a delightful add-on and great to show off the skills in design and technology. However, banknote printers nowadays as part of the cash cycle are under the same pressure of becoming ever more efficient, leaner and faster. We operate on tight margins in a very competitive environment.

Infosecura: What are the crucial factors to be successful as a private provider of solutions for currency, especially looking at the printing part?

BK: For me, trusting relations with our customers are one of the foundations for success. Innovation, quality of products and solutions, and reliability also play a part. In printing, we have to find a balance between efficiency, functionality, attractiveness and cost. We have been optimizing our processes where possible, also through digitalization, and increased our flexibility in order to be able to react faster to customer demands. Operational excellence is our motto. It is in our power to keep cash attractive, through design, security, cost-efficiency and innovative solutions for the currency cycle. Cash is the benchmark for all other forms of payment, and at G+D we passionately believe in cash.■

MEGA COUNTERFEIT BANKNOTE BUST

Law enforcement authorities from Italy, Belgium and France, supported by Europol, dismantled an organised crime network involved in euro counterfeiting.

On the action day on 15 July 2020, officers from the Italian Carabinieri Corps and its specialised Anti-Counterfeit Currency Unit arrested 44 suspects and froze criminal assets worth €8 million in Italy.

During the overall operation in Italy, assets confiscated included 50 apartments, 8 business premises, 2 farms, 10 companies operating in various sectors, 12 vehicles, 1 luxurious boat and 22 bank accounts.

In October 2017 counterfeit €50 banknotes were seized in Benevento, Campania, Italy, which were produced with sophisticated printing methods, requiring both high-level of technical expertise and good quality of machinery and raw materials. The counterfeiters imitated all main security features of genuine euro banknotes. The criminal network is believed to have produced and distributed over the years more than three million counterfeit banknotes for a total face value of over €233 million, which represents one quarter of all counterfeit euro banknotes detected in circulation since the introduction of the euro.

This network could very well be the largest ever disrupted since the very first days of the euro currency.

The mastermind behind the criminal organisation has been involved in currency counterfeiting for more than 20 years. He had not only established the whole network in charge of the production of counterfeit euros and other currencies, but also organised their dissemination on the European market. The investigation uncovered links to the Italian criminal network, the Camorra. Other criminal affiliates sought new distribution channels in Italy and abroad.

In Naples in February 2018, preliminary investigations resulted in the seizure of almost 450 000 counterfeit €50 and €100 banknotes for a total face value of €41 million, found hidden in barrels. In July 2018, an illegal mint shop of 50-euro cent coins was also dismantled in the Italian province of Lombardy. Four suspects were arrested during these action days.

At the same time, simultaneous actions coordinated by Europol took place in France and Belgium. Europol supported the operation by facilitating the exchange of information, providing analytical support and coordinating harmonised law enforcement actions in different Member States. During the raid, Europol deployed an expert to Italy to cross-check operational information against Europol's databases in real time and provide specialised knowledge in euro counterfeiting on-the-spot. ■

De La Rue: which way to go?

De La Rue, probably the world's best known banknote and passport printer, has been facing a tough two years, since the contract for the new «old blue» UK passport was awarded to Gemalto, instead of to the local champion. The company is certainly trying to regain its old glory, but there are hard choices ahead.

Much reported in the British press as yet another landmark in a time that is full of them, it was like many such current ones a sad one: De La Rue will stop production at its Gateshead factory that has made the UK's passports for the past decade, with work on post-Brexit documents fully passed to Franco-Dutch company Gemalto from June. The 189-year-old company said it would also stop printing banknotes at the factory, with 250-260 job losses expected as a result. It will retain about 100 staff that work in its authentication division and IT on the site, the Financial Times reported.

The loss of the passport order came after England and Wales, although not Scotland and Northern Ireland, had voted in a referendum to exit the European Union. It was an unexpected loss, as the contract to print the new "old Blue" passport was almost certain to go the local champion rather than to a 'foreign' bidder. Producing this 'national icon' anywhere else than in Britain would have been an affront to the newly awakened patriotism of the Brexit Nation. But affront or not, the printing order did go to a foreign company, Gemalto, a French/Dutch one and it was announced just when many experts in the field of ID documents and banknotes had assembled in Dublin for Intergraf's Security Printers Conference 2018.

A CHAIN OF DIVESTMENTS

Now, two years later, it looked as if this loss had triggered a chain of other decisions that ultimately led to the exit of CEO Martin Sutherland and the appointment of Clive Vacher, brought in last year to head De La Rue's turnaround amid warnings by the company that its future as a going concern might

be in doubt given high debt and falling profits.

De La Rue, once a large conglomerate and a leading company in banknote printing and security paper making, got into trouble first in 2010, when due to faults in banknote paper production for India, the company was blacklisted by the Indian government for all currency related contracts. This ended a very profitable relationship with India, which began in 1876 and saw support by De La Rue for the construction of India's banknote paper mill in Hoshangabad, Madhya Pradesh. Eight years after the Indian debacle, DLR left the security and banknote paper business entirely by selling is paper mills in Overton and Bathford to a new company, called 'Portals De La Rue' owned by Epiris. DLR retained a 10 per cent stake in the business.

In 2016, the company sold its Cash Processing Solutions business to CPS Topco Limited, a company owned by Privet Capital, because it was felt that cash processing was not part of its core business.

A further calamity befell the company in 2019 after it had printed another issue of Venezuela's Bolivares Soberanos banknotes. After US sanctions against the country were stepped up this year as the Trump administration sought to drive president Nicolás Maduro's government from office, US banks could no longer handle cash from Venezuela. This left De La Rue with an outstanding £18m bill for notes already delivered and no way to collect, although DLR's chief financial officer insisted the Central Bank of Venezuela "really does want to pay that debt".

After failing to win the contract to print the post-Brexit "blue UK Passorts" DLR sold its International Identity Solutions business for £42m in order to "strengthen its balance sheet and focus on other strategic growth areas such as Product Authentication & Traceability and Security Features". This leaves the company with little to cushion it from the volatilities of the banknote printing market. Although the £ 42m did indeed strengthen its balance sheet a little, it does not make up for the loss of a deal that had contributed £400m in revenues to De La Rue over a decade or the £260m it did not get by the passport contract going to Gemalto.

HUMAN AND POLITICAL COSTS

The end of passport and banknote production at Gateshead will not only come as a shock to the workers at the Gateshead plant, 170 of whom were made redundant last year and a further 80 in June, it will also be most unwelcome to the UK Government, which had talked reassuringly about 'up-levelling' the North-East of England before the last election, which already has one of the highest unemployment rates in the country.

Unite, the union, which represents the workforce at De La Rue's Gateshead factory, urged the company to reconsider its banknote printing announcement and called on the UK government to reshore passport production. The union argued that UK passport production and banknote printing should be UK-based on grounds of jobs and national security.

Worth more than £1bn in 2012, De La Rue now has a market value of about £200m. Investors look back ruefully at 2010 when a £926m takeover bid from French rival Oberthur was rejected by the board, the *Financial Times* wrote.

De La Rue, disclosed in August that it would raise £100m through a share placing to help complete the crucial turnaround strategy. The company said money raised would also allow it to invest in its authentication and security features divisions. It regards these as crucial for its future amid rising demand from governments and companies to track and verify goods and services, and prevent counterfeiting and fraud.

Since then, De La Rue has done much to get back on its feet. The company said it had already taken actions expected to result in £24.8m of annualised savings, out of the total £35.9m targeted under a three-year plan. The company stated that "in Currency, De La Rue continues to experience strong demand and has been awarded contracts representing approximately 100 per cent of its available full-year banknote printing capacity for Financial Year 2020/21, an increase on the 80 per cent of capacity announced on 1 June 2020."

But for its location in the north of England, now Gateshead's fame will have to rest a little more in a gigantic work of art, a sculpture by the British artist Antony Gormley. It is called 'the Angel of the North' and its defiant air of optimism is something that will be much needed in England's Northeast.■

WILL CORONAVIRUS MEAN THE DEMISE OF BANKNOTES?

In an opinion piece in the UK paper The Guardian, Sir Howard Davies, the first chairman of the UK's Financial Services Authority and now chairman of Royal Bank of Scotland, recalled that four years ago, Kenneth Rogoff, a former chief economist of the International Monetary Fund, made a powerful case for phasing out paper money. The following is an edited version of Sir Howard's post.

In his book The Curse of Cash, Rogoff argued that much paper money, especially high-denomination banknotes, facilitated tax evasion and fuelled the drug trade. Although that claim seems debatable, his other claim, that cash makes it harder for central banks to implement negative interest rates when investors have the alternative of keeping a safe full of cash seems obvious. That seemed an abstruse point to some at the time, but the Covid-19 crisis has placed negative rates firmly on the policy agenda in several countries, albeit not yet in the US. Since Rogoff wrote, cash has been in retreat as a payment mechanism. In Sweden, for example, the demise of the paper Krona seems within sight. The mobile payment system Swish dominates the small-denomination landscape.

And the Covid-19 crisis has given people another reason to steer away from banknotes. It was widely reported that the virus could be transmitted through handling them, prompting many outlets to put up "no cash" signs. In fact, there is little or no validity in that scare story. The World Health Organization has said there is no evidence that currency notes transmit coronavirus. The virus lasts just as long on plastic cards. But the damage was done, and in the first month of the crisis cash usage in the UK fell by more than 60 per cent. Transaction volumes halved. In a survey, nearly 75 per cent of respondents said they expected to use cash less in the future.

That trend, which has been replicated across the developed world, has given a further boost to digital banking and non-bank payment system providers. Apple Pay and PayPal are doing well. Digital-only challenger banks have continued to expand their user base, though many question whether they have yet found a sustainable business model. Facebook's Libra currency is waiting in the wings, with its backers trying to persuade regulators that its model is safe and compliant with anti-money laundering protocols.

The further decline of cash has also given greater impetus to central banks' own work on digital currencies. Through banknotes, citizens and businesses have for centuries been able to hold a direct claim on the central bank. If cash were to disappear, is there not an argument for a central bank digital currency, whether wholesale, retail, or both? The Bank for International Settlements reports that several central banks are actively considering introducing one, though none has yet taken the plunge. The Swedish Riksbank may well be the first, with an e-krona ready to roll.

So, is a farewell to cash at hand? Will even the greenback go the way of all flesh?

The answer is not so clear. In the first place, while the number of transactions fulfilled through cash transfers has indeed been falling, even at the bottom end of the range, the volume of cash in circulation has in fact continued to rise in many countries. Since the end of last year, according to the BIS, the value of currency in circulation has increased by 8 per cent in Italy and 7 per cent in the US. Precautionary holdings of cash have risen. It is not only drug dealers and tax evaders who see the attraction of cash as a store of value and who value privacy. Of the largest economies, only China has begun to see an absolute decline in the ratio of physical currency to GDP.

There are also signs of a political backlash against the withdrawal of cash handling facilities. The Bank of Canada has asked retailers to continue to accept cash, citing concerns about financial exclusion, as people without access to bank accounts and cards find themselves unable to shop. New York City, San Francisco and the state of New Jersey have barred retailers from refusing cash. Even in Sweden, the Swishers are not having it all their way. An activist group called Kontantupproret (Cash Rebellion) is now campaigning to sustain poorer consumers' ability to use paper money. In the UK, the government has published an "access to cash" review, which recommends the mandatory maintenance of a large national fleet of ATMs, even though use is falling fast.

In sum, it may be too soon to write the banknote's obituary. Demand for its services remains strong. It may make sense for central banks to offer digital services to "non-banks", perhaps partly to avoid the loss of lending income, which would enrich Facebook, rather than governments, in a Libra-dominated world. But unless central banks wish also to enter the credit allocation business, they will want to avoid large-scale disintermediation of the banking system.

I suspect that, for the foreseeable future, we will live in a kind of mixed-economy payment system. Cash will continue to play a role, albeit a more modest one than in the past, alongside a variety of cards and direct digital transfers. ■

CHINESE CITY GIVES AWAY 10M YUAN IN LOTTERY OF NEW DIGITAL CURRENCY

Authorities in the Chinese city of Shenzhen, on the border to Hong Kong, have begun giving away more than 10m yuan ($1.49m) in a citizens' lottery, as part of trials of a new digital currency, the South China Morning Post and several European papers wrote on October 9..

The idea was to test the technology and boost consumption in the face of the Covid 19 pandemic. Almost 2 million people applied to be one of 50,000 randomly selected citizens receiving a "red packet" valued at 200 yuan (about US$30) on Sunday, to spend at 3389 designated outlets in the district of Luohu. This means that only 2.61 per cent of applicants were successful. It is the latest in a series of trials to test and promote the new digital yuan, officially known as the Digital Currency Electronic Payment (DCEP). Participants must download the official digital Renminbi app, which is not yet publicly available, to receive the currency for purchases. In April, several cities, including Shenzhen, reportedly began a trial adoption of digital currencies into the local monetary system, including paying the salaries of public servants.

The currency is backed by China's state-run People's Bank of China, and is part of the government's push for a cashless society, with digital currencies more easily monitored than paper money or cryptocurrencies. Digital payments in China are already a widespread and increasingly essential part of the consumer economy, mostly through apps run by tech firms TenCent and AliPay.■

A COUNTERFEIT BANKNOTE CAN BE RECOGNISED IN A SECOND

Recent research by De Nederlandse Bank, (DNB) the Dutch central bank, showed that people can easily distinguish between genuine and counterfeit banknotes even within the space of a single second. If they take more time, the results are even better and the combination of looking and feeling works best. The report states that Dutch people do not commonly check euro banknotes for authenticity, because the chance of running into a counterfeit is small and because they trust the banknotes issued from ATMs or received as change in shops. However, in some situations they do tend to check their banknotes more closely. For example, if they have previously been the victim of money counterfeiting, if they buy something directly from another person, or if the banknote has a strange feel to it.

In order to find out how well people could distinguish between genuine and counterfeit banknotes, which senses played a role in this process and how much time was needed for proper authentication, the DNB conducted two field experiments to find the answers to these questions.

In the first experiment, participants were asked to recognise counterfeit notes in circulation by looking only at pictures of banknotes on a computer screen. After each picture, the participants had to indicate whether the banknote was genuine or counterfeit. In the second experiment, people were asked to say whether a banknote was genuine or counterfeit by either feeling it while being blindfolded, or by feeling it and looking at it as in normal circumstances. Both experiments were conducted with a short assessment period (1 second) and a longer assessment period (up to 10 seconds). For comparison, experts were asked to do the same. The analyses used a measure of sensitivity, which takes into account both the correct classification of counterfeit notes and the incorrect classification of genuine notes.

When the participants could only watch the notes on a screen, the average assessment scores were insufficient but still better than simply guessing, even with a viewing time of only 0.5 seconds. A longer viewing time had no impact on the outcome, however.

When the participants could only feel the notes, the assessment scores were also insufficient. This contradicts the often expressed opinion that you can always feel that a banknote is counterfeit. As in the case of just looking, the result is still better than guessing. In this case, a longer feeling time does result in better scores, however.

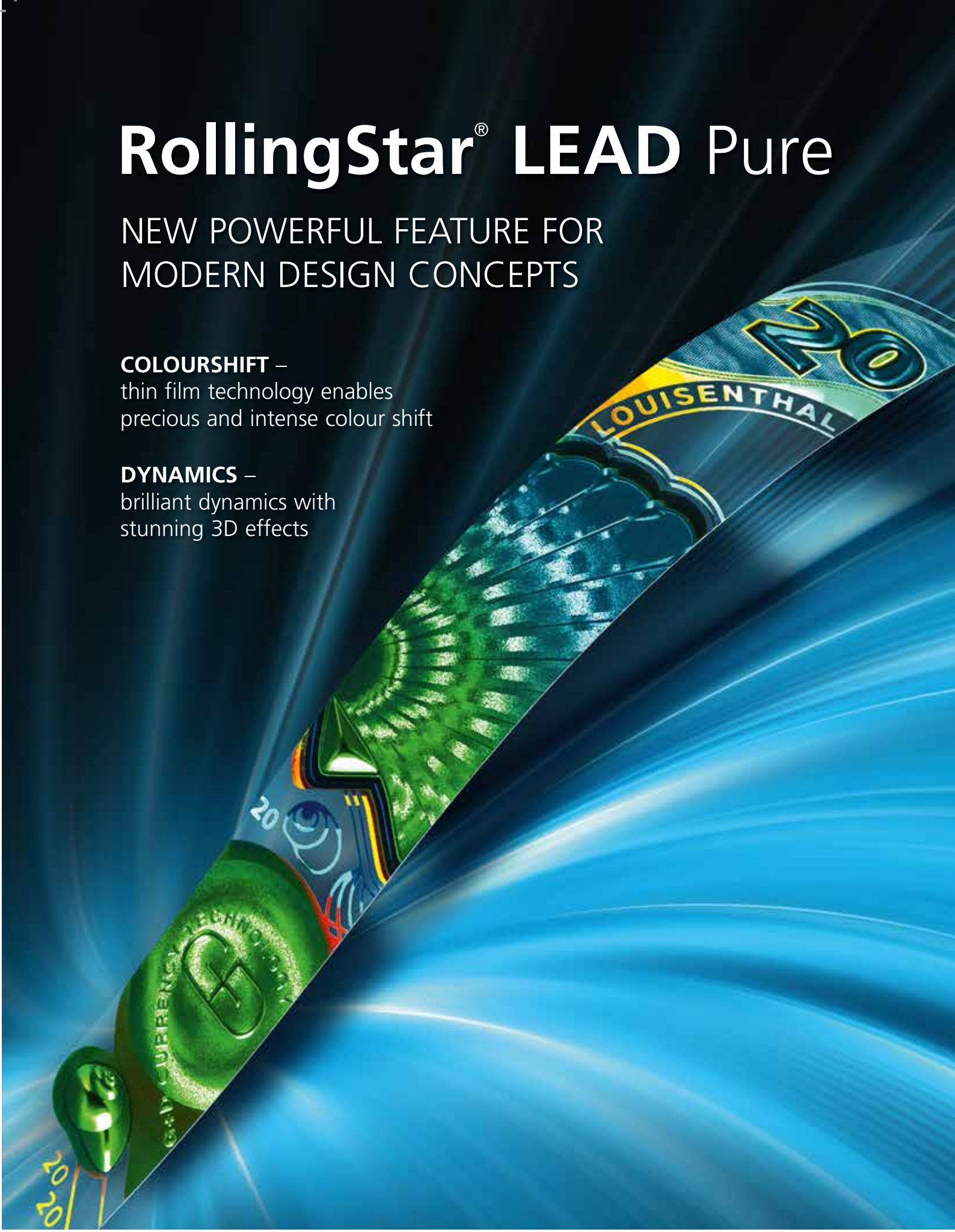
On the basis of both experiments, the researchers concluded that people are surprisingly good at distinguishing genuine and counterfeit banknotes by looking and feeling at the same time, even with an assessment time of just 1 second. Assessment scores increase with a longer assessment time. Although the chance of receiving a counterfeit banknote is only small, the results of this study show that checking your banknotes can be effective and literally takes just a second. It is a sensible thing to do, given the fact that the share of "low-quality" counterfeits has increased in the past six months. ■

RollingStar® LEAD Pure

NEW POWERFUL FEATURE FOR MODERN DESIGN CONCEPTS

COLOURSHIFT –
thin film technology enables
precious and intense colour shift

DYNAMICS –
brilliant dynamics with
stunning 3D effects



Louisenthal