

YEAR 22 MARCH 2019 ISSUE 79

INFOSECURA

23-25/10/2019

SecurityPrinters Banknotes+Identity

DENMARK
COPEN
HAGEN

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.

INTERGRAF

www.securityprinters.org
www.intergraf.eu

Contents

3

UK access to cash review

5

Easy money - fast regrets

6

Banknotes: not just for paying bills

8

ISO 22382 Tax Stamps

10

PWPW: looking ahead and looking back

12

ID cards: to know who is there

14

Big data and its problems

15

A lifeline in a crisis

17

Your face is your passport

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. All rights reserved. No part of the publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or use in any information storage or retrieval system without the express prior consent of the publisher. 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

IT'S ALL IN THE MIND - OR IN THE FACE



About half of this issue of Infosecura is about cash. In the last year or two, central banks across Europe have been worrying about cash. Sweden and Finland, where cash seems to be on the 'endangered species' list, are seriously considering what can be done if it becomes too expensive to provide cash for everyone who needs it, which means also in locations far from bank branches or ATMs.

As we reported in Infosecura 75 and 78, Finland looked at the possibility of Central Bank Digital Currency (CBDC) as did Sweden's Riksbank. In Britain, as the website "Quartz" noted in February, cash usage is shrinking faster than in most places, and the debate about what to do about it is getting louder. That is important because, like just about every country where digital payments are taking over, the UK doesn't have much of a plan for what happens next. The disappearance of cash seems like a preordained destiny. Why?

Lahcen Hadouni, formerly of the Central Bank of Morocco, in a re-share on LinkedIn, made an important point: According to philosopher Louis Althusser's concept of interpellation, one can get people to internalise beliefs by addressing them as if they already had those beliefs. "Twenty years ago nobody believed that cash was "inconvenient", but every time I walk into the London Underground now I see adverts that address me as if I was a person who finds cash inconvenient. The objective is to reverse-engineer a belief within me that it is inconvenient, and that cashlessness is in my interests. But a cashless society is not in my or your interest. It is in the interest of banks and payments companies. Their job is to make you believe that it is in your interest too, and they are succeeding in doing that," Mr Hadouni writes.

The idea that cash is inconvenient is also forcefully rejected in a recent study by the German Bundesbank, that finds that cash is still "the fastest and most cost-effective means of payment". According to the study, paying by cash takes just over 22 seconds and costs around 24 cents per transaction, while payments by card needing PIN entries take around 29 seconds.

In the section of Infosecura about ID issues, we talk about the missed opportunity of the UK to manage intra-EU migration by issuing ID cards. Migration has been among the main issues driving the "leave" (the EU) vote in the UK referendum, and by the time of writing we still don't know which way the UK will turn, no deal, the Prime Minister's deal or a new referendum. It is, however, peculiar to note that the UK has one of the densest networks of CCTV cameras in Europe, but its citizens are not required to carry any ID documents. Using ID technology would at least have given citizens a sense that migration is under control. Any attempts in the UK to use advanced technology, such as facial recognition in real life situations seem to have flopped. That would never happen in China, which seems to be well on the way to a total surveillance society, as our article on facial recognition explains. But on second thoughts, perhaps, on this subject, a flop is preferable to total success.

The Editor

THE UK'S ACCESS TO CASH REVIEW

In most highly developed countries, the majority of technical and societal forces are moving consumers away from cash. Barring catastrophic events, electronic payments in different forms are here to stay but a move to electronic payments only, would be very detrimental to a large number of people, especially the old and the poor. The aim of central banks and all companies involved in the production of cash and in the cash cycle must be to continue to make cash available to all who need it and not to let usage fall below a point where it would be uneconomical to produce and use cash. A preliminary report from the UK looks at the realities on the ground. The full report is to come out in spring and will attempt to offer a set of concrete actions. (Access_to_Cash_Interim_Report(1).pdf)

In the last couple of years central banks have become interested in how, and to what extent the currency they issue is used. In September last year (in issue 77) Infosecura wrote about the Bank of England's call for evidence on the use of cash and electronic means of payment, in the same issue we reported on the survey of the Swiss National Bank on the use of cash and in issue 75, in March 2018 the large study by the European Central Bank on the use of Euros and a smaller study by the US Federal Reserve on the use of US Dollars were reported. Now it is again the turn of Great Britain to publish a study, but this time not one initiated by the Bank of England but by LINK, the UK's largest ATM network and it is not their final report, but only an interim one. The final report is due in the spring of 2019 but even the preliminary results are very interesting. The full report will explore the end-to-end cash cycle and will propose a concrete set of actions for policy makers, regulators and commercial entities.

THE ANSWER IS NO

Entitled "Access to Cash Review", this first report asks the question 'is Britain ready to go cashless?' and it also delivers the answer; a firm 'no'.

Cash is still an economic necessity for around 25 million people in the UK (out of a total of 65.5 million). There is, however, no doubt that there is a strong shift away from cash. In the last ten years cash payments have dropped from 63 per cent of all payments to 34 per cent. Similarly, the number of cash withdrawals from ATMs is 8 per cent lower now than a year ago, and the rate of decline has increased from 5 per cent at the beginning of 2018. This is a worrying trend. A straight-line trajectory of current trends would see an end to cash use in the UK by 2026. However, the report's authors believe that cash will still be here in 15 years' time, but potentially accounting for as few as one in every ten transactions. This assumes that technology continues to develop at its current rate or faster, that most people who are able to use digital technology increasingly do so, but that we hit a 'floor'

because digital payment methods still won't meet everyone's needs.

The key driver behind the move away from cash has been the growth in debit card payments, now the UK's most frequent payment method. A total of 98 per cent of adults have a debit card, and they're using them more and more. There were 13.2 billion debit card payments in 2017, up 14 per cent from 2016. Contactless payments also surged, growing by 99 per cent in 2017 to 4.3 billion. By the end of 2017, nearly 119 million contactless cards had been issued.

CASH IS STILL IMPORTANT

However, there were still 13 billion cash payments in 2017, making up over a third of all payments, and cash stayed (and is forecast to remain) the second most common payment method. Cash is also still hugely important as a store of value both in the UK and overseas. The total value of notes in circulation has also increased in recent years, with over 3.6 billion Bank of England notes (worth £69 billion) currently in use.

Public concerns on a cashless society

Percentage of UK population who believe that a cashless society would mean:

- 74%** that we would be more vulnerable to cyber attacks
- 60%** that we would all have less privacy
- 74%** that it would take away people's right to choose
- 75%** that some older people would find it difficult to do everyday things like paying bills
- 72%** that vulnerable groups of people would be more likely to get scammed or defrauded
- 67%** that people on low income might struggle to balance their household budget
- 63%** that people might lose the sense of the value of money i.e. holding a large amount of cash in your hands makes you think more about how you spend it.

Around 2.2 million people are using cash for all their day-to-day transactions. For this group, lower income is a common factor. Over 15 per cent of people with an income under £10,000 a year rely completely on cash, compared to less than 2.5 per cent of all higher income groups. There are also significant generational and regional differences. Some variation is likely to be due to lack of mobile and broadband connectivity outside of cities, which inhibits digital transactions. Despite these variations, most of the UK sees significant benefits in digital payment methods. At the same time, many have a strong preference for continued access to cash, because it gives them

choice (34 per cent of the population), privacy (6 per cent) or simply peace of mind (55 per cent), as we know that cash will always 'work'. But for 47 per cent – or 25 million people – cash is not a choice, but a necessity.

ACCEPTING NEW FORM OF PAYMENT

When it comes to the latest forms of digital payments, contactless, there are again great generational and regional differences. While 63 per cent of all adults in the UK made a contactless payment in 2017, those between 25 and 34 were most likely to use contactless, while those over 65 or older were least likely to. There are also some very clear differences in contactless use between the regions: London has the highest use, with almost three quarters of people using contactless, while the North West has the lowest at 52 per cent.

The differences also persist in people's perception of when and if cashless will happen. 41 per cent believe it will happen in their lifetime. But others struggle to see how they could function without cash. Research by UK Finance, the industry trade body for financial services, shows that those who are most reliant on cash are the poor.

As already stated, only a small proportion of the UK population use cash for all their day-to-day payments – just 2.2 million people. There are also 1.3 m people who don't have access to bank accounts. Most of the UK population use digital payments for some things, like Direct Debits for household bills, while using cash in other aspects of their lives. Contrary to common perception, the elderly are not the most reliant on cash. Research for the report showed a wide range of needs for cash. Some of these are likely to reduce over time (37 per cent need cash because local shops or services don't yet take digital). But other needs will need thoughtful and tailored solutions, including physical or mental health issues which make it hard to use digital services (2 per cent), the risk of overspending and going into debt (9 per cent), and those who rely on others to buy things for them (4 per cent).

For these groups, cash offers a degree of control which digital doesn't yet achieve. There are technological developments in small segments of the market, which could address some of these needs, but the vulnerable are rarely early adopters, and technology is often designed for the mass market rather than for the poor, rural or vulnerable. It's clear from the research that, if the technological revolution continues apace, millions are likely to be left behind.

The debate about cash access and use in the UK often focuses on consumers and – even more narrowly – on ATMs. But the death knell for cash

could also come from shops insisting on digital payment rather than from a loss of ATMs. With bank branch closures and rising costs of depositing cash, it could become more and more expensive for retailers to handle cash.

The report looks at the potential consequences of an unplanned rush to a cashless society. These risks include:

- Loss of independence for many, particularly the old and disabled.
- Exploitation and abuse for the vulnerable, as digital can lead to a loss of control.
- The loss of viability of rural communities as shop costs rise and the local cash economy collapses.
- An even higher burden being placed on the poor through the 'poverty premium', where people end up paying more if they can't shop around, buy online or buy in bulk. As cash use is reduced, this premium could increase as people lose access to the high street, and debt could increase as they lose cash as a mechanism for controlling their budgets. This is not an acceptable outcome for Britain, and it's not what the majority of people in the UK want, the report states. To address these risks, it is necessary to keep a reliable and effective cash infrastructure in place for those who need and choose to use cash, while developing digital solutions that work for everyone. ■

Why do some people need cash?

The reasons why 17% of the UK population are unsure of how they would cope, or would not cope at all in a cashless society, are varied.

- 2%** care for an elderly or disabled relative who mainly buy things using cash
- 4%** get paid in cash
- 37%** need cash for when cards aren't accepted at the point of purchase
- 18%** believe that it is good to have some cash in case the IT systems go down
- 7%** can't get a debit card
- 4%** can't get a credit card
- 6%** don't always have access to good broadband or mobile reception, so cash is sometimes the only way to pay
- 23%** stated that a lot of local businesses still only accept cash
- 6%** are involved with a community group (e.g. church, sport club), which only uses cash
- 2%** have physical or mental health issues that can make it hard or unsafe to use digital payments
- 7%** can't afford to go into debt so they use cash for budgeting
- 9%** worry that they will overspend, or let their spending get out of control if they use digital payments so try to stick with cash

EASY MONEY, FAST REGRETS

Borrowing money is one of the important mechanisms of the economy, whether for companies or individuals. However, one of the common results of financial inclusion and thus access to credit, especially in developing countries and among the poor, is overborrowing, which can lead back to financial exclusion.

One of the undoubted characteristics of cash is that it is very easy to keep track of. If the cash in one's wallet or that hidden under the mattress is spent, there will be a wait until the next payday or a potentially difficult visit to the next lender, whoever that may be. That is a good or a bad thing, depending on individual circumstances, self-discipline or moral outlook. It is however not an immediate problem for anyone with a credit card or access to "mobile money".

Financial inclusion is a subject often talked about and mobile money, which offers the equivalent of a basic bank account to everyone with some kind of mobile telephone, can be seen as a quick way to increase financial inclusion. In some countries, e.g. in India, mobile money may prevent having to go to a "money lender", who usually charges exorbitant interest, which in rural areas often leads to debt-bondage. But there are also less positive sides to mobile money. Recent evidence shows that digital credit through mobile phones may also lead to over-borrowing and hence to similar problems to those caused by avaricious moneylenders.

One of the regions in which mobile money was taken up on a large scale is east Africa. The Economist writes that "thanks to M-PESA, its largest mobile-money service, with over 20 million users, Kenya has been a pioneer in both mobile money and mobile financial services, such as lending. Anecdotal evidence is mounting of abuses—most notoriously of young Kenyans borrowing to splurge on online betting sites. The number of Kenyans blacklisted by the country's credit bureaux, and so unable to borrow, has risen to more than 500,000, up from 150,000 three years ago. The proliferation of mobile credit, offered by over 50 competing lenders, is blamed for the increase. The loans are mostly a few dollars and the maturities a matter of days or weeks. But the damage could be lasting."

In one of the first large scale survey which included more than 3,000 Kenyans and 4,500 Tanzanians, the Consultative Group to Assist the Poor (CGAP), a consortium of donors affiliated to the World Bank revealed that more than a third of mobile phone

owners in Kenya and a fifth in Tanzania have used digital credit. These digital borrowers tend to be young, urban men. And they borrow actively—more than half of digital borrowers in each country had a digital loan outstanding at the time of the survey.

Digital loans are primarily used for household purposes, followed by business purposes and, in Tanzania, airtime purchases. They are only rarely used for medical needs or emergencies. The surveys indicated some reasons for concern. About half of digital borrowers in each country reported having repaid a loan late at some point. In Tanzania, 31 per cent reported having defaulted, as did 12 per cent in Kenya. Twenty per cent of digital borrowers in Kenya and 9 per cent in Tanzania reported reducing food purchases to repay a loan. And a significant minority in each market reported poor transparency—such as not understanding the loan costs or terms—which correlates with higher levels of late repayment and default.

A second report, one in a series that started in 2008, by the Centre for the Study of Financial Innovation (CSFI), a London-based think-tank, asked micro-lenders around the world about their main worries. For the first time the most often cited risk was "technology". CSFI took this to mean that technology "is facilitating growth but making excessive risk-taking more likely, particularly by encouraging people to over-borrow."

Many micro-lenders claim a social mission to alleviate poverty. However, their policy is often carried out by commercial lenders. Making it easy to borrow is certainly attractive to poor people, and not only to them, especially if there is no paperwork and no collateral involved. But the annualised interest rate on many microloans in Kenya is several hundred per cent, suggesting that lenders are, in effect, pricing in high rates of default. The danger is that the problems seen in east Africa may appear also in other markets, where mobile money has not yet made such inroads. Before that happens, better regulation should be introduced, or in countries where the problem has not yet arisen, 'mobile money' and micro loans should be regulated for the first time.

As a second measure, The Economist recommends better credit assessment. By analysing payments and other data on a client's phone, algorithms can be used to lend to borrowers to whom banks would never lend. As data pile up, micro-lenders' judgments should improve. Undoubtedly, mobile money is one way to financial inclusion for the poor but it should also be recognized that ease of access and accompanying lack of discipline, or sudden overwhelming need, can just as well lead to the opposite - financial exclusion. ■

BANKNOTES, NOT JUST FOR PAYING BILLS

The International Bank Note Society Journal regularly publishes new banknote issues from countries the world over. The images of banknotes show, how countries are portraying themselves to their own citizens and to the world.

A banknote is a means of exchange, a unit of account and a store of value, economists will say, but that definition leaves out a large area that has little to do with economics. The look and the feel of a banknote is also of great importance. Many countries also use their banknotes to reinforce patriotism and to teach their citizens and any foreigner handling their money, a bit of history. Take for example the new 500 Apsar note of Abkhazia. It shows the portrait of the former president, Vladislav Ardzinba, who led Abkhazia

in the war against Georgia 25 years ago, and in the background there is a picture of soldiers raising the flag of Abkhazia, a close copy of the raising the US flag in Iwo Jima in WW2 or of the raising of the Soviet flag on the Reichstag in Berlin in 1945. On the reverse side the note shows the map of Abkhazia, a small triangle of land on the Black Sea just south of the Caucasus

mountains, that was part of Georgia and who's independence has only been recognized by five countries. For the rest of the international community Abkhazia is still a part of Georgia.

For many countries, banknote are an effective, long-term medium to get a political point across without any additional cost. A good example for this is Argentina's 50 Peso note issued in 2015, which evokes the 1982 Falklands war with a map of the Islas Malvinas (or Falklands Islands), and the cruiser Belgrano, sunk by the British navy in 1982. It also shows the Argentinian Darwin war cemetery among some other images. The notes of the fourth series, which started in 2016, are more

discreet. The only possibly political image there is a map of Argentina showing the claimed Malvinas and the large triangle of territory, Argentina claims in the Antarctic.

As far as convincing the world, or the local citizens, of the country's modernity is a political act, the 200 Manat note of Azerbaijan is being political by showing the spectacularly modernist architecture of the Heydar Aliyev Center in Baku. It is all very



aspirational. The extravagant architectural image is tied to the name of the last secretary of Soviet Azerbaijan and first president of the post-soviet state, Heydar Aliyev, who also was the father of the current president. The map of the country on the back is accompanied by a small European map to tie the country to Europe rather than to the Middle-East, although, as a transcontinental country, it is part of Europe as well as Asia.

The teaching of history and promotion of patriotism finds perfect expression in the 2018 commemorative issue of Poland's 20 Złoty note, which celebrates the re-founding of Poland after WW1. On the front it shows a portrait of a pensive Marshal Józef Piłsudski, first head of state and head of the military and the dates 1918 and 2018. The back of the note



displays next to the Polish coat of arms, an unusually large Polish flag.



The majority of new issue notes pictured in the last number of the International Bank Note Society Journal (IBNSJ), serve up the usual and safe portraits of past or present presidents or kings and past heroes. South Africa gives Nelson Mandela pride of place front and back, with a portrait of the statesman at the front and a picture of the young Mandela linked to various locations, in different stages of his life on the back.



Thailand shows even more reverence to rulers, past and present. Every note of the new issue, 20, 50, 100, 500 and 1000 Baht, shows a portrait of the young king, who ascended to the throne in 2016. On the back are the portraits of two (different) kings that preceded the current ruler in a kind of dynastic procession. The throne is seen in Thailand as the cement that keeps the country with many ethnicities and languages together.



A country where one would expect strong political expressions on banknotes, is remarkably restraint. Venezuela, that finds itself currently in great economic and political difficulties, in 2018 issued a complete series of Bolívares soberanos, which replaced the previous Bolívares fuerte due to hyperinflation. The notes of the new Bolívares soberanos series as well as the preceding Bolívares fuertes notes give no hint of the political turmoil of the years they were issued. They are very



handsome and dignified notes, which on the front side show a portrait of a historic political personality in a striking upright format and on the back, in landscape format, a typical animal of this tropical country in front of a dramatic landscape. The imagery has largely been taken from the original 2008 Bolívares fuertes series, but portraits now appear on different denominations to the originals and with different colours. The three series



of the last ten years were obvious attempts to escape hyper-inflation. They did not succeed. The IBNSJ quotes the value of the 2 Bs. note as € 0.03 and the highest denomination the Bs. 500 as €6.92.

If a country chooses to depict an abstract idea on its banknotes, patriotism for example, the visual equivalent is often quite simple. To express more profound ideas about the essence of a country is more complicated. One of the most ambitious attempts to do this is the current series of Swiss francs, in which six notes - all but the Sfr. 100 note already in circulation - express key motifs: time/organisational talent, light/creativity, wind/wealth of experience, water/humanitarian tradition, matter/scientific experience and finally language/communication, via an action, a Swiss location and various graphic elements. No wonder it took eleven years (from design competition to issue of first note) to develop the series and a very large educational effort to explain to the Swiss and to the world, what was behind the images and symbols they saw on the banknotes. ■

ISO 22382 TAX STAMPS: WHAT DOES IT MEAN FOR SECURITY PRINTERS?

by Ian Lancaster



A sample modern tax stamp, made on a tamper-evident frangible material with a DOVID, serial number in alphanumeric and data matrix formats and printed graphics including security elements.

(Photo courtesy of Leonhard Kurz)

In November 2018 the International Organization for Standards (ISO) published ISO 22382:2018, titled Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the content, security, issuance and examination of excise tax stamps.

I had the privilege to be the Project Leader for this new security document standard, which was created under the auspices of Working Group 4 (Authenticity, integrity and trust for products and documents) of ISO Technical Committee 292, Security and Resilience, with support from the International Tax Stamps Association (ITSA).

This is a guidance standard, intended to guide and advise tax authorities and their

procurement agencies on the processes they should go through to achieve best practice in the tax stamps they issue.

Many readers of InfoSecura from organisations that are certified under ISO 14298, are familiar with ISO compliance standards, which require an inspection before a certificate can be issued to show that the certified organisation complies with a particular standard. This can be an expensive process which is nonetheless commercially worthwhile, so it's not appropriate to issue a compliance standard for government agencies. This means it's not possible to know how many organisations have adopted and follow a guidance standard, but ISO 22382 has already been welcomed by tax authorities which have become aware of it, as they lack any other source of independent, objective help in working through the maze of procedures that precede actually issuing tax stamps.

SMALL BUT NUMEROUS

Before explaining what's in the Standard, it's important to understand its context. Tax stamps are the most numerous secured document produced; there are at least 200 billion produced every year - so they may be small but there are a lot of them! And the number continues to increase, driven by three key factors:

1. their use is spreading from the historically core application of taxable alcohol and tobacco products to many other consumer items, including soft drinks and books;
2. more countries and states are adopting tax stamps as they learn how effective they are at reducing tax losses;

3. international agreements or regulations are coming into force which require traceability of tobacco products, (particularly the EU Tobacco Products Directive and the WHO's Protocol to Eliminate Illicit Trade in Tobacco Products), which can be achieved through the use of tax stamps, so they become a cost-effective dual function item.

One reason for developing this new standard is that the quality and security of these stamps varies enormously. Some are no more than monochrome print on standard paper, while the best are produced on frangible substrates, have origination artwork created using security print software and carry additional authentication features such as diffractive optically variable devices (DOVIDs). Additionally, the procurement process in some jurisdictions doesn't meet acceptable standards. Hence the requirement for an international standard to help more tax authorities achieve best practice.

WHAT IS THE BENEFIT?

So what's the benefit of this new standard for security printers and others involved in the production of tax stamps?

The Standard does not set rules or prescribes how to design, produce and issue tax stamps, but guides tax authorities through their decision processes as they consider issuing tax stamps for the first time or upgrading stamps they already issue. It covers the functions, design, construction, security features, serialization and examination of tax stamps, but the procurement process section has particular relevance to producers. This explains how an authority should go about specifying and then issuing a request for proposal (RFP) for new tax stamps. It lays out the expectations that the process should be transparent and fair, with both the authority and bidders understanding who is involved in the supply chain where - as there often will be - there is more than one organisation involved. It recommends that the first step is the publication of a request for information (RFI), so that the authority can get an idea of which parties might be interested in submitting a proposal and what their capabilities are. The Standard then guides the authorities through drawing up a specification to publish in the RFP, but also encourages them to publish their tax stamp objectives and allow proposers to submit their own specification as to how they would achieve these objectives. Thus the Standard encourages authorities to have an open mind on what might be proposed to best meet their published criteria.

In other words, ISO 22382 sets out how a tax authority should run a fair and open tendering process that gives all interested and capable

parties the opportunity to bid, avoiding the possibility of preferred suppliers – informally or otherwise. Note, though, that the Standard also explains why suppliers should be specialists in security procedures, recommending that bidders are either certified security printers (certified under ISO 14298, for example) or are otherwise known to follow security procedures (perhaps because they are a state-owned printer of the country's banknotes).

POST PRODUCTION CONSIDERATIONS

While the Standard guides, advises and recommends on the procedures a tax authority should follow, it tries to ensure that these procedures include a full and proper consideration of the risks and threats there will be to the stamps once they are in circulation and how these should be countered in the design and construction of the stamps. So one of the longest sections is titled Tax stamp construction, covering size and design, authentication features, tamper evidence, substrates, printing, inks, coatings and adhesives. This section also covers security aspects of direct-marked stamps, i.e. those that are printed directly on to the product or its packaging. While this is not immediately relevant to security printers it is important to know what the competition might be for substrate-based tax stamps as produced by a security printer.

SERIALISATION AND EXAMINATION

There are two other important sections in the Standard that are relevant to security printers, which are the sections titled Serialization and unique identifiers and Examination of tax stamps.

Serialisation of tax stamps is, of course, a critical part of fulfilling their function as a tax collection vehicle, but as product traceability becomes a more important factor for consumer goods markets (see my reference above to the TPD and WHO Protocol), then this component of a tax stamp may take on additional functions which impose their own security needs, not to mention secure infrastructure system requirements for storing, scanning and checking the unique identifier (UID). This section therefore sets out the security requirements and the different formats for the printing of the UID on the stamp.

Examination of tax stamps once issued and applied to taxable product is a critical aspect of keeping them secure. This seems to be something that tax authorities too often overlook in the design of their stamps, which is one reason why this is included in the title of ISO 22382. The section on examination, which complements the sub-section on authentication features, guides tax authorities through the levels of examination and the means of examination. The Standard explains that authentication is

achieved through the examination of the security features using appropriate tools by appropriate examiners. The process of choosing authentication features is therefore not only a matter of design but functionality, having regard to the competence and motivation of those examiners.

These sections, which necessarily only give an overview of the procedures to be followed, are supported by appendices which give more detail and descriptions of design and construction, substrates, authentication features, printing and authentication tools. It is ISO practice that appendices fill out the guidance in a standard but do not form part of the standard, so these are included as information for tax authorities.

To recap, the underlying rationale for this tax stamp standard is to improve the quality and effectiveness of tax stamps while making the procurement process transparent and fair, which should benefit security printers, component and system suppliers involved in the production and supply of tax stamps. As mentioned above, this Standard has already been welcomed by tax authorities as it provides them with objective and independent guidance and information.

I recommend organisations active in the tax stamp supply chain to purchase and become familiar with ISO 22382 (it can be downloaded as a pdf file from the ISO online store and should also be available from your national standards body). You will then recognise the approach being taken by tax authorities seeking to source tax stamps, you will share and understand the terms that they use, and thus be better prepared to submit a proposal that meets or exceeds the tax authority's specification. ■

NEWS

The EU Tobacco Products Directive (TPD) requires the 28 EU member states to implement national traceability and security feature systems by 20 May. The UK has appointed De La Rue as the issuer of the unique identifier (UID) required for track and trace. France was one of the first to publish its five selected security features. However, since then, it has apparently not moved on much further. Bulgaria, Czech Republic, Germany, Italy, Lithuania, Poland, Portugal, Romania and Spain have appointed either their state printing works or national tax revenue authorities as UID issuers, and some of these have in turn sub-contracted this job to private IT companies such as Atos. Belgium, Croatia, Luxembourg, Malta and the Netherlands have contracted directly with private companies, including INCERT, AKD, OpSec Security and Atos.



The Polish Security Printing Works (PWPW) in Warsaw is celebrating a double milestone in its history. There is - as an important part of the national history - the 100th anniversary of the company, which was celebrated in January 2019. The second milestone is an equally important marker of success, the completed certification of all three of its production units.

Although it may often feel like that, not everything in and about Poland is linked to history. Sometimes it is also about modernity, efficiency and competing successfully with the rest of the developed world.

In the security sector, both ID and Banknotes, as a sign of being on an equal footing with the best of their competitors, Polska Wytwórnia Papierów Wartościowych or PWPW, the Polish Security Printing Works, announced that the third, and last, of its production sites in Warsaw had been awarded Intergraf's ISO 14298 certificate after completing the thorough audit and the necessary changes demanded to gain the certificate.

The headquarters of PWPW with central Warsaw as a backdrop



The newly certified sites are the company headquarters in Sanguski Street and the site in Niepodległości Street. In the former, PWPW produces security paper, banknotes, visa stamps, postage stamps, excise stamps and other security printing. The range of products for both the domestic market and for export is constantly

growing. Production technology, machines and processes are getting more and more sophisticated. But certifying the headquarter site was a serious challenge. The external elevations (external walls, fences, windows etc.) of the building are classified as a historic monument and any alteration needed to be co-ordinated with and agreed by the Mazovian Heritage Conservator (Mazowiecki Konserwator Zabytków). The internal construction of the building is also very complex and the architects who designed it all those years ago definitely did not have ICR requirements in mind. Many complicated investment and organizational changes were needed to adjust the building and its use to create proper security areas. It required hard work and investments as well as raising the building awareness of employees to achieve this undoubted success.

The other site that was certified, the Niepodległości Street site, is relatively „new” in the history of the company. It became PWPW property in 2004 when the company acquired Drukarnia Skarbowa, the printing works of the State Treasury. At the time of the acquisition, the building was not a production site, but after making some business decisions, PWPW placed several production lines there and today communication documents (i.e. driving licenses, registration cards for vehicles etc.) are produced in Niepodległości Street. The building itself was a little easier to adapt to ISO 14298 and ICR requirements, but still much investment and training of staff was needed to fully comply with the certification requirements.

THE STORY OF CERTIFICATION

The story of certification at PWPW in general began in 1999 when the company received its first certificate for ISO 9001. Over the years the company's Integrated Management System was enlarged with new standards: ISO 14001, OHSAS 18001 and ISO 27001. In 2005 PWPW decided to add production security to its IMS, because security itself is and always has been the core of its business.

The first Intergraf certification standard gained was CWA 14641. After the CWA standard was transformed into ISO 14298:2013, the Management Board decided to start with certifying only one site, the one on Karczunkowska street, since the rest of the sites were not ready to meet such strict requirements. The next step was to certify the paper mill in accordance with CWA 15374 in 2017. Finally, after another two years of work, PWPW was completely ready to certify the whole company.

The reason to “rebuild” PWPW and create an organization, that functions in accordance with the highest standards worldwide was, among others,

the need to develop the organization and project a new image of PWPW in the security printing sector and towards its customers. The recognition among its customers that awareness of quality and the importance of security are paramount has shown the company that it has to stay on this track if it wants to be present on the market as a competitive and trustworthy producer.

Implementation of ISO 14298:2013 in Sanguski Street and Niepodległości Street sites started in 2016 after the positive decision of the Management Board. The next step was to invite the external auditor to perform a pre-audit and assess the preparedness of the PWPW sites. The auditor delivered numerous observations and remarks which the company decided to follow as instructions on how to implement the standard properly. After almost three years the company was ready and the certification audit passed completely satisfactorily.

The auditor was impressed by the amount of work the company put into this process, by the changes that had been made and also by how seriously PWPW took the ICR requirements and his observations from the pre-audit. During the closing meeting the auditor expressed his appreciation of PWPW's approach to security and to the ISO standard itself. This certification was a necessary step in PWPW's improvement process.

PWPW stated that as a national producer of banknotes, ID documents, passports and other security products for the Republic of Poland it was necessary for the company to keep the security and confidence of its customers and Polish citizens on the highest level. It is not only a question of business, first of all it is a question of national security. ISO 14298 and ICR requirements were the best guidelines that helped PWPW to organize its security system.

PWPW's main building has a special place in the wartime history of Warsaw and Poland. A poster exhibition on the perimeter fence tells the story.



AND NOW TO HISTORY

The history of the company dates back to January 1919 when the Council of Ministers, chaired by the Prime Minister and famous pianist Ignacy Jan

Paderewski, decided to establish the State Graphic Works. This was just one year after Poland had re-emerged as a country (in November 1918) after over a century of partitions by Austro-Hungary, Russia and Prussia/Germany and only five months after its independence was confirmed at the Treaty of Versailles in June 1919. In the twenties, the State Graphic Works were transformed into a joint-stock company operating under the name Polska Wytwórnia Papierów Wartościowych (Polish Security Printing Works). Building the new headquarters was begun in 1926 and finished in 1929.



For the 100th anniversary of the Polish Security Printing Works, Poczta Polska (the Polish Post) issued a special postage stamp showing Ignacy Jan Paderewski, which is both a promotional bank note and a traditional postage stamp.

THE WAR YEARS

During the Second World War, instead of surrendering, the government set-up a "Polish Government in Exile" in London, while at home, the underground "Home Army (AK)" and the underground Polish state tried as much as possible to continue a civilized administration under German occupation, including printing clandestine banknotes. During the "Warsaw Uprising" PWPW's headquarters was the site of one of the fiercest battles. PWPW employees captured the building from the Germans and defended it for nearly one month. On 27 August 1944, 1600 German soldiers, supported by artillery, attacked the building in Sanguski Street, which was defended at that time by as few as 200 AK insurgents. After a pitched battle for every floor, the insurgents left the building one day later. During 27 days of fighting, almost 100 AK insurgents were killed in the building.

The building itself was left in ruins. After the war, during the reconstruction between 1946 and 1950 banknote production had to be moved to Łódź before it returned to Warsaw.

Between then and now, many important things happened. The brave fight of Solidarnosc, the fall of communism and the re-establishment of a free, western oriented Polish Republic, among them.

Today, PWPW is not only concerned with security printing but also with security digital products. ■

TO KNOW WHO IS THERE

Migration and immigration are among the most contentious political subjects in Europe and America, as they touch personal and national identity and the rights and needs of fellow human beings, often in distress. As the example of the UK shows, they can also lead to great national upheavals. In the Brexit context, a report in the UK suggests that migration could have been managed better, even within existing EU rules.

At the time of writing it is still impossible to say whether Great Britain will exit the European Union or not, and if so under which conditions or under no conditions at all. Much has been written about the reasons for the results of the 2016 referendum on EU membership, which led to 52 per cent of voters wanting to leave the EU and 48 per cent wanting to remain. However, most commentators agree that immigration - or migration - was an important trigger and it also became one of the seemingly immovable 'red lines' the UK government laid down in the negotiations with the EU.

It should be noted that the UK had been very generous with access to its labour market after eight former communist countries joined the EU in 2004. It was one of only three countries, along with Ireland and Sweden, to place no restrictions on workers from the new entrants, which led to the arrival of an estimated 600 000 workers from Central Europe in two years. Most of the other EU countries placed restrictions on labour movement, which was legal according to EU law for up to seven years after a country joined. Romania and Bulgaria, which joined in 2007, generally faced restrictions until 2014.

AN UNNECESSARY DIVORCE

A recent report by the independent think tank 'Global Future', backed by Lord Andrew Adonis, member of the UK's Upper House, argues that instead of allowing uncontrolled access to the UK labour market for Central Europeans, the government had the possibility to manage inter-EU migration all along, by using existing EU rules and thus probably avoiding the hugely disruptive UK-EU divorce. In the report, Lord Adonis suggests that the UK needs, urgently, an advanced Electronic ID Cards scheme, as is commonplace in Europe, so that "we know who is here, what entitlements they have and crucially what entitlements they don't have. This would enable us to monitor who is working, so that like other European countries, we can ask EU citizens who have been here for 3

months without finding work, to leave."

EU migrants are estimated to bring a £4 billion dividend in annual benefits to the UK. They contributed a net £2 300 (€ 2 500) per head more to the UK's public finances in 2016/17 than the average adult UK citizen, and make a net lifetime contribution to the UK's public finances of £78 000 (€86 500) per person. However, those benefits are too often not seen in the communities most impacted by migration. At least half of that dividend should be used to invest in a new Strengthening Communities Fund – investing £2 billion in the public services and infrastructure that has suffered because of new demand, Andrew Adonis recommends. This would give communities a better, fairer share of the benefits created by the migration that they absorb.

Finally, he said, the UK should follow Switzerland in delivering both proper enforcement of the Minimum Wage – to prevent unregulated migration forcing wages down illegally – and in obliging employers within occupations or areas where unemployment is above average to give local residents priority before recruiting from overseas. This would help the country to show voters that migration for economic reasons is a skills safety valve, rather than the preference of lazy or prejudiced employers who don't want to train British people.

THE EU HAS TIGHTENED FREE MOVEMENT

In recent years EU Member States have recognised the need to tighten free movement rules to prevent exploitation, especially with regards to labour and social security. Among these are Reforms to the Posting of Workers Directive which seek to prevent undercutting of wages of national workers by those posted by another Member State with lower rates of pay or working conditions, and the Introduction of the Labour Mobility Package (including the establishment of a European Labour Authority and a European Social Security Number), which aims to strengthen enforcement to prevent cross-border labour market abuses. EU countries also initiated stronger action on external borders and non-EU migration through establishment of processing centres, greater funds for FRONTEX and border countries, and accelerated return of irregular migrants. Additionally control of secondary movement through the Schengen Area is also planned. The European Court of Justice also confirmed the right of Member States to restrict 'welfare tourism' and to enforce permanent residence conditions.

A BRITISH E-ID CARD

Great Britain is the only country in the EU without an ID card system. The central recommendation of the report is to introduce a compulsory electronic ID card to provide compulsory registration for anyone

staying more than 90 days, giving government up to date information on who is living and working in the UK. A valid e-ID card should be a requirement to live, work and access public services and benefits. As the card would provide the necessary data, the government could release extra funding for public services in areas experiencing surges in migration.

According to the report, an e-ID card could also answer the key demands of those preferring to leave the EU, namely monitoring and security, pressure on public services and the benefit system, fairness in the labour market and integration. In particular, the e-ID card would control access to the world of work (replacing the NI number requirement), housing (through tenancy agreements), the benefits system and non-emergency public services through a digital verification system, and in doing so would apply the same standards to everybody regardless of race or background.

The e-ID card would provide the first ever database of who is living and working in the UK, ensuring that each citizen is fairly accounted for in the funding of public services. This would allow resources to be quickly, and correctly allocated to areas facing rising migration.

The card would contain minimal information, owned by each citizen, anonymised and protected from abuse, with citizens' rights clearly established and amendable only following full and open debate in parliament. The card would be digital first, and would build on existing infrastructure to keep costs low.

WHAT ABOUT THE NEIGHBOURS?

In the debate about migration, it is instructive to compare the UK to the other big country in the European Union, Germany. According to the Pew Research Centre, in 2017 there were 4 920 000 people born in the UK living outside the country, while the foreign-born population was 8 840 000. The total population of the UK is about 65 million. In Germany, 4 210 000 German born people lived outside their country, while the foreign born population was 12 170 000. The total population of Germany is 81.5 million.

In December last year, both the United Kingdom and Germany announced a radical overhaul of their immigration rules. Britain billed its stricter regime as "a route to strengthened border security and an end to free movement", while Germany said it was easing immigration rules to attract more foreign job-seekers, 'The Guardian' wrote. The British home secretary, Sajid Javid, said that the Conservatives' 2017 election manifesto had made clear the party's "commitment to bring net

migration down", while his German counterpart Horst Seehofer, said: "We need manpower from third countries to safeguard our prosperity and fill our job vacancies."

STAY OUT

Britain's priority appears primarily to be establishing a system of tough controls capable of keeping certain people out. The new system will require skilled workers to earn a minimum salary, to be decided next year, which is obviously designed to keep low paid workers out and to avoid wages being undercut by migrant labour.

Business leaders have warned that the system will leave the UK poorer, depriving industry of a migrant workforce on which it has depended. The proposed £30,000 salary threshold for skilled workers would leave hospitals, the construction and hospitality sectors, manufacturing, agriculture and logistics desperately short of labour, they said.

The UK's system does not put a cap on numbers but aims to reduce annual net migration to "sustainable levels". After Brexit there would be no more special treatment for EU citizens; a transitional temporary worker scheme would allow them, and workers of any skill level from other "low risk" countries, to enter Britain without a job offer for up to 12 months.

COME IN

Germany's *Fachkräftezuwanderungsgesetz*, or skilled labour immigration law, will make it easier for employers to recruit from outside the European Union, amid clear evidence that there are not enough German and EU workers to fill demand. About 1.2 million jobs remain empty in Germany, according to the Federal Labour Office, from lorry drivers to carpenters and care workers. Under the new law, skilled workers from outside the EU will be allowed to enter the country for six months to try to find a job, provided they can support themselves financially. More controversially, the law will offer the prospect of permanent residency to asylum seekers who have a job and speak good German but currently face deportation if their asylum applications are turned down.

As in the UK, immigration has been a key political issue in Germany since Europe's 2015 migration crisis, when the country absorbed more than 1 million mostly Muslim refugees and migrants, sparking a xenophobic backlash and surge of support for the anti-immigration and populist Alternative für Deutschland (AfD) in federal and regional elections. Some in Angela Merkel's conservative alliance also said that such a move ignores public concerns about immigration. ■



The challenge of devising a biometric identification scheme for well over 1 billion people, speaking one of 22 official languages, and using almost as many writing systems, living in a federal union with 29 states and having widely different levels of education and IT skills has always been monumental. Add to this, citizens being very protective of their privacy and very skilful malicious hackers and the troubles of Aadhaar become almost inevitable.

India's Aadhaar system, launched in 2009, is the largest biometric program of its kind in the world, with 1.22 billion Indian residents enrolled - out of 1.31 billion inhabitants (in July 2018). Aadhaar's 12-digit codes are assigned by the Unique Identification Authority of India (UIDAI) and linked to data from fingerprints and iris scans as a means to confirm the identities of anyone who works or resides in the country, including non-citizens. The government's intent was to create digital identities as a way to ensure access to welfare, health, and education programmes. The country has one of the largest populations of internal migrant workers, many of whom often carry no identification, making it difficult to prove who they are when traveling state to state.

The Aadhaar system is not directly linked to a specific card format such as many European ID cards. There seem to be several formats and there is the possibility of having the card stored on a smartphone. The security is therefore not so much in the physical document as in the biometric information that is stored in a central database.

A VOLUNTARY SYSTEM

Although Aadhaar is nearly universal in India, it is a voluntary system, a fact that was confirmed in a Supreme Court of India ruling in 2013, which stated that "no person should suffer for not getting Aadhaar", adding that the government cannot deny a service to a resident who does not possess Aadhaar, as it is voluntary and not mandatory. The

court again reconfirmed the voluntary nature, and thus the right to privacy several times. Court challenges to the system or to specific aspects of it seem to be a common occurrence. Despite being challenged, the central government has pushed citizens to link their Aadhaar numbers with a host of services, including mobile sim cards, bank accounts, the Employee Provident Fund, and a large number of welfare schemes and old age pensions. Recently, the relevant Union Minister said the government will soon make it mandatory to link Aadhaar with driving licences. He justified the linkage by saying: "At present, what happens is that the guilty person who causes an accident flees the scene and gets a duplicate driving licence. This helps him go scot-free. However, with the Aadhaar linkage you can change your name but you cannot change your biometrics, neither iris nor fingerprints. So the moment you go in for a duplicate licence, the system will say this person already has a driving licence and should not be given a new one." There is little doubt that this decision will again be challenged in court.

TOO EASY TO HACK?

The Indian press reported late last year that the Aadhaar system has been widely criticized for its lack of regulatory framework and there have been several large-scale security breaches. In November, the news website HuffPost India revealed the existence of a malicious patch said to disable critical security features, making it easier not only to create unauthorized Aadhaar numbers but to fool the system's biometric recognition systems from virtually anywhere in the world. The purpose of the patch, which is reportedly in widespread use and easily obtained on WhatsApp for roughly Rs 2,500 (around \$35), is not to grant access to information in the database; rather, it allows unauthorized users to introduce information to it—i.e., create identities, potentially with fraudulent biometric data.

However, UIDAI dismissed the accusation and called the report "incorrect and irresponsible". In a 24-tweet thread, it said: "it is not possible to introduce ghost entries into the Aadhaar database." If an operator's or resident's biometrics were not captured or were blurred and sent to the system, "the same is identified by the robust backend system of UIDAI, and all such enrolment packets get rejected and no Aadhaar is generated. No operator can make or update Aadhaar unless the resident himself give his biometrics." It also insisted that the operator's biometrics had to be authenticated before enrolments or updates were processed. In spite of criticism, the system has some impressive backers, such as World Bank Chief Economist Paul Romer, who described Aadhaar as "the most sophisticated ID programme in the world". ■



A lifeline in a crisis

Issuing secure temporary documents to desperate people in appalling circumstances is something normal passport offices or consulates will likely never encounter. But for organisations such as the International Committee of the Red Cross it is part of their daily work and whatever the conditions, the temporary documents they issue still have to be correct, reliable and secure. The ICRC Emergency Travel Document is designed to help in a crisis. It may in the future even become a crisis-fit-document, a concept that defines the technical and organisational steps required to make documents survive a crisis in full functionality.

(Images: ICRC, secoia.ltd)

WHAT IS THE ICRC EMERGENCY TRAVEL DOCUMENT?

The International Committee of the Red Cross (ICRC) at the last ICAO TRIP Convention in Montreal introduced its new Emergency Travel Document (ETD), which on January 1st 2019 replaced the 2015 version of the document, in order to follow the ICAO guidance on ETDs more closely.

The ICRC ETD is issued for humanitarian purposes to people who do not have a passport or other recognized travel document and find themselves unable to return to their country of origin or residence, or to proceed to a country offering temporary or permanent refuge or asylum. These people could be asylum seekers, refugees, migrants in particularly vulnerable situations or displaced or stateless people. The ICRC issues these documents only as a last resort, and the holder must have the necessary visas and meet the travel requirements.

The new ETD is limited to a single journey to the holder's country of origin or habitual residence, or to a receiving country. It is valid for three months, to allow time to make the arrangements and undertake the journey. The personal information on the document is based on the applicant's own statements and any other identity evidence available. It is issued only by ICRC delegates and is free of charge. There is a photograph, a signature and two fingerprints on the documents, which link it to the bearer without necessarily guaranteeing the correctness of the name. It also contains information about the holder's travel itinerary, has a section for visas and a variety of security

features. As it is a one-way document, the bearer is expected to return it to the ICRC when the journey is completed. It is important to note that the Emergency Travel Document is not a passport or an identity card, or a means to establish or alter the status or nationality of its holder, nor is it valid for a return journey.

A GOOD DOCUMENT FOR A CRISIS

The new Emergency Travel Document was developed with the help of Swiss security consultants SECOIA. It has the format of an A4 sheet folded in the middle down to A5 and again to A6, thus creating a format and layout similar to ID-2.

The personal information, if need be, can even be handwritten with a ball-point pen. Each ETD has a unique, letterpress printed, six-digit serial number, which is tactile, front and back, and which is fluorescent green under UV light. It appears in four different places on the document. On the front and back is a line of microtext, which lists the seven 'Fundamental Principles' of the International Red Cross and Red Crescent Movement in English, French and Spanish.

In the section on personal data on the front of the sheet, the bearer's photo is printed in colour inkjet directly onto the document. In extreme cases - the ICRC said this happens in five per cent of all cases - even a normal photo can be affixed to the page. This section also contains information about the document itself (i.e. validity, date and place of issue).

Further biometric identifiers, namely the prints of the two index fingers in red, are on the top right quarter of the page, where the holder also signs the document in blue ballpoint pen. Next to this is a section on the travel itinerary, to inform border control officers. If the relevant information arrives to late for printing, it can be completed by hand. On both the front and back of the document there are sections for visas, entry, exit and/or transit. The section for validating the document with the name and signature of the ICRC representative and the ICRC embossed stamp is at the bottom of the reverse side.



Both sides of the document carry green-blue-green rainbow background printing which changes to blue-green-blue under fluorescent light. There are also UV-fluorescent, multi-coloured fibres, visible fibres and two-level watermarks. The paper itself is UV-dull.

SECURE LOGISTICS AND THE NEED FOR CRISIS-FITNESS

While the document itself is sufficiently secure, the greatest security challenge 'in the field' will be secure storage of the blank documents before completion. In its present state, the document carries almost all security features before personalisation. It is therefore of utmost importance that the document stock is protected from theft during transport and storage.

It is precisely this shortcoming that the concept of a crisis-fit document, developed by the consultancy SECOIA is designed to address. Considering that ETDs are issued in precarious and often insecure conditions, it is prudent to spread the application of security features into several different phases, both physically and by authorisation to access and use. When all these components, physical and digital, are finally present, as close to personalisation as possible, the document is crisis-fit. This means in most cases decentralised production.

SECOIA has assembled a group of highly specialized suppliers to the security printing industry to support its concept. They are united in the Consortium for Robust Official Credentials (CROC). These are European papermaker Lahnpaper, Schreiner Printrust and TraceTag as well as US-based Troy Group with select others to be joining shortly. Starting with the substrate, SECOIA

suggest the synthetic paper *neobond*. This paper consists of paper fibres and additionally a significant percentage of synthetic fibres, and in spite of it being called 'synthetic', it is made on a paper machine and can carry the usual embedded - specially formulated - security features of high-security documents. It can be printed in offset, silkscreen, letterpress and intaglio. It can be personalized by inkjet or toner laser printing. Inkjet inks with UV capabilities and inks that deeply penetrate the substrate are now available and can be used in printers that are often available even in remote locations. Apart from the typical visual data, printable data can include even machine-readable encrypted QR codes and specific patterns created by secure and encrypted algorithms. More sophisticated equipment can additionally print data, including photographs, in UV ink. It is possible to broaden the issuing infrastructure by including buffering power supplies, allowing for continued production during a power failure of several hours.

An important characteristic of a crisis-fit document is the very strong bond between the substrate, the *neobond* paper, and the print, which in a promotional video is very amusingly demonstrated by attaching the paper to the sole of a boot for a 15 km hike, (mis)treating it with a high pressure water compressor, running over it with a 26 ton caterpillar in mud and gravel, etc. Each individual component of the document and the ETD as whole survived this treatment in fully functional condition. (<https://croc.secoia.ltd> - login-required)

The issuance process and critical data are additionally protected by a security transfer seal, which itself includes numerous security features and unique identifiers. This replaces the conventional rubber-stamp or chop, adding a comprehensive audit-trail to the issuance process, as well as further security to critical data and to the document itself. Finally each component can be additionally secured and tracked by the use of the source-controlled and secure technology of TraceTag. ■

(below) Schreiner Printrust security transfer seal, including numerous security features and unique identifiers



(right) Lahnpaper's *neobond* with inkjet personalisation from Troy Group



(far right) Sophisticated equipment can print data, including photographs, in UV ink. (Images: secoia.ltd)



Your face is your passport

The use of facial recognition technology, although not quite as accurate as iris or fingerprint recognition, is growing rapidly in a multitude of environments. It has many positive applications, but we cannot afford to ignore the negative ones.

If we look at the available identification technologies - fingerprint recognition, iris recognition and facial recognition - the latter has the greatest potential for mass surveillance, in fact, among the three it is the only one which can be used for that purpose. In our industry, use of facial recognition, especially in European ABC Gates at airports, is overt and generally voluntary, as it is used to verify that the passport or ID card presented matches the face of the bearer. As long as there is the possibility to have your ID checked by a real person if you object to having your image in a government database, even a person very strict about privacy would have little to protest about. The coming Schengen Entry and Exit System (EES), will do away with that possibility, as passports will no longer be stamped but entry and exit will be recorded electronically.

In the USA, ABC gates seem to work without the need to scan a passport or an ID document with a photo, as the system compares the face in front of the camera with an encrypted image in a government database. In 2016, the US Department of State had a database of the facial images of 117 million citizens, mainly drawn from state driving licence databases and US Customs and Border Control has a record of people's faces, and often other biometrics like fingerprints, from passport and visa applications or from when visitors go through immigration entering the country. CBP shares access to that information with airlines for them to check against, the US magazine Wired said. There has been disquiet about facial recognition in several parts of the world. In the US, some companies have asked for oversight for AI application and last July, Microsoft, which both researches and commercializes AI, called for "a government initiative to regulate the proper use of facial recognition technology." As a good part of our industry is involved with identification, we should be concerned about its use as

much as about its misuse.

USING FACIAL RECOGNITION IN THE STREETS

In December last year, the Metropolitan Police in London, UK, ran a public trial of facial recognition technology, several papers reported. In Soho, Piccadilly Circus and Leicester Square, cameras scanned faces in crowds and ran them against a database of people wanted by the Metropolitan Police and the courts. Whenever an alert was made, police on the ground reviewed it and carried out further checks to confirm the individual's identity. The scanners were deployed for around eight hours per day and positioned visibly alongside a uniformed police presence. Passers-by were entitled to avoid being scanned, and all footage was deleted immediately after the trial. Faces matching the watch-list were kept for 30 days. The privacy campaign group 'Big Brother Watch' nevertheless described the use of such technology as "authoritarian, dangerous and lawless". In London there are about 500 000 CCTV cameras and in the whole of the UK, it is estimated that there are about 4 million (generally not used for facial recognition).

The Metropolitan Police said that it is committed to four more trials of facial recognition technology by the end of the year. The December trial and several trials before that date were not very satisfactory. The Met used facial recognition at the 2017 Notting Hill carnival, where the system was wrong 98 percent of the time, falsely telling officers on 102 occasions it had spotted a suspect. Police in South Wales had been given £2.1m by the Home Office to test the technology, but it got it wrong 91 percent of the time, the Guardian said last year.

South Wales Police says the government's Home Office has not set any false positive rates that should be targeted but the system does allow the "operator to vary the match threshold against a watch list as a whole". One can only hope that the next trials will have lower error rates than the last ones.

In spite of the high error rate, Met Police Commissioner Cressida Dick said that she was "completely comfortable with the trials", but nevertheless complained that "we are finding ourselves quite hamstrung by a quite complex regulatory system, a quite complex legal framework," while "bad guys" were getting up to speed with technology, she told the Telegraph. She also said (to the Guardian) that she was "very keen that the law keeps up with the technology and I don't feel that we are working in a tremendously enabling environment at the moment."

These error rates are of course never found at

airport ABC gates and the technical challenges of identifying one-to-one and one-to-many are different. Airport security via facial recognition technology is only tangentially linked to the on-going debate on privacy and surveillance by the state. However, the UK error rates point to either mistakes in the collection of images or in the databases, against which they are matched, or, quite simply, to inexperience, in which case we can expect swift improvements.

IN CHINA, THE ALL-SEEING EYE

Contrast the UK error rate with that in China, where, as Bernard Marr wrote in *Forbes* in December 2018, the error rates of the technology can be as low as 0.8 percent; eight out of 1,000 scans could be misidentified. Chinese technologists are certainly experienced. The Chinese Ministry of Public Security began to build the world's most extensive facial recognition database in 2015. For mass surveillance, facial recognition is uniquely useful. Unlike fingerprints, faceprints can be scanned at a distance. The individual faceprint is a unique code that is applicable to an individual. It is created by measuring distances between points on a face such as the width of the nose or the distance between the eyes. 80 of these so called nodal points are used to create a faceprint. Once a faceprint is made, it is run through identity databases to connect the face to a name in the database.

Going back to the facial recognition at airports scenario, Shanghai Hongqiao International Airport's Terminal One now uses facial recognition technology for their automated clearance system. In just 12 seconds, passengers can scan their ID cards and use the security-checking machines equipped with facial recognition technology to complete the security check process. This allows the terminal to clear 2,000 passengers through security in an hour. Beijing's new airport, designed to handle 100 million passengers annually, will use facial recognition technology to match passengers to their belongings as well as for security checks, *Forbes* writes.

There are many more facial recognition applications currently deployed in China including driver authentication for Didi, an Uber rival; or, famously, to prevent theft of toilet paper at Tiantan Park in Beijing; to support the registration process for universities and to notify teachers when children aren't paying attention in the classroom. Facial recognition technology can also determine what ads to serve you when you walk by.

Many of China's facial recognition systems and the databases behind them are local or regional and are used in local attempts to improve public behaviour, such as identifying jaywalkers and people who

litter, displaying their faces and names on large public image boards nearby. But it is equally clear that the central government aims or plans to cover the whole country with facial recognition surveillance. The *New York Times* (28-10-2018) writes that the two most important Chinese companies developing this technology are both start-ups, SenseTime and Megvii, whose AI-powered facial recognition systems are likely the most powerful in the world. SenseTime began as a research project at the Chinese University of Hong Kong and was established as a company in 2014 and is today the world's most valuable AI start-up with a market valuation of at least \$4.4 billion.

Sense Time's rival Megvii is 'only' valued at an estimated \$2 billion, but the company is the originator of the world's largest open-source facial recognition platform, Face++. More than 300,000 developers use Face++ to build their own face detection programs. Founded in 2011 by three graduates of Tsinghua University—China's MIT equivalent—Megvii claims it wants to "build the eyes and the brain" of Chinese cities and extend police powers to a point "beyond what is humanly possible", the NYT article continues.

With technology like this, the Chinese government has the ability not only to identify any of its 1.4 billion citizens within seconds, but even to predict their behaviour. With the world's largest detention programme for an ethnic minority, the Muslim Uighurs in the Xinjiang region in China's west, who are suspected of separatist tendencies under way, one can but wonder how facial recognition technology and AI is used there. ■

NEWS

New leadership for IHMA

The International Hologram Manufacturers Association (IHMA), which represents the global hologram industry, has appointed Opsec's Dr Paul Dunn the new chairman to lead the IHMA as it continues to promote the advantages of holographic technology, particularly for product authentication and ID documents. As chairman, Dr Dunn heads-up a board and leadership team which includes Diavys' Alessio Pastorelli, Surys' Corinne Murcia Giudicelli and Professor Seung Hyun Lee from South Korea's Hologram Forum. Brad Hilbert of Crown Roll Leaf will represent the Americas and ITW's Joanne Ogden will oversee the EU & EFTA, while Demax Holograms' Valentin Monovski will represent Eastern Europe and the FSU/CIS. Asia will be covered by Rohit Mistry from Holographic Security Marking Systems and Umendra Gupta (ASPA).

EXPERIAN: BIOMETRIC HACKING AMONG TOP CYBER THREATS FOR 2019

In its sixth annual Data Breach Industry Forecast, Experian, a consumer credit reporting company, expects that biometrics will come increasingly under attack by hackers. These criminals will try, and eventually succeed, to exploit vulnerabilities in touch ID sensors, facial recognition and pass-codes. Biometric data is considered the most secure method of authentication, but it can be stolen or altered, and sensors can be manipulated and spoofed or deteriorate with too much use, the forecast noted.

“Expect hackers to take advantage not only of the flaws found in biometric authentication hardware and devices, but also of the collection and storage of data. It is only a matter of time until a large-scale attack involves biometrics either by hacking into a biometric system to gain access or by spoofing biometric data. Healthcare, government, and financial industries are most at risk”.

The forecast said that organizations need to ensure their biometric systems are secure in all layers. Biometric data should be encrypted and stored in secure servers.

Recent academic research has found that a number of fingerprint authentication systems could effectively be spoofed by AI-generated fingerprints that emulate highly common fingerprint features. Even highly sophisticated biometric authentication systems such as Apple’s 3D facial recognition system have been shown to be vulnerable to more elaborate hacking efforts. 2019 may well be the year that will show which biometric security systems are truly effective and which are outdated

As organizations must now work within parameters dictated by the General Data Protection Regulation and other privacy regulations, turning to biometrics as part of a multi-factor or stand-alone option appears to be the best approach. In addition, an increasing number of personal devices like smartphones and tablets have biometric options. ■



MÜHLBAUER TECURITY®

COMPREHENSIVE GOVERNMENT SOLUTIONS

Security is not a product, but one of the most valuable goods of a nation. The core of a holistic ID program is the constant capability to increase and optimize the integrity of the national identification scheme. Mühlbauer is strongly committed to providing reliable and secure government solutions for your citizens, thus creating trust and absolute confidence whilst meeting all your individual requirements.

Mühlbauer – Your Reliable Partner for Your National ID Program






www.muehlbauer.de



SecurityPrinters

Banknotes+Identity

3 DAYS OF BIG IDEAS & PROVEN STRATEGIES

Bella Center Copenhagen
Center Boulevard 5
2300 Copenhagen - Denmark

70+ SPEAKERS

An independently funded, non-profit platform of learning
and sharing for banknote and ID document experts

900+ PROFESSIONALS FROM ALL FIELDS OF SECURITY PRINTING

Network and together shape the future of the industry

110+ EXHIBITORS

Be at the forefront of innovation: move security
printing forward

www.securityprinters.org