YEAR 21 MARCH 2018/ **ISSUE 75**

INFOSECURA

CYBER SECURITY CURRENCY EVERYTHING

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

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

Cyber everything

This year we can celebrate yet another anniversary: 70 years ago, the American mathematician Norbert Wiener coined the word *cybernetics*. In a book published that year, he defined cybernetics as "the scientific study of control and communication in the animal and the machine." It is a broad field and the essential goal is "to understand and define the functions and processes of systems that have goals and that participate in circular, causal chains that move from action to sensing to comparison with desired goal, and again to action". We can see how this may apply to phenomena such as cyber currencies and many other things that Wiener and his colleagues at the Massachusetts Institute of Technology probably never thought about. But even at that time, cybernetics was closely linked to computers, although a large computer at the time was the size of a small house.

Now, that computers have become immensely powerful, small and ubiquitous, not only mathematicians and technologists have to think about them, but sociologists, psychologists and criminologists as well. We are devoting the first article in this issue to an interview with a cyberpsycologist, Dr Mary Aiken, who will give the keynote presentation at the forthcoming Security Printers Conference in Dublin. Cybernetics, shortened to just cyber, has become a kind of 'catch-all' for everything that uses a computer. Even our business, the design and manufacture of banknotes and identity documents, can only be understood in connection with computers and computerized processes. Going back to the root of the word, cybernetics is a better term than the, perhaps more popular, 'digital' or 'noumerique' as the French call it. The word cybernetics comes from Greek *cyberneticé*, meaning "governance", i.e., all that are pertinent to *cybernáo*, the latter meaning "to steer, navigate or govern", hence *cybérnesis*, meaning "government", as Wikipedia, another product of cybernetics, puts it.

The connection between cyber and bitcoin, or more generally cyber-currencies, is obvious. We just don't know whether they will be a threat or an opportunity, or perhaps both. A greater challenge will probably be 'central bank digital currencies' or CBDC, which the Bank of Finland has been looking at. It may be worrying that in all these cyber or digital developments, may they be simply means of payment or fully fledged currencies, it is not the central banks that are in the driving seat but technology companies. That Finland's and other central banks are now looking at the technology and the implications for their economies and societies is an encouraging sign.

ANALOGUE IS STILL ALIVE AND KICKING

Although the title page proclaims "cyber everything", analogue is still going strong, as illustrated by an important study by the European Central Bank on the use of Euro banknotes and an equally important one by the US Federal Reserve System on how Americans spend their Dollars. Analogue is not only tactile and physically present, it is also able to stir emotions, as is shown by the brouhaha around the proposed re-appearance of the old dark blue passport of the United Kingdom and the coming exit of the burgundy-coloured one. Advocates for 'Brexit' claimed this as their first victory against the EU, only to find that the UK could have kept the "old blue" all along, as there never was a EU regulation on a uniform passport colour. Some Brexiteer faces may have turned the colour similar to that of the present UK passport.

The Editor

INTERVIEW WITH KEYNOTE SPEAKER DR MARY AIKEN

Could you define cyberpsychology in just a few words?
Cyberpsychology is the study of the impact of technology on human behaviour, it's about twenty years old as a discipline - some say that cyberpsychology is the new psychology.

Much of your research has centered on forensic aspects of cyberpsychology. Which areas are especially vulnerable to cybercrimes?
Card-not-present (CNP) fraud is dominating fraud related to non-cash payments, and this impacts the retail sector heavily. Airline ticket fraud continues to have an impact globally and is linked to other criminal activity such as human trafficking. Europol's latest Internet Organised Crime Threat Assessment report has highlighted Darknet markets as key facilitators and enablers of cybercrime, providing access to compromised financial data to commit various types of payment fraud, firearms, counterfeit documents to facilitate fraud, trafficking in human beings, and illegal immigration.

Are cybercrimes mostly affecting individuals or corporations, especially in the context of our industry: identity and finance?
Forbes recently predicted that cybercrime will cost businesses approximately $6 trillion per year on average through 2021. The cost of cybercrime to enterprise is also increasing, in 2017, Accenture reported that organisations are spending nearly 23 per cent more than the previous year, the average annualised cost of cybersecurity was $11.7 million per business.

In terms of the individual, identity theft is also soaring. An estimated 15.4 million consumers were hit with some kind of ID theft in 2016, up from 13.1 million the year before. Recent events such as the massive 2017 Equifax hack further compound the problem with data belonging to over 143 million people compromised. From a forensic risk perspective victims of the Equifax breach have a heightened risk of becoming a victim of identity theft.

What is the difference between a cybercriminal and a conventional one? Does such a criminal fit into the pattern normally associated with criminality, or is this a new type of criminal?
I am often asked to quantify traditional crime versus cybercrime – but technology is now ubiquitous; with a camera on practically every street corner, connectivity everywhere and devices in the hands of some five billion users, it would be hard to commit a crime that did not have some cyber component, we are moving towards an era where all crime could be considered as involving cybercrime. The same holds for traditional criminals, they are also increasingly engaging in cyber criminality along with a new generation who practice their criminal activities almost exclusively in cyberspace.

Here is a woman that made the fight against cybercrime the centre of her professional life.

Dr Mary Aiken is one of the foremost cyberpsychologists, who is fighting against financial and identity cyber fraud and - even more passionately - against what cyber technology and cyber criminality are doing to our children and young people. She fights by advising police organisations, such as Europol, by writing, teaching and lecturing and by using the power of Hollywood imagery . She is the inspiration behind the successful CBS series CSI: Cyber. Listen to Mary Aiken at Intergraf's Security Printers International Conference in Dublin.

What does a cybercriminal look like - what are his/her characteristics?
Malicious hacking costs companies up to $600 billion annually, a recent study published on Frontiers in Human Neuroscience now found a positive association between an individual's drive to build and understand systems - called 'systemizing' - and hacking skills and expertise, other studies have focused on human motivation to engage in criminal hacking which ranged from profit to revenge, and "just for fun" to political idealism.

What does a typical victim of cybercrime look like?
There is no such thing as a typical victim of cybercrime - in an age of ubiquitous technology we are moving towards a point where everyone is potentially what we describe in forensics as a "high-risk victim" – from the teenager in their bedroom at home to the CEO of the company.

What is the most challenging aspect of your work as a researcher in such a different environment as the web?
The most challenging aspect of my work is dealing with child vulnerability in cyber contexts – there is no shallow end of the swimming pool online for kids. We are seeing increases in anxiety, depression, low self-esteem, insomnia, eating disorders and 'sextortion' attempts associated with young people's use of the Internet – they say it takes a village to raise a child – this is also true in cyberspace.

Where did the idea of the Hollywood television show CSI: Cyber come from? Is this show inspired by your research only? Is Avery Ryan's life in the show similar to yours?
The CBS show CSI: Cyber was inspired by my work as a cyberpsychologist, in the real world I work as an academic advisor to police organisations such as Europol, in the show they made my character (played by Patricia Arquette) a police officer – apart from that, the show was pretty authentic.

What was one of the most interesting projects you worked on?
The show CSI: Cyber was a fascinating project – creating an hour of Hollywood style TV drama every week was very demanding but immensely rewarding, at one point the show aired in 170 countries worldwide, for me as an educator it was a fantastic platform to educate and inform concerning cybersecurity and safety. ■

Dublin: it's about the future

THE PANELISTS

Joy Macknight,
The Banker

Michael Lambert,
US Federal Reserve

Linus Neumann,
Chaos Computer Club

Wolfram Seidemann
G+D Currency Tech.

Martin Sutherland,
De La Rue

Leif Veggum,
Norges Bank

The programme of the forthcoming Security Printers conference in Dublin will give participants a very thorough picture of what is going on in the world of currency and ID documents, from the latest improvements in their functionality to the threat to their physical existence. Of course, currencies will never go away, even cowrie shells were currency once, and the need to identify oneself or to be identified will persist as long as people interact with each other, but the forms these functions will take have never been more in flux as today. The Dublin conference will try to answer where the neuralgic points are, that can either reaffirm - a continually improved - existence of physical means of payment and identification or the partial or total change to a non-physical or cyber form of them. The line-up of speakers shows both the deep technological knowledge and managerial and political weight the programme offers.

A TALK AT THE TOP

Both will be given equal importance in the panel discussion on the last day of the conference, Friday, March 23rd. Under the moderation of the UK journalist Joy Macknight, Deputy Editor of *The Banker*, a sister organisation of the UK daily *Financial Times,* the panelists will discuss the future payment ecosystem - digital money, e-currency, mobile payments or cash. Will just one of these dominate and thus relegate the others to niche applications? Which considerations will be important to consumers, industry and regulatory bodies? And, of course, there will be questions from the audience.

The panel itself will consist of central bankers, top representatives of the security printing industry and a "gadfly". The latter is Linus Neumann, the Senior IT Security Consultant of the Chaos Computer Club (CCC) in Germany, that has challenged and annoyed the established cyber-world since 1981 and that is described by the financial news-service *Bloomberg BusinessWeek* as "a multigenerational army of activists (that) has made the country's democracy a lot tougher to undermine."

Bloomberg continues: "its 29 local chapters are stocked with professionals who run security for banks, head encryption start-ups, and advise policymakers. The group publishes an occasional magazine, produces a monthly talk radio show, and throws the occasional party, too." In September, Bloomberg wrote that the 'white hat' hacker group "by exposing weaknesses in German banking, government, and other computer systems, has helped make them more resistant to attack and contributed to a society that's exceptionally careful about believing what it sees online. In the run-up to their federal elections, Germans were tweeting a much higher proportion of real news—as opposed to campaign spin, amateur screeds, or outright b.s.-than Americans or Brits did during their latest political campaign seasons, according to researchers at the University of Oxford." "The only way to save a democracy is to explain the way things work," says Linus Neumann, the CCC spokesman and information security consultant. "Understanding things is a good immunization."

How the other panelists, Michael Lambert, Director of Banknotes, Board of Governors of the Federal Reserve System in the USA, and Leif Veggum, Director, Cashier's Department, Central Bank of Norway for the central bank side and the heads of the two largest private security printers, Wolfram Seidemann, CEO of G+D Currency Technology and Martin Sutherland, CEO of De La Rue for the side of the currency producers, will react, will be one of the interesting high points of the conference. Both the leading international companies in the field have made changes in their organisations to take account of the developing situation the world over and as such decisions are always long-term, how their leaders think, will shed light on the future of the industry as a whole.

DUBLIN

Dublin is by no means an accidental choice as the venue for the Security Printers, International Conference and Exhibition. Dublin has attracted many tech companies that have based their European headquarters here, among them Microsoft, Google, Amazon, eBay, PayPal, Yahoo!, Facebook, Twitter, Accenture and Pfizer with several located in enterprise clusters like the Digital Hub and Silicon Docks, leading to Dublin sometimes being called the "Tech Capital of Europe". Since the establishment of the International Financial Services Centre, Dublin has gained prominence on the financial side as well, and many financial companies, including Citybank and Commerzbank have headquarters in the city. The Irish Stock Exchange (ISEQ), Internet Neutral Exchange (INEX) and Irish Enterprise Exchange (IEX) are also located in Dublin. Dublin is one of the main cities vying to host financial services companies hoping to retain access to the Eurozone after Brexit. ■

How Euros are being used

A recently published detailed ECB study sheds light on the daily use of Euros at the point of sale. Here is a short overview.

In a speech in October, Victoria Cleland, Chief Cashier of the Bank of England, reflected on the apparent contradiction that the amount of banknotes in circulation is rising, while more and more people pay for everyday purchases with cards or contactless systems or shop online. She, as well as a report by the Reserve Bank of Australia, listed a variety of reasons for this phenomenon, but it seems clear that they and many other central banks have no really detailed information on how people pay for purchases. The European Central Bank commissioned a research project to close this information gap.

The ECB's report on "The use of cash by households in the euro area" acknowledges that although Euro banknotes have been in use for 15 years, not much was known about how households really use cash. But now, the survey taken in all 19 Euro area countries, delivers clarity on how consumers pay at points of sale (POS). Such information will contribute to improving the efficiency of the cash cycle and the payment system as a whole.

The "Survey on the use of cash by households (SUCH)" was conducted from October to November 2015 and from January to July 2016. It involved 65,281 respondents, who kept a diary to write down all the payments and cash withdrawals or replenishments that they carried out during the course of a single day, except for Cyprus and Malta, where three-day diaries were used. A total of 128,677 payments were reported. A subset of 28,099 respondents also completed a questionnaire on consumers' access to payment instruments, their payment behaviour, in order to analyse these results together with the reported transactions. Germany and the Netherlands did not participate directly in the study, as their central banks have been carrying out similar studies since 2008, the results of which have been incorporated into the ECB study. The total number of survey participants for the whole Euro area, including Germany and the Netherlands, was 92,080, reporting a total of 198,600 payments.

CASH STILL WIDESPREAD, BUT UNEVENLY SO

The study indicates that the use of cash at POS is still widespread in most Euro area countries, challenging the perception that cash is rapidly being replaced by cashless means of payment. However, it is worth noting that there are considerable variations from country to country. In total, to pay for their POS purchases, Euro area consumers made 124 billion cash payments, 30 billion card payments and 3 billion payments by means of other instruments, such as cheques, direct debit, credit transfers and mobile payments. Although cash was mainly used for low-value purchases, it was used four times more often than debit or credit cards, bringing the total value of cash payments above that of all card payments. In terms of number of transactions, 78.8 per cent of purchases at POS were paid using cash, 19.1 per cent using cards and the remaining 2.1 per cent was paid using various other payment instruments. In terms of value, cash payments accounted for 53.8 per cent of all POS payments, cards for 39 per cent and other means of payment accounted for the remaining 7.2 per cent.

But in spite of cash being used more often, a larger share of consumers said they preferred cards rather than cash. This contradiction may be explained by the fact that nearly two-thirds of the transactions conducted at POS in 2016 were below €15 and only 8 per cent were above €50, and only 14 per cent were made in shops for durable goods or in petrol stations.

Access to payment cards does not seem to fully explain differences in payment behaviour, because on average, access is high in all Euro area countries. However, there seems to be a relationship between card acceptance and cash usage. In countries and market sectors where card acceptance is still low, cash usage may decrease once infrastructure for making card payments becomes more widely available. The same applies to contactless payments, which in many countries are still low, but once contactless cards and terminals are available more widely, their share of payments could increase significantly. Contactless payments at POS are typically relatively low in value and as 81 per cent of all payments at POS are below €25 and consumers value quick check-out, contactless payments could quickly impact the use of cash.

RELATIVE USE OF PAYMENT INSTRUMENTS

Cash was used most in southern Euro area countries, as well as in Germany, Austria and Slovenia (resulting in country shares of 80% or above for all POS transactions). The market share of cash was lower in Latvia, Lithuania, Slovakia and Ireland, ranging from 71 per cent to 79 per cent. Belgium, Luxembourg and France follow with a cash share

ranging between 63 per cent and 68 per cent. The Netherlands, Estonia and Finland had the lowest shares, ranging between 45 per cent and 54 per cent of all payments at POS. In all countries the share of cash in terms of value was much lower than the number of payments. In Cyprus, Malta and Greece the share of cash in value of payments was the highest, ranging from 72 per cent to 75 per cent. In Lithuania, Slovakia, Austria, Spain, Italy and Slovenia the share ranged from 62 per cent to 68 per cent. In Ireland, Portugal, Latvia and Germany the range was between 49 per cent and 55 per cent, while in the Benelux countries, France, Estonia and Finland the share ranged from 27 per cent to 33 per cent.

AVERAGE VALUE OF TRANSACTIONS

On average in the Euro area, the value of a cash transaction was €12.38 with the highest value in Cyprus, Luxembourg and Austria where it ranged from €18.60 to €17.80. The average cash transaction value was the lowest (below €10) in Spain, Latvia, France and Portugal where it ranged between €8.80 and €7.50, indicating that in these countries cash is mainly used for small payments.

Contrasting these findings with card payments, their transaction value was the highest in Luxembourg, Malta and Germany, where it ranged from €70.78 to €51.38 and the lowest in Slovakia, Estonia and Latvia where it ranged from €16.05 to €14.33, indicating that consumers in these countries use cards for relatively low-value payments. Diary results suggest that cheques or credit transfers and direct debits are commonly used to pay for larger amounts, such as at hotels, certain service providers or at public authority offices. The average transaction values of these kinds of payments were therefore higher than those of cash and cards, the highest being in Ireland, Cyprus and Luxembourg, where they ranged from €387 to €130.

USE OF PAYMENT INSTRUMENTS BY VALUE RANGE

Consumers spent on average €18 every time they made a payment at POS using cash, cards or other payment instruments. Most POS payments involved lower transaction values; over a third of payments were lower than €5, and 65 per cent were lower than €15. Conversely, only two in over 100 payments were worth more than €100.

Which payment instrument consumers use is strongly influenced by the payment amount; cash is mainly used for low-value payments - under € 45, used in 91 per cent of POS purchases - while cards are used for larger-value payments. Although absolute levels differed between countries, within each country the average value of a cash transaction was lower than the average value of a card transaction. However, even at payment amounts above €100, the use of cash remained relatively high. Almost a third of POS transactions with a value above €100 were paid with cash, amounting to 10 per cent of the value of all cash payments at the POS in the euro area, although with 2 per cent the number of payments above €100 was relatively small. The share of cash payments above €100 in the total value of cash payments at the POS was wide-ranging, from 3 per cent in France or 5 per cent in Belgium, to 21 per cent in Ireland and Slovenia or 26 per cent in Greece.

THE USE OF CASH FOR RECURRENT PAYMENTS

In some countries it is not unusual to pay recurrent expenses such as rent, utilities, telephone subscriptions and insurance, but also home delivery of oil or gas, or medical services in cash. On average, in the whole Euro area (excluding Germany) only 6 per cent of rents were paid in cash, but in Greece this figure was 26 per cent and around 15 per cent in Slovakia and Malta. 56 per cent of respondents in Greece and nearly 25 per cent of those in Italy said they paid their electricity bill in cash. Also, 9 per cent of respondents indicated that they paid their taxes and 10 per cent stated that they paid their insurance mainly in cash. Furthermore, on average almost one out of three respondents indicated that they paid their medical bills mainly in cash.

AMOUNT OF CASH PEOPLE CARRY

In 2016 euro area consumers carried on average €65 in their wallets but again there are large national differences. Germans carried on average the most (€103) in their pockets, followed by the Luxembourgers (€ 102) and the Austrians (€89). The Portuguese carried, on average, the least (€29), followed by the French (€32) and the Latvians (€41). Men carried on average €12 more than women. Moreover, the amount of cash carried by consumers increased sharply with their age. Consumers in the oldest age group carried up to €43 more than those in the youngest age group but there does not seem to be a correlation with education levels.

CARD OWNERSHIP AND WITHDRAWALS

The vast majority of Euro area consumers (93 per cent) owned or had access to a payment card in 2016, but only 66 per cent of the Cypriot adult population said that they owned a payment card.

In general, card ownership seems to explain little about the general payment behaviour in a certain country. But since a payment card does not necessarily need to be used for card transactions and can be solely used for cash withdrawals from ATMs, this is not surprising.

ATMs were by far the most important source of cash (61 per cent) by value, while on average 8 per cent was withdrawn from bank counters and only 2 per cent was obtained via cashback in shops, although in terms of numbers of operations both cash withdrawals and bank counter cash withdrawals amounted to 6 per cent.

Considering all sources combined, consumers added cash to their wallets 1.2 times per week with an average value of €62. The average amount of cash added to wallets differed widely between countries. The highest average amount withdrawn or replenished was in Luxembourg with €129, followed by Germany with €109 and Cyprus with €81 and the lowest average amounts withdrawn were in Belgium (€27), France (€29), Portugal and Latvia (both €36). The vast majority of Euro area consumers (84 per cent) did not receive their cash from any regular income. Nevertheless, on average, 16 per cent of consumers received at least a quarter of their regular income in cash. Roughly half of this 16 per cent actually received more than half of their income in cash.

CASH AS A STORE OF VALUE

The ECB estimated that in 2008 around one-third of the value of euro banknotes in circulation was held as a store of value in the euro area (ECB, 2011). Considering that since 2008 the amount of euro banknotes in circulation has grown faster than private consumption and taking the low interest rate environment into account, it can be expected that this share has grown even further. Survey respondents were therefore asked whether they keep any precautionary cash reserves and to give an indication of the amounts they keep outside of bank accounts.

On average in 2016, 24 per cent of respondents said that they had saved cash outside a bank account as a precautionary reserve. The countries in which most respondents answered that they kept cash as a reserve were Slovakia and Lithuania, where respectively 40 per cent and 37 per cent of the respondents said that they kept cash as a precautionary reserve. Elsewhere, no more than one-third of respondents said that they put cash aside. The lowest share of respondents who said that they kept cash aside could be observed for Belgium (19 per cent) and France (15 per cent). Despite the banking crisis in Greece, as a result of which cash withdrawals increased significantly, on average only 22 per cent of Greek respondents said that they kept cash as a precautionary reserve.

Out of those who responded that they put cash aside, 23 per cent kept up to €100, 22 per cent stored between €101 and €250 and 19 per cent stored between €251 and €500. In general it appears that the proportion of respondents who save larger sums of money decreases as those sums of money increase. Only 9 per cent of the respondents put between €1,001 and €5,000 aside and 2 per cent kept more than €5,000 at home or in a safety deposit box.

USE OF HIGH DENOMINATION BANKNOTES

It is often claimed that high denominations are hardly ever used for regular transactions and that an average citizen rarely encounters these denominations, since they are supposedly not needed or used by ordinary citizens. To test this assumption, survey respondents were asked if in the year preceding the survey they had had a €200 or €500 banknote in their possession and if so, how they obtained it and what they did with it.

Results show that in the year prior the survey, 19 per cent of euro area consumers had a €200 or €500 euro banknote in their possession. This is a lower share than in 2008, when an ECB survey with exactly the same question was carried out among eight euro area countries. At that time 25 per cent of the respondents in these eight countries reported having had a high denomination in their possession more than once a year (ECB, 2011).

The countries where at least one-third of the respondents answered that they had a high-value banknote were Slovenia (47 per cent, Luxembourg and Slovakia (both 42 per cent) as well as Lithuania (41 per cent) and Austria (36 per cent). The lowest proportions can be seen in the Netherlands (7 per cent), France (8 per cent) and Ireland (11 per cent).

Compared with the 2008 survey results, the shares of those who had a €200 or €500 banknote in their possession remained nearly the same for France, the Netherlands and Austria. In these three countries the share dropped by 1 percentage point only. The share in Spain was 6 percentage points lower than in 2008, but the share dropped significantly in Belgium and Italy, by 13 percentage points and 18 percentage points respectively.

The ECB study, focussing on households' daily payments, which tend to be small and often overlooked, concludes that despite numerous articles claiming a cashless society is imminent, it appears that the use of cash at POS is still robust in most Euro area countries. The results give insight into the differences in payment choices in the 19 Euro area countries, for most of which it is the first time they have had estimations on the use of cash. ■

The paper can be downloaded from www.ecb.europa.eu, from the Social Science Research Network electronic library or from RePEc: Research Papers in Economics.

...AND HOW US$ ARE BEING USED

Echoing the European Central Bank's study of payment behaviour, the US Federal Reserve produced a similar study on the use of cash, called Understanding Consumer Cash Use: Preliminary Findings from the 2016 Diary of Consumer Payment Choice (DCPC).

As in Europe, in the USA, the public's demand for cash continues to grow as the amount of currency in circulation reached $1.43 trillion in October 2016. The demand for high value denominations is especially strong. Since 2009, the annual rate of growth of the number of banknotes has been 5.6 per cent and the growth in value 7.4 per cent.

The study followed a similar principle as the ECB study by using a payment diary and it produced broadly similar results: cash remains the most frequently used payment instrument with 31 per cent of all consumer transactions, most consumer payments are for small value transactions, and they are mostly in cash with about 60 per cent of them for under $ 10, but only 20 per cent for over $25 or more. Cash is held and used by a large majority of consumers, regardless of age and income; however, how it is used varies across demographic groups. Cash is mostly used in payments between persons, but only 75 per cent of all payments were conducted in person.

Cash is also frequently used as a store of value, but demand for $50 and $100 notes is greater in the international market, while demand for lower denomination is greater domestically. While most $100s are held internationally, the majority of currency shipments to and from the Federal Reserve are destined for the domestic market.

On average, DCPC participants made 46 transactions per month, and used cash to pay for 14 of them (31 per cent). Debit and credit made up 27 and 18 per cent respectively. By value, the average cash transaction was about $22, while average debit card and credit card transactions were $44 and $57, respectively. Overall, cash payments accounted for eight per cent of the average $4,000 that participants reported spending during the month, while debit accounted for 13 per cent and credit card payments accounted for 14 per cent.

US consumers make - on average - 14 cash transactions per month, regardless of household income. However, households with an annual income of less than $50,000 per year rely more heavily on cash than do higher income groups. Households earning less than $50,000 per year have considerably fewer transactions overall and, as a result, their cash transactions make up a larger share of their total – 8 to 16 percentage points higher than those making more than $50,000.

In numbers of transactions, people under 35 years-of-age use cash less than those over 35, with the number of cash payments equaling approximately 9 and 16 transactions per month, respectively. Many consumers hold cash as a secondary payment option and nearly 85 per cent of participants held cash at the end of at least one survey day with the average value of nearly $59.

Technological developments and the continued growth of electronic and mobile commerce are changing consumers' shopping and payment habits. When consumers shop online, or not-in-person, using cash is almost never an option and increased online payments are causing downward pressure on cash use.

Overall in the digital age, cash use remains resilient, the report concludes, but recent natural disasters have shown the limits of electronic payments. During these times, the need for cash is great. As long as the public continues to demand, use, and hold cash, the Federal Reserve will deliver it. ■

BITCOIN'S BULL AND BEAR RIDE

The cyber-currency is unlikely to take over, as no national currency could survive such wild oscillations between high and low.

...or, on second thoughts, perhaps not

One reason to take an interest in bitcoin - there may be many others - is that it is a kind of competition to banknotes and competition needs to be examined. Although the facts about bitcoin are widely known, it is remarkable how wide opinions about this digital or crypto currency diverge. Warren Buffett, CEO of Berkshire Hathaway warned: "A real bubble in that sort of thing"; and "bitcoin is not a currency", Lloyd Blankfein, CEO of Goldman Sachs was more neutral: "Still thinking about bitcoin. No conclusion", Mark Carney the governor, Bank of England, was perhaps carefully positive: "Potential to enhance resilience", Vítor Constâncio, vice president of the European Central Bank, compared the digital currency to the 17th century mother of all financial bubbles: "bitcoin is a sort of tulip", while Mario Draghi, president of the ECB remained carefully noncommittal: "It would actually not be in our powers to prohibit and regulate", an opinion later echoed by Mark Carney. Nobel price winning economist Paul Krugman, professor at City University of New York and New York Times columnist said bluntly: "Bitcoin is evil", while Christine Lagarde, managing director of the IMF said enigmatically: "Might just give existing currencies and monetary policy a run for their money". Zhou Xiaochuan, the governor of the People's Bank of China was being realistic, even after banning mainland China residents from trading in crypto currencies on

exchanges in September last year: "Digital currency and cash will co-exist for a long time." So, whatever you think, you will have someone important in the financial world to back you up.

At the end of the year, bitcoin made it very often on to the front pages of the "quality papers" and it was hardly ever absent from the financial pages, mainly because the price of one bitcoin had hit $19 500 on December 16, 2017. Just before Christmas, bitcoin lost $ 4000 in a day, pushing it down to $ 15 000 again, only to recover again to over $ 16 00 a few days after Christmas. As a comparison, the digital currency stood at $ 12 in 2013. Between these dates there were many sudden rises and deep falls of the cryptocurrency, indicating that it would certainly not be fit to replace any national currency.

By February it looked as if the bitcoin bubble had burst, as its price, which rose by 900 per cent last year, fell to below $6000. The cryptocurrency had been the best performing asset of 2017. It is unlikely that this feat will be repeated in 2018, but it seems to be impossible to make any clear forecasts about bitcoin.

Apart from being too volatile to be a real currency, bitcoin also seems to be eminently hackable. In mid December, the BBC said that North Korea had hacked the Bithumb cryptocurrency exchange in South Korea and stole at least $7m in digital money, a figure that has meanwhile ballooned in value to $82.7m. In its short history there had been several other grand scale thefts of bitcoin.

While some economist worried that cryptocurrencies could jeopardize the economy and cause a crisis, a great majority of them do not think so. The top cryptocurrencies are worth about $350 billion - less than the $513 billion market value of Facebook. "Despite recent growth, the market cap of cryptocurrencies remains modest, compared to the size of 'conventional' financial markets," argues Robert Kollman, an economist at Université Libre de Bruxelles. "Cryptocurrencies do not seem to represent a threat to financial stability – for now."

This somewhat detached view was challenged a few months later, when the new head of the Bank for International Settlements, Agustín Carstens, said in early February that bitcoin had become a combination of "a bubble, a Ponzi scheme and an environmental disaster" that threatened to undermine public trust in central banks. "If authorities do not act pre-emptively, cryptocurrencies could become more interconnected with the main financial system and become a threat to financial stability," he said, speaking at Goethe University in Frankfurt, Germany. "There is a strong case for policy intervention. Appropriate authorities have a duty to educate and protect investors and consumers, and need to be prepared to act," he continued.

Carstens, a former governor of Mexico's central bank, said central banks should in particular pay attention to the ties linking cryptocurrencies to real currencies, to ensure the relationship was "not parasitic". His comments were a clear sign that global regulators are preparing a crackdown on bitcoin.

Even if bitcoin itself is not seen as a possible currency, the way it solved the problem of digitally copying and thus reusing of spent bitcoins - the digital currency equivalent of counterfeiting - has caught the eye of experts in many industries. The bitcoin solution to this is the blockchain, an online ledger that records and validates all peer-to-peer payments to eliminate double-spending, while encrypting transactions to provide anonymity. ■

FINLAND'S CENTRAL BANK THINKS ABOUT CBDC

It is hard to think what would happen if central banks no longer issued cash. The Bank of Finland looked at the posibilities of Central Bank Digital Currency (CBDC), but it certainly does not advocate its use.

Given the obvious disadvantages of bitcoin, or of any other digital currency, it is remarkable that even central banks ponder the theoretical case of using it. In 2017, the Bank of Finland, a part of the Euro System, published a paper in its BoF Economics review, entitled "Central Bank Digital Currency". The paper said that banknotes, issued by central banks to the public, are becoming technically out-dated. Central bank-issued electronic money would offer the public the possibility to hold central bank money in a potentially cashless future.

There are two forms of central bank money, cash - the only form in which it is held by the general public - and reserve deposits from commercial banks, held with the central bank. Both types are entered as liabilities on the central bank's balance sheet. No central bank is known to have issued any other type of central bank money, to be used by the general public. But central bank money represents only a part of the money supply in an economy. Most money is 'scriptural currency' created as a result of lending by deposit banks and could be

fully converted into central bank money. New central bank money is always created via central bank accounts and based on monetary policy decisions.

As for central bank digital currencies (CBDC), neither the technology nor the economic impacts have been thought out and there is scarcely any academic research on the topic. Nor is there relevant legislation or an international standard.

WHAT WOULD CENTRAL BANK DIGITAL CURRENCY BE LIKE?

The BoF paper says that central bank digital currency would need to meet the following criteria:

- The central bank issues it in digital form.
- Anyone has the right to hold it. It is not a privilege reserved to e.g. credit institutions.
- It is the same currency as banknotes and central bank deposits, and perhaps banks could convert it freely into central bank money.
- It can be used in retail payments.
- In a transaction between two people, there is no third party that verifies or executes the payment as a central counterparty, just as with banknotes.

Cash, in its current form, has many characteristics that users find important but that e.g. cards lack, among them anonymity, immediate finality and transaction clearing without third parties. Anonymity in cash payments means identification of the parties is neither necessary nor important. In Finland, only 2 per cent of respondents found anonymity important for selecting a payment method. In Germany, anonymity of payment is of much larger importance and the euro area, 13 per cent of consumers wanted anonymity in retail payments. A further feature of cash is that the payment instrument itself is also an asset. Cash is a liquid asset, and it is often used in saving 'for a rainy day'. Card payments, credit transfers and direct debits are not assets as such; they only provide access to the payment system where settlement takes place.

In the case of cash, anonymity, immediate settlement and independence of central counter-parties are all based on the fact that cash is a bearer instrument, i.e. the person who is physically in possession of the banknotes and coins is legally their owner. In addition, they include all the information required for authentication and settlement finality.

Making a bearer instrument digital does not make it fully equivalent to cash. To do that, it should be convertible into a sequence of numbers, which would verify ownership. This would correspond to the private key in the bitcoin system, where the distributed ledger includes real-time information on the amount of purchasing power owned by the holders of each private key. To make this type of system independent of a central authority, the purchasing power of each private key is recorded in a distributed ledger, instead of a centralised ledger, a difficult thing for a CBDC to pull off.

A further aspect of money is the resistance to counterfeiting. Banknotes are secured by a sophisticated and expensive production process with many verification features and in electronic recordkeeping, non-counterfeitability is based on verified transaction records and double-entry bookkeeping.

One key requirement of a payment instrument is confidence in the acceptability and continuity of the instrument. In the euro area, this is guaranteed by the full convertibility of scriptural money of commercial banks into cash. Another issue is the stability of value, which is influenced by the inflation targets of central banks. While cash is not dependent on technology, digital money can never be fully independent of technology or devices.

There are a number of ways to implement central bank digital currency. The central bank could provide a system in which the digital currency is stored, transferred and authenticated. Another possibility is to create a standard for digital currency in which the private sector would be responsible for creating the storage and transaction applications. The third alternative is to limit the central bank's role to the creation of money in respect to balance sheet and debt relationships. The private sector would be responsible for the technical arrangements.

If the objective is to create a CBDC with the characteristics of cash, the key characteristics are anonymity, immediate settlement, the possibility to make retail payments, and a distributed ledger system. Bitcoin has created these characteristics in digital form, but bitcoin's blockchain technology is not very suitable for retail payments, as it is considerably slower and less efficient. The paper said that it would thus be more advisable to implement CBDC, and also other retail payment systems, using other technology, e.g. a centralized ledger.

THE BENEFITS OF CBDC

While the paper explains the 'what' and 'how' of CBDC quite well, on the 'why', the possible benefits of it, the paper is less sure. It argues that with payments shifting increasingly online, and with mobile devices, there are signs that there would be a demand for CBDC among consumers. Not all consumers have a credit card and some also perceive online card payments as unsecure. Also it is not possible to use cash in online payments, but there might be a need for payments in central bank money. These arguments for a CBDC are

not terribly convincing and the paper recognizes that because of the regulatory obligation to pay wages and other earnings into a bank account, and because consumers pay expenditures from their bank accounts, retail banks' central role in the provision and settlement of retail payments is secured at present. This also applies to their role as lenders, since bank lending and borrowers' loan repayments concentrate on the same bank accounts. Therefore, in the current system, banks play a key role in households' and companies' economic affairs. However, one could ask whether the current arrangement between banks and income earners will also be optimal in the future, and whether it is the best possible solution to use the banking system in the organisation of payments. This argument may perhaps suffice, but it does not show great urgency.

CBDC could also have implications for financial stability. Banks have played a pivotal role in society because payments are at the centre of economic activity and exchange. Financial crises typically stem from banks' risk-taking and other economic actors' over-indebtedness. Central bank-issued digital cash would offer a new alternative to payments, but this could have implications for the stability of banks' deposit stocks and thereby also for bank funding.

PROBLEMS AND UNINTENDED EFFECTS

Technically, it would be possible to extend the functionality of ATMs and online banks to handle digital cash, to offer an alternative to bank deposits. However, low interest-bearing deposits by private customers as a source of bank funding could become more unstable. Banks could offer higher interest rates on accounts or additional services to attract deposits back or they would have to borrow from somewhere else. If deposits of the public were to flow to the central bank balance sheet in the form of digital cash, this would result in a financial surplus for the central bank and, correspondingly, a financial deficit for commercial banks. In such a case, the central bank would need to increase its financing to commercial banks. Since central banks provide liquidity against collateral, commercial banks would need more securities as collateral.

Another potential problem could be the impact of CBDC on the risk of bank runs, where, in principle, bank runs could also occur at times when bank offices are closed. The higher risk of bank runs should be taken into account e.g. in bank liquidity regulations: retail deposits would no longer be as reliable and stable a form of funding as has customarily been the case. On the other hand, modern deposit guarantee schemes have effectively prevented bank runs.

It is extremely difficult to estimate the macroeconomic implications of digital cash without historical experience and we have problems to assess the macroeconomic or other broader effects. Therefore, no actual conclusions can yet be drawn. However, among the few hypotheses the paper offers, is that people would treat digital cash the same as they threat credit card payments, with which they are usually less disciplined than with real cash. Of course, digital cash would be determined as cash without the possibility for credit, in which case the central bank would not need to worry about the credit risk.

UPDATING FINLAND

On December 24, the Israeli newspaper Haaretz claimed that Israel's treasury is considering issuing digital currency similar to bitcoin, a move that would stem the millions lost annually to the country's black-market economy. It is claimed, that the latter makes up 22 per cent the country's gross domestic product, costing the treasury about 50 billion shekels in uncollected taxes annually – almost equal to the country's education budget.

The proposed digital money would be identical in value to the country's existing currency. It wouldn't be designed to change the country's monetary system and it would enable payments directly from smartphones to anyone, without involving payment transfers between banks. It would simply be a substitute for cash. However, if one of the reasons to introduce digital money is to combat the black market, it could not be anonymous like cash and it would have to be the only central bank money available. If digital and paper-based shekels existed side by side, black market payments would still be conducted in hard cash. And eliminating cash and forcing all consumers to use smartphones for payments seems unrealistic. The card and banking industry would also complain bitterly, as the only difference between CBDC and commercial bank digital money, at least as long as interest rates are negligible, would be that an account at the bank can be overdrawn. But doing away with cash without having central bank money in any form may spell even grater problems. Central banks around the globe do have concerns over the power of commercial banks in a bank-based digital currency system. However, whatever the answer, it's a good bet that Israel won't be the first to issue digital currency, instead letting others try it out first.

AND THEN THERE IS VENEZUELA

Israel was not the only country to muse about a central bank crypto currency. In early December, Venezuela's President Nicolás Maduro announced the creation of a new virtual currency, called the Petro, in a bid to ease the country's economic crisis.

The Petro would be backed by Venezuela's oil, gas, gold and diamond wealth. Maduro said the new crypto-currency would allow Venezuela "to advance monetary sovereignty, to make financial transactions and overcome the financial blockade". He gave no details on how, or when, the new currency would be launched. Opposition leaders scorned the announcement, doubting whether the digital currency would ever see the light of day in Venezuela, where the 'standard' currency, the Bolivar, is in free fall.

...AND RUSSIA

In early January, the New York Times reported that Russia as well, is toying with the idea of introducing a crypto currency. Just as in Venezuela, the idea is not to end tax avoidance, but to find a way around sanctions imposed by the US or the UN, which are usually enforced through regulatory and banking disclosure rules. "We can then settle payments with our business partners all over the world regardless of sanctions," one of Mr Putin's aids said.

Economists doubt that the Petro and the Russian crypto Ruble would work in the way the governments seem to anticipate. That's because virtual currencies are decentralized systems with no one in charge, while the Russian and Venezuelan plans would give the leaders of both countries a measure of control over the new currencies. That runs counter to the basic concepts of virtual currency. However, the fact that governments and central banks are talking about cyber currencies means something is afoot, unless, by the time you read this, the bitcoin bubble has burst and cyber currencies are off the table again.■

SWISS NATIONAL BANK ACQUIRES MAJORITY STAKE IN LANDQART AG, ORELL FÜSSLI TAKES MINORITY SHARE

On December 20, 2017, the Swiss National Bank (SNB) announced that it had acquired 90 per cent of the shares in Landqart AG. The remaining 10 per cent of the share capital will be purchased by Orell Füssli Holding Ltd. Landqart is a subsidiary of Fortress Paper, which is listed on the Toronto stock exchange. At the same time, and at the same 90/10 split, the share capital in Landqart Management and Services will also be acquired; this company holds the relevant patents for Landqart's activities. The purchase price for the acquisition of 100 per cent of both companies is CHF 21.5 million.

The acquisition of Landqart takes place against the background of an acute need for liquidity. Following the unexpected cancellation of an order by a customer abroad, Landqart experienced a sharp drop in turnover. As a result, the company introduced short-time working in December and is facing a liquidity shortage. This poses a direct and existential threat to Landqart. Therefore, after the takeover, the company will be provided with the necessary liquidity to ensure its survival.

Landqart manufactures the Durasafe substrate used in the production of the new Swiss banknotes. It is the only supplier to provide the Durasafe technology and associated production capabilities. The SNB has decided to acquire the company because, otherwise, issuance of the new Swiss banknote series would not have been guaranteed across the entire production stream. By taking this step, the SNB is ensuring the continued supply of cash and, hence, the fulfilment of its own statutory mandate.

So far the official announcement by the SNB. At the beginning of November, Landqart had announced that one of its significant international customers - believed to be India - had cancelled that portion of purchase orders which were scheduled for production and delivery in the fourth quarter of 2017 and in fiscal 2018. The cancelled purchase orders represented approximately 16 per cent of the budgeted order book at the Landqart Mill for fiscal 2017 and 30 per cent for fiscal 2018. Although Landqart tried to get the cancellation rescinded, it proved to be futile. The company's management tried to fill the production void by pulling forward existing purchase orders, seeking new orders from existing and new customers, and requesting special one-time supplemental orders from existing customers for immediate production.

The Swiss National Bank, that had always relied on private suppliers for the production of its banknotes, now finds itself as the majority owner of a security paper mill that not only produces the Durasafe substrate for the Swiss banknotes but other banknote paper as well. It remains to be seen what the bank will do with this acquisition.

As the communiqué of the Swiss National Bank indicates, the printer of the Swiss currency, Orell Füssli Security Printing, through is parent company Orell Füssli Holding AG, now owns not only 10 per cent of the shares in Landqart AG, but also in Landqart Management and Services, which holds the relevant patents for the activities of Landqart AG. By acquiring the shares, Orell Füssli is, firstly, ensuring the supply capacity of the substrate. Secondly, Orell Füssli Holding expects strategic cooperation in the recruitment of new customers for high quality, innovative banknotes to create wider opportunities in the medium term, the company said. ■

This is a mock-up of the coming blue UK passport. (left) The Original 'old blue' did not thave the biometric symbol.

The rebirth of the 'old blue'

After the UK leavs the European Union, the UK passport will be the traditional blue again. Will the patriotic feeling of having a different passport colour than everybody else compensate for having to join a longer line at EU border crossings?

In December last year, the British government announced that after the country leaves the European Union in 2019, the UK passport, which is currently the standard EU burgundy colour, will return to being dark blue. The pro Brexit press, conservative MPs and Brexiters generally, rejoiced, claiming that this is "the first real, tangible victory", an end to "humiliation" and a proud expression of Britain's national greatness. Brandon Lewis, the UK immigration minister, said: "Leaving the EU gives us a unique opportunity to restore our national identity and forge a new path for ourselves in the world. That is why I am delighted to announce that the British passport will be returning to the iconic blue and gold design after we have left the European Union in 2019", the *Guardian* wrote. Brexit supporters had been complaining about the colour of the passport for quite some time. The Conservative MP Andrew Rosindell said last April that "the humiliation of having a pink European Union passport will now soon be over and the United Kingdom nationals can once again feel pride and self-confidence in their own nationality when travelling, just as the Swiss and Americans can do." He did not only get the colour wrong, but the insinuation that the colour of the passport was forced upon Britain when the country joined the EU was equally false.

It was Charles Powell, a key foreign policy adviser to (conservative) Prime Minister Margaret Thatcher, who pointed out that it was Thatcher's government who "chose" to ditch the blue passport in the 1980s – under no pressure from the European Union. He said that the clamour for the old-style travel document was "part of the nostalgia on which the predominantly elderly Brexit constituency thrives". He added: "So long as they are content with symbols, rather than substance, I see no harm in letting them have their way. Perhaps we should go the whole hog and reintroduce ambassadorial dress uniforms, as well as bowler hats and stiff collars for senior civil servants." The European parliament's chief Brexit coordinator, Guy Verhofstadt, also chimed in on Twitter: "There is no EU legislation dictating passport colour. The UK could have had any passport colour it wanted and stay in the EU." The first burgundy machine-readable passports were issued in the UK in 1988, after the common format introduced by the European Economic Community.

While the colour of a passports cover is wholly irrelevant - even now, EU member state Croatia has a dark blue passport - what counts is what is inside and that, at least on the data page, is neither dictated by the EU, nor by the British government. Just as now, the UK passport will still have to follow ICAO standards. That also applies to the size, as the nostalgia-gang used to complain that the burgundy passport was smaller than the old blue one. Unless the UK envisions that their nationals shun all ABC gates the world over, the new blue passport will have to have the same size as all others.

Most of the recent changes to British passports have been driven by the US rather than the EU. The US requires certain passport features for participation in its visa-waiver programme, which allows citizens of most developed countries to enter the US for business or tourism trips of up to 90 days without a visa. The US demands compliance with ICAO standards, but it also imposes more stringent photo requirements and biometric features. These US requirements have been imposed on the UK via the EU, which incorporated the demands into its own passport standards. But the UK would only be able to escape these requirements after Brexit by giving up visa-free travel to the US.

NOT QUITE SOVEREIGN DECISIONS

On closer inspection, passports are probably poor instruments for nationalistic individuality and bravado, as their purpose and usefulness depends on other countries recognizing and accepting them. Even the 'old blue' was imposed by an international body. The first modern British passport, the product of the British Nationality and Status Aliens Act 1914, consisted of a single page, folded into eight and held together with a cardboard cover. It was valid for two years and, as well as a photograph and signature, featured a personal description, including details such as "shape of face", "complexion" and "features". In 1920, the League of Nations organised a conference on passports and customs formalities in Paris, which imposed a new set of standards that passports would have to meet to be internationally recognised, which lead to the "iconic blue" UK passport.

It remains to be seen, which privileges UK passport holders will enjoy after Britain leaves the EU and conversely, which privileges all other passport holders will have when they want to visit the UK. ■

Border security and fingerprints

The EU has high ambitions to improve border security with new systems. But the fingerprints encoded on EU passports seem to be merely back-ups.

Infosecura has written several times about the threat posed by "morphed" ID photos, even at automatic border control gates. A similar problem is that of 'look-alike' photos in passports, which can also deceive human border controls. The problem is not new and the resolution is already there - but the use of it seems to be patchy.

Late last year, the online paper *'Dutch News'* ran a story that pointed out, that eight years after fingerprints became a part of the second generation of Schengen ePassports, the technology has never been used to check a passenger crossing a border. The measure aimed to stop 'lookalike fraud', whereby somebody travels on the passport of someone who strongly resembles them, or, since technology has moved on since then, morphed ID photos, which try to enable two people to use the same passport. The point of all ID checks at borders is to verify that the bearer of a passport is indeed the person to whom it was issued. Both human border control agents and ABC gates can be deceived by look-alike or morphed ID photos, as they compare a physical or encrypted photo with the face of a real person and the look of a person's face can change. A second line of biometric defence would provide greater security. That second line of biometric defence would be fingerprints stored on the chip in the passport.

The article in Dutch News claims that Dutch local authorities have spent €32 million installing 4,800 scanners, which have taken 20 million prints in the last eight years, but border control agencies are still unable to use them to verify non-Dutch passengers, according to an investigation by Dutch public broadcaster NOS. The Dutch interior ministry admitted to NOS that it had not shared its 'key' with any other country or received the necessary information from any foreign government.

While it seems to be generally true that fingerprints are "under-used", some countries have agreed to share each other's keys, e.g. Germany, France, Czech Republic, etc.. But electronic security features have evolved to use facial recognition as a primary information source, because it is non-contact and fast and it is used much more widely internationally. Speed is a vital factor in border management and fingerprint checking requires contact, which slows things down and some countries' passports, such as those of the USA, do not even contain fingerprints. However, fingerprints are often checked when facial recognition throws up doubts, and not only in border controls but in general policing operations as well.

Fingerprints appear also in another EU border scheme, the Visa Information System (VIS). Since October 2011, the EU collects fingerprints of Schengen visa applicants, which are held in a central database that can be accessed e.g. by border guards in all 25 Schengen countries. VIS connects prints of all 10 fingers to digital pictures and personal information of each applicant for a Schengen visa, so as to avoid fraud. Having a shared database on visa applications also allows governments to check if the person is not also applying for visas, or has already been denied entry, in another Schengen country. The VIS obviously applies to the citizens of countries that require a visa to enter the EU. However, there are 42 non-EU countries whose citizens can enter the EU without a visa and whose fingerprints will therefore not be verified - at least not until the next EU effort to secure borders, the EES system becomes operational.

The new EU Entry-Exit System (EES), which was passed by the European Parliament in late October 2017 and by the EU Council in November, calls for third-country nationals entering the EU to be fingerprinted and photographed at the border. This biometric data, along with the personal information on their travel documents as well as entry, exit or refusal of entry information, will be stored for up to four years and will be accessible to law enforcement, border control and visa authorities. In addition to EU nationals, citizens of non-EU countries in the Schengen Zone of visa-free travel will be exempt from the new system.

It looks as if there are now three systems that collect fingerprints. The fingerprints contained in the EU biometric passports are under the jurisdiction of the member states. As the member states are mostly not exchanging the keys of the digital fingerprints, EU citizen's identification is verified upon leaving or entering the EU by comparing their face with the ID photo in their passport or doing the same by electronic mean in ABC gates.

The second system is the Visa Information System, which requires any non-EU citizen applying for a EU visa to supply a digital ID photo and fingerprints of ten fingers. EU visa holders are then fingerprinted on entry into Schengen area territory and their fingerprints and digital ID photo data is compared with the data taken at the border.

The third system is the Entry and Exit System (EES), which is also supposed to increase general security in the EU, since the passenger data would be available to EUROPOL, where it would serve "to prevent, detect and investigate terrorist offenses or other serious crimes on certain specified conditions," an explanatory text on the EU Parliament's website states. After all necessary sign-offs, the system is set to start operations in 2020.

It looks as if the difference between the Visa Information System and the Entry-Exit System is that the former only applies to travellers from countries that require a EU visa, while the Entry-Exit System applies to all non-EU travellers. There is another system in development, called the European Travel Information and Authorization System (ETIAS), which is a visa waiver system similar to the ESTA system in the USA. It will plug the gap in pre-identification that currently applies to non-EU travellers that do not need a visa to enter the Schengen area. As of January 2020 all visitors that currently do not need a visa to enter a Schengen member country will be expected to apply for an ETIAS authorization.

Many of the information websites use the words 'EU territory' and Schengen area interchangeably. However, the mentioned systems apply only to the Schengen area, as non-Schengen countries in the EU - Ireland and Great Britain - make their own border arrangements and four other EU countries are not yet members of Schengen - Bulgaria, Croatia, Cyprus and Romania - but are expected to join. ■

INDIA'S PASSPORT PROBLEMS: OLD AND ORANGE

Handwritten or non-machine readable passports seem an anachronism, but many are still around in India. The other development in India's passport scene is that migrant workers with little education will in future carry orange passports - for their own good, apparently. Anyone else will travel with a blue one.

Back in December 2013, the International Civil Aviation Organisation decided that November 25, 2015 would be the deadline, after which handwritten or "non-machine readable" passports would be no longer valid. About two years, the organisation decided, would be sufficient for the gradual withdrawal of handwritten passports. ICAO warned that countries might deny visas to such passport holders after the deadline date. The message had obviously not got through to all passport holders in India (the same may apply to other countries as well, but the Indian press picked up on the problems). Over two years after they were declared invalid travel documents and their holders asked to change them, over 100 000 handwritten Indian passports are still in circulation. The Indian government issued several public notices, urging the citizens to get their handwritten passports changed into machine-readable ones but with little success. India is keen to get its travel documents "in sync" with the globally prescribed standard.

India had been issuing machine readable passports since 2001. However, between 1997 and 2000, over 100 000 non-machine readable passports with a validity of 20 years had been issued, the majority of them seem to be still in circulation.

"We have been running campaigns in the country and abroad urging the citizens to get their handwritten passports changed with the one that is machine readable. There are still over a lakh of such passports in circulation," said an official familiar with the process. However, cases of people found travelling with handwritten passports and "ending up getting in trouble" are rare, which may mean that the kind of mass tourism common in Europe and elsewhere is still not very widespread. A further consideration may be that India is a very large country and travel to at least some of the neighbouring countries, such as Pakistan, is not very common.

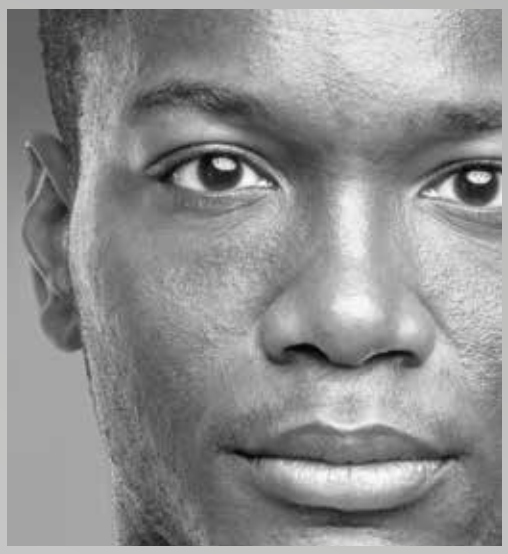
ORANGE: WELL-MEANING BUT STIGMATIZING

In mid January, India's Foreign Ministry issued new rules saying that citizens who are in the "Emigration Check Required (ECR)" category will now carry orange passports, while those who don't will carry blue ones. India is the world's largest exporter of migrant labour and these workers, usually with only primary school educations or even below, are often exploited, while more educated workers are less likely to be exploited abroad.

To offer some protection, India requires unskilled migrants to get clearances from the Indian government before traveling to a number of countries, including the United Arab Emirates, Qatar, Malaysia and Yemen. Until now, unskilled workers who need emigration checks are identified on the last page of their passport. The new passport design, the Foreign Ministry said, would do away with the last page and instead use the coloured covers as a differentiation, to make it easier for immigration officers to spot travellers who require vetting before they travel to certain countries. The theory is, this would also make human trafficking more difficult as border officials and police would immediately know which people need the extra permission to travel. The new rule may be efficient and practical, but critics say this could render migrant workers "second-class citizens", as the new passport cover clearly refers to social status. ■

Let them pass?



The KINEGRAM security solution gives you certainty.
Learn more at kinegram.com.

OVD Kinegram AG | Zaehlerweg 11 | CH-6301 Zug | Switzerland
www.kinegram.com | mail@kinegram.com | A KURZ Company

KINEGRAM®

The success and perils of cyber government

Complex ID systems, such as ePassports and eID cards and even more so, eGovernment that lets citizens conduct their business with the government via the Internet, are prone to attacks by hackers. But sometimes the problem lies in the hardware used.

There is probably no other country that has embraced eGovernment as thoroughly as Estonia, a tiny country on the Baltic Sea that was once a part of the Soviet Union. The country benefitted much from the decision of the government in 2002 to turn it into the world's most sophisticated 'cyber-democracy'. The country also experienced the perils of being a cyber pioneer, more than any other country, when in 2007 it faced sustained waves of cyber attacks that hit its banks and critical national infrastructure. Recently, Estonia faced another cyber security crisis, which also affected its e-residents, foreign nationals that can have their official residence in Estonia, without actually living there.

The latest crisis, in autumn last year, centred on the last version of its national ID card, which is mandatory for all Estonians to have and which is the cornerstone of its e-government. The hardware behind the ID cards was found to be vulnerable to attacks, which could theoretically have led to identity thefts of Estonian citizens and also e-residents. Fortunately, nothing of the sort occurred but Estonia's prime minister, Jüri Ratas, called a special press conference to inform the public of a potential security threat that affected almost 750,000 ID cards issued in the past three years, including thousands of e-resident ID cards. Estonian citizens and e-residents alike had to quickly renew the certificates of their ID cards to eliminate the danger of identity theft.

THE POSITIVE SPIN

"The Estonian government has no intention of letting a good crisis go to waste, as the saying goes, and will use this as an opportunity to carry out further robust development of e-services," the director of the e-residency program Kaspar Korjus said. "The vulnerability and the update of the ID card certificates have already forced the government and private companies, who provide around 5,000 e-services, to think about new and even more sophisticated security arrangements for their services, find even more convenient alternatives, and implement updates at a fast pace."

The Estonian ID card, when connected with a smartcard reader and specific software, gives its owner access to web portals and e-services, enables payments, bank transactions, and digital signatures. Cardholders can even use it to take part in electronic voting. The ID cards use 2,048-bit open-source public-key/private-key encryption, holding two separate digital certificates: one for confirming the holder's identity, and the other to allow them to sign documents with a digital signature. Entering the second PIN is the equivalent of signing a document in person, and it's considered just as legally binding in Estonia.

In October 2014, a new chip, made by Gemalto, had been introduced in Estonian ID cards. According to the Estonia's Information System Authority (ISA), it was faster, based on the latest technology and considered even more secure. It had French and German security certificates confirming compliance with all security requirements. The same chip is used in the identity card of several other countries, as well as bankcards and access documents, explained the ISA. Then in August 2017, a group of Czech researchers informed ISA of a security risk they had discovered in the Gemalto chips. Estonian experts started immediately assessing the risks and a little later, the public was informed although the risk was deemed minimal.

"Theoretically, the reported vulnerability could enable the use of the digital identity for personal identification and digital signing without having the physical card and relevant PIN codes," said ISA. As a precaution, Estonia restricted access to Estonian ID-card public-key database to prevent illegal use.

As days went by and the danger of receiving attacks exploiting the security flaws loomed larger, the government endorsed the proposal by the Estonian Police and Border Guard Board and the ISA to block the certificates of ID cards at risk on November 3. This meant that the 760,000 ID cards issued after October 16, 2014 could only be used for identification and travel. Access to e-services such as the health registry, banking or tax systems was restricted until the certificates had been updated. To guarantee that e-government continued to function, about 35,000 people who had to use their ID card for their work, such as doctors, justice officials, and civil servants, were updated first. In November, the process of remote updating and renewals had finally started to run smoothly, ending the crisis.

In spite of theses difficulties, at the beginning of October, a month after the theoretical vulnerability was announced, a new record was set in the municipal elections in Estonia. Of a total of 582,542 votes, 186,034 were cast online, confirming the trust of the public in eGovernment. ■

INDIA'S UIDAI INTRODUCES 'VIRTUAL ID'

In a bid to address privacy concerns, India's UIDAI (Unique Identification Authority of India) has introduced a new concept of 'Virtual ID' which Aadhaar-card holders can generate from its website and give for various purposes, including SIM verification, instead of sharing the actual 12-digit biometric ID. This will give the users the option of not sharing their Aadhaar number at the time of authentication.

The Virtual ID, which would be a random 16-digit number, together with biometrics of the user would give any authorised agency like a mobile company, limited details like name, address and photograph, which are enough for any verification. A user can generate as many Virtual IDs as he or she wants. The older ID gets automatically cancelled once a fresh one is generated.

From June 1, 2018, all agencies that undertake authentication will have to accept the Virtual ID from their users. UIDAI has also introduced the concept of 'limited KYC' (know your customer) under which it will only provide need-based or limited details of a user to an authorised agency that is providing a particular service, according to sources. ■

NEWS

De La Rue sells majority stake in Portals
De La Rue has sold its banknote and security paper business to Epiris Fund II. De La Rue's paper business, consisting of the Overton and Bathford paper mills in the UK, will be renamed Portals De La Rue (Portals) Limited and sold to a newly formed company Whickerco Limited.

Epiris, together with the management of De La Rue paper business, is buying a 90per cent shareholding in Portals for £61.0m (€69m) payable upon completion. De La Rue will retain the remaining 10per cent interest.

Bundesdruckerei under new leadership
On 1 February and as scheduled, Dr. Stefan Hofschen (50) took over the helm as CEO of Bundesdruckerei GmbH. He succeeds Ulrich Hamann who is retiring after 14 years at the head of the company. Back in May 2017, the Supervisory Board had appointed Dr. Hofschen CEO with effect as of 1 February 2018. Christian Helfrich (CFO) remains the second member of the management board.

For centuries, Ireland was known as a country of emigration. Even now, there are about two million fewer people living in Ireland as there were around 1840. Now, political events that are out of Irish hands, suddenly make Ireland look like a country of immigration.

In most countries and in 'normal' times, the demand for passports is fairly stable, with renewals making up a large part of the total. But these are not 'normal' times, at least not for the British Isles, that is Great Britain and Ireland. Since the UK referendum on membership of the European Union there has been a surge in applications for Irish passports. Many UK citizens want to keep their freedom of movement around the European Union by getting a passport of an existing EU country and the Irish one is an obvious choice.

In 2016 the Irish government pleaded with Britons not to place too much strain on the passport service. Last summer Dan Mulhall, Ireland's ambassador to the US and previously to the UK, said that the extraordinary number of passport applications following Brexit reflected well on Ireland. "People around the world, many of them may be British people living in Europe, living elsewhere, with Irish connections, are looking for Irish passports in order to safeguard their position for the future," he told the *Today* programme on BBC Radio 4.

According to statistics issued by Ireland's department of foreign affairs in early January this year, 779,000 Irish passports were issued in 2017. "This is the highest number of Irish passports ever issued in one year. It represents an increase of over 6 per cent compared to 2016, which was itself a record-breaking year, and an increase of over 15 per cent since 2015," said Simon Coveney, the minister for foreign affairs. Of this total, 81,572 passports were issued in Northern Ireland alone, where everyone born on the island of Ireland has a birth-right, under the Good Friday agreement, to identify as British or Irish. That represented a 20 per cent increase on the number of applications for Irish passports in 2016, when the figure stood at 67 500. Of these, about half were new applications and half were renewals. There was a similar number of applications, 81,287, from Britain, a rise of 28 per cent. At the same time, the number of people born in Britain registering as Irish shot up by 95 per cent.

The scramble for Irish passports in Britain and Northern Ireland has been widely linked to Brexit. However, Simon Coveney, the Minister for Foreign Affairs said that while the UK's impending departure from the European Union was undoubtedly linked to the increase in Irish passport applications, other factors such as increased mobility and population growth were also relevant.

The Passport Service has undertaken what Mr Coveney has described as an "ambitious reform programme to meet the unprecedented demand for passports from Irish citizens at home and abroad", which is also looking at how to "continuously strengthen systems guarding against fraud and protecting the integrity of the Irish passport".

There were 17,800 people entered on the *Foreign Births register* last year. The fastest growing group of registrations was from Great Britain, which grew 95 per cent compared to 2016. As many as six million people living in the UK are estimated to have at least one Irish grandparent. There was also a 33 per cent rise in applications from the United States and a 30 per cent rise from South Africa.

TO BE OR TO BECOME IRISH

Ireland's nationality law is more 'inclusive' that that of many other countries. A person may be an Irish citizen through birth, descent, marriage to an Irish citizen, or through naturalisation. The law grants citizenship to individuals born in Northern Ireland under the same conditions as to those born in the Republic of Ireland. This means that someone living in Northern Ireland, which is a part of the United Kingdom, can choose to be a citizen of the Republic of Ireland without ever having lived there.

Overall, Irish law deems that everyone born on the island of Ireland is automatically an Irish citizen if he or she is not entitled to the citizenship of any other country. Distinct from this is the entitlement to Irish citizenship, which applies when at least one of the parents of an applicant is an Irish citizen or entitled to be one or is a British citizen or a legal resident, etc.

And then there is citizenship by descent, for which at the time of his or her birth, at least one of a person's parents needs to be or have been an Irish citizen. Place of birth is not a deciding factor. Failing that, and subject to registering themselves in the *Foreign Births Register,* anyone with an Irish citizen grandparent, born on the island of Ireland is eligible for Irish citizenship. Dual citizenship is permitted under Irish nationality law. ■

INTERGRAF

ISO 14298

Management of security printing processes

CWA 15374

Security management system for suppliers to the security printing industry

ISO 14298 specifies requirements for the management of security printing processes. The security management system will enhance your organisation's resilience to risk and potential threats. Combined with risk assessment, this strengthens your business.

CWA 15374 specifies requirements for suppliers of products that include security features or for suppliers of services that ensure the physical security of printed matter manufactured by a security printing company, e.g. producers of inks, foils, security paper.

Achieve conformity - Experience value generation - Feel trust

- Secure your processes with the worldwide standards for the security printing industry
- Ensure information security via ISO 14298 as it is in line with ISO 27000
- Support your preferred supplier status and/or tender responses
- Manage and address security risks in your organisation with clear specifications
- Demonstrate how information systems and production processes are safeguarded
- Help to prepare for the unexpected
- Secure market differentiation

INTERGRAF CERTIFICATES CREATE TRUST AND DEMONSTRATE YOUR COMPETENCE