YEAR 21 NOVEMBER 2018 **ISSUE 78**

INFOSECURA

the good the bad and the scary

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

Looking positively but carefully

As the cover of this issue indicates, there is much in our industry that is positive and commendable: The story of how papermaker Portals De La Rue became the first supplier to gain the updated CWA certification is just one. Certification has been a boon to the industry, not only in encouraging management to look at processes and risks, thus increasing efficiency, but also - and even more importantly - in giving customers, both central banks and ID document issuing authorities and banknote and ID document producers themselves, an easy and convenient way of identifying suppliers that they can trust. The Portals De La Rue certification also underlines the fact Intergraf and the "security printers" part of it, is equally concerned with and equally valuable for the banknote and the ID sector. This is an important factor for the success of the "SecurityPrinters Banknotes+Identity", and on pages 4 and 5 you will find a quick overview of the sessions the conference in Copenhagen will offer.

As for the "bad" part, the Europol "Internet Organised Crime Threat Assessment" (IOCTA) gives stark warnings about the threats ahead. Of interest for the industry is in particular payment fraud, but while Europol sounds general warnings, it does not give actual numbers. However, a national report for the UK from the trade body UK Finance does, and if one sets these figures for one country of ca. 66 million people in relation to the about 512 million people of the European Union, which is the field of interest for Europol, it becomes clear that Internet payment fraud dwarfs e.g. counterfeiting of banknotes. This is also the reason for prefacing the IOCTA article with the latest figures on counterfeit banknotes given by the ECB. Of course there is also cash fraud other than counterfeit currency, but the latter is as 'stealthy' as internet fraud, as it is also not usually detected immediately.

To squeeze the advantages and challenges of our industry into the title matrix of the ancient spaghetti western "the Good, the Bad and the Ugly" is a bit of a stretch, but the editor thought that especially the last part, the 'scary' one, that refers to Sweden's possible trial of 'Central Bank Digital Currency' needs examination. So far just about all central banks are committed to offering their populations cash, along with other payment modes. It is, however, prudent to think about the consequences of a cashless society. That does not only apply to Europe, but to China as well.

The main item in the ID document part of this issue is the "Entry/Exit System" for the members of the Schengen area. We still have until 2020 for the system to become operational, but until then, we can expect more criricism of the use of facial recognition technology and the length of time the captured data is kept.

With best wishes for a peaceful and successful 2019

the Editor

A First in Trust

Receiving the very first upgraded Intergraf CWA certification for suppliers to the security printing industry was an important milestone for the newly independent banknote and security paper maker Portals De La Rue in England. But is was important for Intergraf as well, as certifying an important company validates the process and raises its image in the eyes of customers.

(above) Intergraf's Certification Manager Doris Schulz-Pätzold at the hand-over of the CWA certificate to the team at Portals De La Rue. (second from right, CEO Dr Ross Holliday)

In Summer this year, the banknote and security paper maker Portals De La Rue became the first organisation in the world to be audited and certified according to Intergraf's upgraded standard CWA 15374:2018 for suppliers to the security printing industry. The successful certification was the culmination of a process that began with a thorough self-evaluation of management processes within the company, all related to thirteen risk groups and a following audit by an independent auditor.

Portals, which operates a banknote paper mill in Overton in Hampshire, England and a security paper mill in Bathford near Bath, was well aware of the processes of certification and the advantages it brings, not only for optimising internal management procedures and being certain to have covered all possible risks the company faces vis-a-vis their customers, but also in providing their customers with complete certainty for soundness of paper supply for their own operations. Until February 2018, Portals De La Rue was part of banknote printer De La Rue, a company certified according to Intergraf's ISO 14298 certification, and was therefore well acquainted with the procedures and the advantages of certification.

In early July, the audit was done in both Overton and Bathford and a little later the CWA certificate was granted. A few days later in Overton, Intergraf's certification manager Doris Schulz-Pätzold handed the certification document to Portals' CEO Dr Ross Holliday and his team, including Risk Director Terry Stears.

"Security is paramount at Portals, so we are thrilled to be the first organisation in the world to be certified for Intergraf's prestigious CWA 15374:2018 accreditation," said Terry Stears, Director of Risk at Portals. "Whilst we have always been committed to delivering to the highest possible security standards, this certification means our customers can be confident we are going above and beyond to meet the extremely high standards of the security printing world." He continued: "The Portals' mills in both Overton and Bathford have proven that their efficient quality management meets the highest possible standards of the security printing world and that they comply with all aspects of Intergraf's strict certification criteria."

CERTIFIED TO MANAGE ALL PLAUSIBLE RISKS

Intergraf currently uses two auditing organisations, one, VPGI, is based in the Netherlands and the other, SQS, in Switzerland. Intergraf's CWA 15374 certification programme was upgraded in early 2018 to take account of evolving risks within the industry supplying security printers. After an intensive revision, the new CWA standard was published in May 2018. The adjustments were established on the basis of contemporary ISO standards with regard to both risk-based thinking and continuous improvement.

CWA 15374 has been set up by Intergraf and CEN (European Normalisation Centre) in 2005 in order to give security printers and their customers the assurance that the suppliers they use, follow the same rigorous risk management procedures as they do themselves. The certification system CWA 15374 is therefore similar in the aims but different in details from the ISO 14298 certification for security printers. CWA 15374 has two categories for certification: MS Suppliers of security machinery / software and SC Suppliers of security components (for example cylinders, foils, inks, laminates, security paper, lamination plates and printing plates, polymer, e-covers for passports, etc.).

The reviewed and upgraded documentation, the *Normative Document* and *Certification Requirements* take greater account of the latest technical developments and are more in line with the risk-based ISO 9000 system and thus also with the ISO 14298 Standard. Both documents are already in force and will be the basis for the next audits. There is a transition period to help companies to adapt to the new system. In January 2019 CWA 15374:2018 will officially replace the former version.

ISO 14298 FOR SECURITY PRINTERS

The main purpose of the CWA certification is to secure the supply chain for security printers. There

are a total of 122 production sites that were certified the world over. 15 companies were certified according to CWA 15374 but 107 companies in 48 countries were certified according to ISO 14298. The latter companies are security printers and hologram manufacturers and they produce banknotes, passports, ID cards, holograms, driving licenses, postage stamps, certificates, tax stamps and breeder documents. There are three certification levels; *Fundamenta*l or NG level, (non-governmental) for printers supplying commercial products for governmental organisations (29 companies), *Governmental* or G level, as above but with additional requirements (51 companies) and finally *Central Banks* or CB level (27 companies), for printers supplying central banks, credit card issuing and ID/passport issuing authorities.

Like the CWA certification, ISO 14298 refers to risks that a company contemplating certification has to identify and secure. The risks, 13 in total, refer to customers, information, security material, product and waste, supply chains, physical intrusion and access, personnel, disaster, security failure, security management, use of machinery, sales of equipment, transportation and any additional security related risk unique to the organisation. The list of risks to evaluate is certainly large and comprehensive. It covers 69 pages, 13 chapters and 99 items.

THE PROCEDURE

ISO 14298 is based on the idea of continual improvement. Therefore there is not only one certification audit, but in the following two years there is control audit 1 and control audit 2. The validity of the certificate is three years.

The process of certification begins with contacting Intergraf at *certification@intergraf.eu* and with buying the ISO 14298 standard from ISO (www.iso.org). Intergraf then sends the application form, which has to be returned with all requested documents for screening by Intergraf. If the certification request is accepted, Intergraf sends the *Intergraf Certification Requirements* and the *Implementation Guidelines,* which are not publicly available. The next step is to schedule an audit with one of the two accredited auditing organisations, pass the audit successfully and receive the certification. The procedure is the same for both the ISO and the CWA certification.

Since the idea of certification was first discussed in 2001 and as CWA 14641 implemented in 2003, followed by CWA 15374 for security suppliers in 2005, certification has gained general acceptance in the security printing industry and among customers. There was a further gain in acceptance when the European CWA format was transposed to the international ISO format in 2013. The advantages are easy to see: the certified company can be assured to have a system in place that meets even the most stringent requirements of its customers, while the customers can rest assured that they can trust the processes of their suppliers - often without having to conduct lengthy and expensive additional audits. Increasingly Intergraf's CWA or ISO certification is asked for in important tenders.■

SECURITY PRINTERS 2019 IN COPENHAGEN: AN UPDATE

SecurityPrinters Banknotes+Exhibition will start with a plenary session for all delegates and then divide into two parallel streams, one for those interested in banknote issues and the other concentrating on ID questions. Here is a short overview of the sessions which are alternately for ID or banknotes:

Wednesday 23/10/2019: Plenary
Banknotes and IDs: combating crime in a digital world
Counterfeiting has increased in complexity with the availability of raw materials on the Internet – but the security of banknotes and IDs have incrementally improved with new, advanced technologies. This session will explore the latest counterfeit deterrent technologies and fraud trends, including the impact of cybercrime and the darknet on the production and availability of counterfeits and the opportunities for industry and academia to raise the bar against crime as a service.

Thursday 24/10/2019
Session 1 - Banknotes: there's an app for that!
Mobile apps in the banknote world have two distinctive uses: communication and authentication. This session will explore how they work, what they can do, and the restrictions that exist today.

Session 2 - Help! My country's ID document has been compromised
The latest forgery techniques and counterfeiting trends – and how to combat them – will be highlighted in this session. Can the Internet of Things and Artificial Intelligence enhance ID documents and their use, or do they present another threat?

Session 3 - Enhancing the security ecosystem
This session is an opportunity for law enforcement agencies, central banks and academia to address initiatives and solutions – beyond traditional approaches – to deter counterfeiting, and to present specific measures to thwart criminal actions.

Session 4 - Identification beyond documents
While identification is still based on physical documents, virtual identities will play an increasing role. We will explore mobile identity, biometrics, blockchain and other means of digital verification of identity and ID documents.

Session 5 - Going digital: risks and opportunities
Digital currencies present regulation and authentication challenges that must be addressed. We will discuss the future of cash as a legal tender and digital currencies from the perspective of law enforcement, central banks and digital cash brokers.

Session 6 - From cradle to grave
ID documents accompany citizens throughout their lives. This session will provide a holistic view of the ID document lifecycle – encompassing dynamic identity, data capture, issuance, use and verification … and how these functions could be improved.

Session 7 - Cash cycle: the infrastructure of the future
The growing demand for cash worldwide presents an ever-increasing need to modernise the global cash cycle infrastructure. This session will examine recent developments including authentication software, equipment enhancements, and cooperation and shifts in responsibilities between public and private sector partners.

Session 8 - Innovation and interoperability
Innovation and creativity never cease, but conflicting interpretations of international standards can make the role of document examiners very complicated. We will present new documents and how they are complying with standards to facilitate their authentication.

Friday 25/10/2019
Session 9 - The future: new trends, new ideas, new leaders, new approaches
What are the new, fresh approaches to production and the management of the banknote lifecycle. This session will unveil the latest trends, innovations, and new developments in banknotes.

Session 10 - What's in your face?
Facial recognition and other forms of biometrics are playing increasingly important roles in identification. This session will explore the advantages and challenges associated with these technologies.

Panel - The impact of changing ownership structures on the banknote supply chain
The banknote supply chain is undergoing massive changes: cost cutting, mergers and acquisitions of printers and papermakers and the delocalisation of manufacturing operations. How does this affect long-standing customer relationships, business continuity management, and business decisions? Is this trend increasing the efficiency of the industry or undermining its core values?

Panel - Crossing borders and boundaries
Managing borders in the face of growing numbers of travellers, immigrants and refugees is challenging. This panel will discuss the streamlining of border crossing systems, how best to identify and track refugees, and innovative ideas to tackle the borders of the future. ■

ECB UNVEILS €100 AND €200 NOTES

Security features: some old, some new

In September, the European Central Bank (ECB) unveiled the new €100 and €200 banknotes, which will enter into circulation on 28 May 2019. After the €5, €10, €20 and €50, the €100 and €200 banknotes are the last two denominations of the Europa series, and therefore mark its completion.

The new €100 and €200 banknotes use new and innovative security features. One is the satellite hologram at the top of the silvery stripe, which shows small € symbols that move around the number. The silvery stripe also shows the portrait of Europa, the architectural motif and a large € symbol. They also feature an enhanced emerald number that shows € symbols inside the numerals.

The new €100 and €200 notes are a different size to the old €100 and €200 notes. Both denominations are now the same height as the €50 banknote. However, their length remains unchanged – the longer the note, the higher the value. Since the €50, €100 and €200 banknotes are now the same height, they can be more easily handled and processed by machines. They will also fit better in people's wallets and last longer, as they will be subject to less wear and tear.

In addition to the security features that can be seen with the naked eye, euro banknotes also contain machine-readable security features. On the new €100 and €200 banknotes these features have been enhanced, and new ones have been added to enable the notes to be processed and authenticated swiftly.

As ECB Executive Board Member Yves Mersch emphasized in his speech unveiling the new banknotes, that with the changeover to the new €100 and €200 the entire set of euro banknotes will continue to offer strong protection against counterfeiting. This makes euro banknotes even more secure, but also easier to check and handle.■

The will of the people

The £50 note, said to be the least used of all four sterling denominations, is getting a new face. Since 2011, the inventive power of Matthew Boulton and James Watt - he, of the steam engine - jointly reminded Britons (and tourists and crooks) of the industrial might of the British empire. The new face on the new polymer note will remind users of the UK's scientific prowess. And there is even a chance that a woman will be chosen.

Among issuing departments of central banks and banknote printers, who or what graces the face of newly issued banknotes matters a lot. It apparently matters quite a lot to people using these banknotes as well, although that may not be universally acknowledged. It seems to be a popular subject in Great Britain. In September, an article in the magazine *The Economist* delivered a gentle - and very British - put-down by writing that there are "few things more controversial - and less consequential - than the design of a national currency."

The article talked about the coming UK £50 note, for which the Bank of England has started a public consultation to determine who will appear on it. It may hardly seem to matter, the article continues, as the £50 is not only the largest, but also the least used UK denomination, used mainly by crooks and tourists. And as only about a third of all purchases in the UK are made with cash, and cash purchases are expected to fall sharply, why not turn paper - or now plastic - Pound Sterling into collectors' items, with £85 bearing the image of George Orwell, a £60 depicting the Beatles, etc.?

The article seems to imply that it would be sensible to abolish the £50 or even cash altogether, without looking at what this would entail. *The Economist* is not usually given to whimsy journalism and easy laughs and perhaps in the future, we can expect an article looking seriously at what would happen when a country gives up on cash and leaves issuing of money totally in private hands. What is certain is that the card companies would laugh all the way to the bank.

The Economist's opinion also does not tally with that of the Bank of England, which said that demand for the £50 note is continuing to rise. There are 330m £50 notes in circulation with a combined value of £16.5bn. A study by the Reserve Bank of Australia from Spring this year, compared the growing demand for high-denomination banknotes in Australia, Canada and the United Kingdom. where demand for cash has been growing overall, but have reached a 50-year peak for the highest denominations: the AUD 100, CAD 100 and the £ 50. The RBA looks at various hypotheses including the correlation between financial uncertainty and the hoarding of cash, overseas demand for foreign currency as well as government and central bank policies. It also reveals a little reported UK peculiarity: In the UK, £50 were mostly dispensed at London ATMs, but rarely beyond. Now that some ATM operators have calibrated their machines to dispense these notes, demand has risen.

Meanwhile the Bank of England's Chief Cashier, Sarah John insists, that "developing a new £50 note is an important step to ensure we can continue to provide secure banknotes that can be used with confidence." Her boss, Bank of England Governor Mark Carney said that "the new £50 will celebrate the UK's contribution to science. There is a wealth of individuals whose work has shaped, how we think about the world and who continue to inspire people today. Our banknotes are an opportunity to celebrate the diversity of UK society and highlight the contributions of its greatest citizens. (We) look forward to hearing from the public as they think science and put forward their nominations."

The press has of course speculated who these individuals, who shaped the UK's thinking about science, are. *The Guardian* ran a full article on the possible contenders with Lord Byron's daughter Ada Lovelace, a 19th-century mathematician known as the "grandmother of computing", an early frontrunner, alongside Stephen Hawking and Nobelprize winner Dorothy Hodgkin.

Governor Carney's speech marks the beginning of the public consultation period, which will end on 14 December 2018. The Governor will then make a choice from the shortlist and the final decision will be announced in 2019 alongside a concept design for the new note. The next new banknote to be issued in the UK will be the £20, bearing the likeness of the 18th/19th century painter JMW Turner, which will be issued in 2020.

In the USA, the question of who will feature on the new $20 note, if and when it will be issued, has been kicked into the long grass. The favourite to replace controversial President Andrew Jackson, blamed for the removal of native Americans from the South-Eastern USA to Oklahoma in the 'march of tears', was anti-slavery hero Harriet Tubman. In 2016 this choice was approved by then US Treasury Secretary Jacob Lew, but President's Trump's Treasury Secretary Steven Mnuchin said after taking office that the new $ 20 note was not one of his priorities. There has been silence on the matter ever since. ■

Sweden: getting serious about CBDC

Putting the faces of very popular and near contemporary people on banknotes did not persuade Swedes to use cash more. Now the Riksbank contemplates e-Kronas.

When the Governor of the Bank of England launched the public consultation on the face on the new £50 note, he also announced the subject of the Bank's next 'listen to the public" round, which it calls *Future Forum*, in which all the governors will host their own virtual live Q&A sessions. He said the theme of this year's Forum will be: "Let's decide the future of money".

Getting British people involved in thinking about the future of money is laudable, and it will of course be about the future of paper - or polymer - money. However, in this the Bank of England is a bit of a latecomer to the discussion. In 2017, the Bank of Finland published an extensive study on a central bank-issued alternative, *Central Bank Digital Currency (CBDC)* in its BoF Economic review (see Infosecura 75). It first reminded readers of the basics of cash, which are namely that 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.

The Bank of Finland study looked into the theory of CBDC while the Swedish Riksbank went some steps further by starting an "e-Krona" project, which published its first report in 2017. The second report on the project has been published at the end of October 2018.

DECISION TIME FOR THE SWEDES

The Swedish Riksbank finds itself in a difficult situation. It has a statutory duty to promote a safe and efficient payment system, and has for 350 years supplied the Swedish public with money. Increased digitalisation means, however, that the use of cash is declining and in Sweden its falling quite rapidly. In the Euro area as a whole the value of cash as a percentage of GDP is just over 10 per cent, while in Sweden is just over one per cent. Half of the retailers in Sweden believe that they will stop accepting cash in 2025 at the latest, as it will ultimately become too expensive to accept cash if use continues to decline. Since the first e-Krona report in 2017, the percentage of respondents saying that they paid for their most recent purchase in cash has declined from 39 per cent in 2010 to 13 per cent this year.

If it believes that Swedes genuinely prefer digital money to physical - paper - banknotes, Riksbank has to decide how to meet its responsibility towards the general public. There are two ways to go: it can either choose not to react to developments on the payments market and pass responsibility for means of payment to the private sector, or it can choose to continue supplying a means of payment to the general public in a new digital form.

As the second report of the e-Krona indicated, the Riksbank has chosen the second path and is continuing to develop the legal, operational and technical aspects of CBDC, without committing to finally issuing it.

THE CHARACTER OF CASH

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. It can be useful to go back to the Finnish study to see which criteria CBDC would need to meet:

- 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.

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 for saving 'under the mattress'. Card payments, credit transfers and direct debits are not assets as such; they only provide access to the payment system where settlement takes place.

THE PROPOSALS OF THE E-KRONA PROJECT

Now let's see what the e-Krona study proposes. The first report had already set out the two possible forms of CBDC - where e-Kronas can either be held in an account at the Riksbank (account-based) or be stored locally, for example on a card or in a mobile phone app (value-based). Both cases require an underlying register to record transactions and safeguard the rightful owner of the digital krona and to make these digital transactions traceable. This will not satisfy the demand for anonymity nor that for no third party involvement, but it is unlikely that the public would object.

Given the bind the Riksbank finds itself in, and in anticipation that it might need to act soon, the project proposes that it should begin to design a technical solution for an e-Krona in order to test which solutions are practical and possible to realise. This would offer the public continued access to central bank money. It would also, the report believes, ensure that payments work in crisis situations, as the private market cannot be expected to take all the responsibility for this. In addition, the project suggests that the Riksbank draws up proposals for legislative amendments that are needed to clarify the Riksbank's mandate and an e-Krona's legal standing.

In a possible totally digital payment market, all means of payment accessible to the general public are issued and controlled by private agents. If the state, via the central bank, does not have any payment services to offer as an alternative to the strongly concentrated private payment market, it may lead to a decline in competitiveness and a less stable payment system, as well as making it difficult for certain groups to make payments. Ultimately, it may also risk eroding basic trust in the Swedish monetary system. Some of these problems could be neutralised or mitigated by an e-Krona.

The e-Krona could offer a competitively neutral infrastructure, which payment service providers can join if they wish to offer services to households and companies. In an aging society such as Sweden, there are groups that are having problems as cash use declines, because they find it difficult to use digital payments for one reason or another. As the private market is unlikely to satisfy these groups, the state could help by designing a simple and user-friendly e-Krona or by legislating and regulating to force the private sector to take greater responsibility.

To make it possible to use e-Krona in physical shops or online, the e-Krona platform with its underlying register needs to interact with a number of other systems and agents. Banks and other companies need to be able to join the e-Krona platform in order to develop payment services to households and companies. Systems also need to be developed to check for money laundering and to link to a settlement system so that e-Krona can be moved into and out of the platform.

MONETARY POLICY AND FINANCIAL STABILITY

How monetary policy and financial stability will be affected by the e-Krona depends on how large demand for an e-Krona will be, which in turn will depend on how the e-Krona is designed. The report concludes that should there be a substantial demand for e-Krona and wide spread availability, it would be prudent to control its demand. For this purpose, interest rates and other tools could be used to limit possible negative effects on the efficiency of monetary policy and financial stability.

A very low take-up of e-Krona would have only minor effects on the financial system. Banks might perhaps receive slightly fewer deposits and therefore have to obtain slightly more wholesale funding. In a financial crisis, when the public wants to withdraw large amounts from struggling banks, the e-Krona could make the change from the banking system to state-guaranteed money both easier and quicker than a traditional run from the banking system to cash. However, the Riksbank already has tools to be able to cope with such situations if they were thought to pose risks to financial stability.

THE PROPOSAL

So far all considerations have been completely theoretical, without a line of code having been written. Now the project proposes that the Riksbank initiate a pilot programme to develop one or more possible technical solutions for a comprehensive e-Krona concept that provides the bank with greater room for manoeuvre and knowledge prior to deciding whether to issue an e-Krona or not. The proposed focus of this programme should be on developing an e-Krona that constitutes a prepaid value (electronic money) without interest and with traceable transactions. An account-based e-Krona requires coordination with other central agencies. It is therefore reasonable for any e-Krona system for account-based krona to be built in agreement, and perhaps even in partnership, with other agencies. A Swedish position on digitalisation on the payment market should also be drafted. The project proposes that the Riksbank initiate a cross-agency dialogue on this issue.

A DIFFERENT TAKE ON RISKS

A slightly different take on the risks of CBDC is provided by a white paper on digital money by Giesecke & Devrient, in as far as it describes a potential new role for central banks. If large numbers of people decide to hold their short-term liquidity in default-free, fee-less digital currency schemes instead of depositing it at a bank and if employers would agree to pay salaries directly into the digital wallets of employees, who could easily pay all their bills from their digital wallets, many people would probably no longer want to have bank accounts. Central banks would find themselves thus acting as substitutes for commercial banks and payment system providers. In the extreme case, this could lead to a one-bank system. It is questionable as to whether central banks are able or willing to provide basic financial services to the public. The White Paper states these services would probably have to include credit assessments, etc.

Many countries also have regulations that limit the amount of cash that can be transferred out of the country without it being declared. In the Eurozone the amount is €10 000. Any digital currency would – by design – be global, i.e. it could be easily moved around the globe, stored in the cloud or a distributed ledger and accessed from everywhere in the world. Even though technical solutions to prevent this are conceivable, control over cross-border money transfers would need to be considered when designing a digital currency, the White Paper suggests. The warnings of the G& D white paper presuppose oversubscription, while a more likely scenario in the Swedish case would be undersubscription.

AND FINALLY

Perhaps, when evaluating the chances of the e-Krona project, which from the viewpoint of the Riksbank is urgent, we should look at why non-cash payments in Sweden, and in other countries, are so popular. Using a card or smartphone app is convenient. You are not confronted with a visibly shrinking amount of cash in your wallet. You are usually unaware of how much money you have available anyway, as even if you overdraw your limit slightly, there is a reserve sum. Cards and payment apps give freedom of action, which all but 13 per cent of Swedes preferred to seeing the cash in their wallet shrink with every purchase. Thoughts of how this may affect the policies of the central bank or any other such opaque considerations will not enter many shoppers mind's.

In contrast, the proposed e-Krona does not offer such soft options. If you load 100 Krona onto your e-Krona card and you want to make a purchase of Skr 110, you are out of luck. Just as with cash. You can't overdraw. So, why would you choose e-Krona? The account-based version might be more flexible, but we don't know yet. However, even a low-take-up e-Krona scheme may have its merits. Discounting any large-scale take-up, as per G&G White Paper, it could function as a low-maintenance and low-cost backstop for groups unable to use conventional non-cash payments and it could be there in the wings in case the commercial money providers fail, for whatever catastrophic reasons. One key feature of e-Krona must be that it is voluntary. Yet it will take a very large educational effort to convince Swedes to put the final integrity of their financial system ahead of convenience.

There is another - unlikely - possibility. By law, Swedish merchants must accept cash, but Sweden's commercial law allows shops to overrule the central bank law if they display a sign saying that cash isn't accepted. Customers are then assumed to have entered into a legal agreement to exclusively use electronic payments. A repeal of this law (or custom) would be unpopular, but it would perhaps solve a problem. E-Krona, in the end, may ease some problems, but in the event of a natural catastrophe or an act of war, when the electricity grid would be knocked out, it would be every bit as useless as the other e-currencies, unlike dear old physical cash. ■

ATMS - THE FIRST TO GO, CASH TO FOLLOW

The highstreet battles in the war on cash are being fought around the ATMs in small, often rural towns all over Great Britain. The final goal of the attackers is to do away with cash completely.

Sweden's Riksbank's second report on Central Bank Digital Currency states that it is difficult to determine with any certainty why the use of cash is declining. It writes that this development is mainly because digital payment forms are perceived as more convenient and easily accessible. The development does not appear to be because access to cash has deteriorated. In 2016 there were just as many ATMs as in 2006, just over 2,800 across Sweden, but the general public chose to withdraw ever smaller amounts from them. It therefore cannot be said that it has become more difficult to get hold of cash through ATMs in Sweden.

The picture in the UK seems to be quite different

from that in Sweden. While in the UK, the main reason for the trend towards cashless is doubtlessly convenience as well, there are also more troubling reasons. As *The Guardian* in late October wrote, access to cash is becoming a challenge in some parts of the UK, forcing retailers to increase prices, affecting low-income households. Nearly 3,000 bank branches have closed across the UK since 2015 and ATMs disappeared at a rate of 500 a month in the first half of this year, according to a survey by *Which?* – a six-fold increase since last November. More than 130 communities, many of them in poor areas, now have no ATM and the 2.7 million Britons who rely entirely on cash are being increasingly shut out of essential services. Banks and regulators blandly say that it is consumers themselves that drive the digitalisation of money, but consumers are usually unaware that they also foot the bill. Credit and debit card payments cost traders on average three times as much as cash because they have to pay a service charge to the bank that processes the payment. Part of that, the interchange fee, is passed to the card issuer (e.g. Barclays Bank, etc.) and most of the rest, the scheme fee, goes to Visa or Mastercard.

Spending habits - and not only in the UK - are being monopolized by the two US companies, Visa and Mastercard. According to forecasts, by 2026 they will control 90 per cent of the total UK electronic payment sector. Both companies receive a cut from every transaction using their cards and both have openly declared a war on cash.

When in 2015, the EU capped interchange fees and, this year, banned traders from recouping the cost through a surcharge on card transactions, Visa and Mastercard quietly doubled their scheme fees. Businesses now pay nearly £1bn a year more in these charges than in 2015, the *Guardian* writes and continues: “Ajay Banga, chief executive of Mastercard, has declared “my enemy is cash”, while Al Kelly, boss of Visa, told an investor conference last year that “we are focused on putting cash out of business and getting more and more consumers into the payments market through more and more transactions on Visa cards”.

“Visa and Mastercard’s main objective isn’t to win ATM market share from (UK ATM operator) Link, but to drive consumers away from cash by killing off ATMs,” says Mark Falcon, former director of regulation and strategy at the Payment Systems Regulator (PSR). “This is because card payments generate much higher fees than cash and ATMs.”

The UK Financial Inclusion Commission said that 1.5 million adults in the UK do not have a bank account – some, like recently arrived immigrants, because they lack the paperwork to open one. More than half of the 2.7 million people who rely mainly on cash have a household income of less than £15,000. Many of the best deals for utilities, telecoms and even train tickets are only available online to cardholders, while universal credit will only be transferred to a bank or building society account, without the previous option of cash cheques redeemable at post offices.

Visa and Mastercard claim their motives for eliminating cash are altruistic, since poor countries are disadvantaged by the costs of handling cash. It is the poor, however, who are paying the price of an increasingly cashless society. ■

WHERE IS THE NEW RS 100?

If you can’t get hold of the new Rs 100 banknote, here is what the main motif, the Rani ki vav looks like.

In July this year, the Reserve Bank of India announced that it would “very shortly” issue a new 100 rupee note. It also published an image of the note - the normal Mahatma Gandhi portrait on the front and a picture of Rani ki vav, a spectacular stepwell in Gujarat, on the back. The new colour is lavender. The RBI never bothered to define “shortly” and although sightings of the new note were reported from Bengaluru in Karnataka (south India), in the capital Delhi, up until the last days of October, no one had seen the new note. But in November, the website of the RBI blandly showed the Rs 100 as being among the notes in circulation. But where is it?

An article in the Indian news site IANS gave a possible explanation. The new note is supposed to be a little smaller than the (green) Rs 100 it replaces. “This means that all the 237,000 ATMs in the country would again have to be re-calibrated to dispense the new Rs 100 notes. This entails a massive effort which is both time-consuming and adds to our costs,” the Confederation of ATM Industry (CATMi) director told IANS.

It is said that even the recalibration of the new Rs 200 notes introduced last year is still not completed in all ATMs, so recalibration of the new Rs 100 notes could take even longer unless planned properly.

India has among the lowest ATM penetration globally, averaging 8.9 ATMs per 100,000 population, compared to Brazil’s 119.6, Thailand’s 78, South Africa’s 60 and Malaysia’s 56.4. China currently has around one million ATMs, which will touch 1.5 million by 2020.■

A CLUTCH OF ANNIVERSARIES

A recent study by McKinsey found that the average lifespan of companies listed in Standard & Poor's 500 is less than 18 years. Companies that practise security printing in some form, such as printing banknotes or identity documents, seem to be made of hardier stuff. In 2003, the Dutch security printer Royal. Joh. Enschede in Haarlem celebrated its 300th anniversary in grand style. Even the Queen of the Netherlands came to congratulate.

PWPW

The three companies that celebrate important milestones this year and next, however, cannot expect royal blessings. The youngest of the three, Polska Wytwórnia Papierów Wartosciowych, the Polish Security Printing Works, will celebrate its 100th anniversary on 25th January 2019. On that day in 1919, the new Polish Republic established the State Graphic Works and one year later, the first banknote of 100 Polish marks was isued. In the twenties, the State Graphic Works were transformed into a joint-stock company under the name Polska Wytwórnia Papierów Wartosciowych.

The occupation period during the Second World War was the most heroic and dramatic time in the history of PWPW. Its building sheltered "Agaton" – a clandestine unit of the Home Army (AK) composed of the employees of PWPW, who secretly produced banknotes and legalisation documents for the Polish underground state. In the Warsaw Uprising, 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 Sanguszki Street, which was defended at that time by as few as 200 insurgents. After a pitched battle for every floor, the insurgents left the building one day later. During 27 days of fighting, almost 100 insurgents were killed in the building.

POST-WAR PERIOD

The reconstruction of PWPW's bombed building started in 1946, while production of banknotes and documents was moved to Łódz. In 1950 the production was moved back to Warsaw. In 1975, the first banknote in the series of "Great Poles" was printed – 500 złotys with the image of Tadeusz Kosciuszko. The last of the series was the banknote of 2 million złotys with the image of Ignacy Jan Paderewski. Since 1998, PWPW has been printing banknotes of the new series, i.e., "Polish Sovereigns".

The end of the nineties of the 20th century and the first decade of 21st century at PWPW was the time of dynamic growth, of new digital competencies, investments in new products and successful undertaking of export activities. Today, PWPW is one of the most modern companies in the security printing sector in Europe.

GOZNAK

The second oldest security printing company to celebrate an anniversary is the Russian company Goznak, which was founded in Saint Petersburg in September 1818 through a decree of Zar Alexander Ist under the name *Expedition of Storing State Papers*. The Saint-Petersburg Mint was established even earlier, in 1724 during the reign of Zar Peter the Great. Many outstanding scientists, inventors, engineers and artists contributed their talent and labor to the development and prosperity of the Expedition of Storing State Papers, among them I.I. Orlov, whose invention is still applied in security printing all over the world. After the October Revolution of 1917, the company was reorganized and renamed Goznak (short for *Gosudarstvennyi znak*, literally State Ensign or Insignia).

From the start, Goznak was a totally integrated company, including paper mills, research departments, design departments and later, even inventing banknote counting machines. During the 2nd World War, the Leningrad Mint and Paper Mill, as well as the Moscow Printing Factory were evacuated to Krasnokamsk near Perm, where work continued.

Today "Goznak" is the Russian market leader for security technologies and solutions. It is a dynamically developing company, successfully competing on the world market. Goznak is also one of the strategic enterprises of the Russian Federation.

Goznak incorporates eight enterprises, two printing factories, two paper mills, two mints, a printing house and an R&D institute.

ORELL FÜSSLI

The third company to celebrate is the most ancient. In 2019 security printers and book publishers Orell Füssli will commemorate the founding of the company in 1519. That year, Christoph Froschauer, a printer from Bavaria, moved to Switzerland and later became a citizen of Zurich. In 1531, his print shop printed the Folio Bible, also called the Zurich Bible and later the company extended to incorporate a bookshop, a publishing company and in 1780 a newspaper. The first securities were printed in 1827 and the first banknotes for the Swiss National Bank followed in 1911. Orell Füssli is planning a year-long celebration with many cultural and artistic events, details of which will be made public over the next year. ■

CASHLESS EXPANSION?

China's Belt and Road Initiative: How to win friends and influence peoples.

China is a surprizing champion of cashless payments. Will it use its huge banknote printing capacity - if surplus - to upset international banknote printing markets?

Cash has been rejected for some consumers in tourist attractions, restaurants, retailers and other industries. This damages the legal status of the national currency, and hurts consumers' rights to choosing payment methods.

This complaint may be familiar to people in Sweden, Denmark or even some remoter locality in the UK, but it comes from a notice posted on the website of the People's Bank of China (PBoC), China's central bank. As the South China Morning Post (SCMP), an English language newspaper in Hong Kong, owned by e-commerce giant Alibaba, which in turn owns Alipay, reported this summer, the central bank tried to dial down what it calls an "overhype" of a cashless society, as mobile payment volumes continue to soar to new heights. They reached a record 81 trillion Yuan (US$12.8 trillion) from January to October last year, figures from the Ministry of Industry and Information Technology show. Payments via mobile-phone apps such as WeChat Pay and Alipay made up over 80 per cent of China's mobile payments. The PBoC insisted, cash should be accepted at all business outlets, with the exception of e-commerce and unstaffed stores. The bank was not just asking nicely. Shops had one month after the announcement to make necessary changes or face being investigated for breaches by the authorities.

The flight from cash seems to have had one undisputed positive effect: The SCMP said that for decades, China was awash in counterfeit banknotes, a problem that mobile payments have effectively resolved. Officials have described cashless mobile payments as one of China's "four great new inventions in modern times", along with dockless shared bicycles, high-speed trains and e-commerce.

THE POSSIBLE KNOCK-ON EFFECT OF CASHLESS

One consequence of the amazing turn to cashless modes of payments is that China no longer needs to print vast amounts of Yuan banknotes. On August 12, the SCMP, claiming that "sources in the China Banknote Printing and Minting Corporation (CBPAMC) confirmed that production plants across the country were running at near full capacity to meet an unusually high quota set by the government this year." And apparently that quota was not for the production of domestic currency but to deliver on international contracts, mainly for countries that had signed up to China's ambitious "belt and road plan", which Beijing launched in 2013 and that involves large-scale infrastructure projects in 60 countries from Asia, Europe and Africa, to stimulate economic growth - and to increase China's influence.

That sounded plausible, but was it? When the president of the CBPAMC, Liu Guisheng, was quoted as saying that his company has since then "successfully won contracts for currency production projects in a number of countries including Thailand, Bangladesh, Sri Lanka, Malaysia, India, Brazil and Poland", he was quickly corrected by the Indian Ministry of Finance, which said in a statement: "Reports about any Chinese currency printing corporation getting any orders for printing Indian currency notes are totally baseless" The claim that China printed banknotes for Poland seems also highly unlikely, especially considering that Poland has a very good banknote printing works, PWPW.

The article in the South China Morning Post was picked up by an Australian news organisation; news.com.au, which recounted that China only recently started printing overseas currency. The first order came from Nepal in 2015, when Nepal Rastra Bank ordered 200 million 1000 Rupee notes. Nepal Rastra Bank CEO Bhuban Kadel enthused to Chinese news agency Xinhua: "The quality is as good as the ones printed earlier in another country but the cost is less than half of the amount we had earlier paid." That again sounds plausible, but high-level sources at two prominent European banknote printers said that that was the first and so far only banknote printing order outside China that CBPAMC managed to pick up and Nepal quickly reverted to the original supplier. One printer said that China is not active on the international banknote printing market but added, that if China really wanted to become active there, it could cause considerable problems for established private suppliers. However, so far it has not done so.

The thoughts of Prof. Hu Xingdou, an economist at the Beijing Institute of Technology, quoted in the Australian article, perhaps give an indication why China might be eager appear to become a trusted banknote producer for other countries: "The world economic landscape is undergoing some profound changes," he said. "As China becomes bigger and more powerful, it will challenge the value system established by the West. Printing money for other countries is an important step. Currency is a symbol of a country's sovereignty. This business helps build trust and even monetary alliances."■

CHINA: UNEQUAL BENEFITS

China's digital payment systems are racing ahead to take the whole country cashless. But in the rush they overlooked 200 million people that are still unbanked. It will be tough to get them all on board.

The concerns of Britain's central bank, regulators and the public regarding the difficulties of the poor and unbanked in an increasingly digital payment environment are dwarfed by the concerns for the poor and unbanked in China. A recent report in the US journal *Foreign Policy* by Rui Zhong, said that the growing "cashlessness" of Chinese cities threatens to create underlying issues of economic instability. Mobile payments expose fault lines between young and old, the urban middle classes and the poor in rural areas and those that want to come to cities. Municipal and provincial governments have also initiated moves to push digital payments and often mismanaged such moves, which could lock the elderly and the poor out of the 'consumption economy' - just when the Chinese economy needs as many spenders as possible.

While realities are created on the ground, regulators debate whether mobile payments can legally substitute the Renminbi and whether local "cashless city" schemes violate China's Renminbi Management Regulations, which define the Renminbi as "the legal currency of the People's Republic of China". That law says that "within China's national borders, the usage of Renminbi for transactions by work units or individuals cannot be revoked." (Renminbi means "people's currency" and Yuan is a unit within it. Both words are more or less interchangeable.)

But while regulators talk, cashless payments are rising, from 57.7 per cent to 67.5 per cent of transactions from the end of 2016 to the end of 2017, the China Internet Network Administration Center reported. The rise until the end of 2018 will be similar. In cities, whether in large brand-name shops or in street food-stalls, colourful QR Code stickers near cash registers from Alipay and Tencent - China's two giant Internet firms, which dominate online payments - are ubiquitous.

The payment-providers do much to increase business by organizing promotional events and municipal lobbying initiatives, mainly in cities. There are "shopping holidays", "cashless city weeks" and annual "cashless days", offering big discounts for purchases paid for cashless. In many cities, cashlessness is so common that even beggars and street musicians use WeChat and Alipay QR codes to ask for change.

A very equal society could cope with such developments, but Chinese society is not equal. The 2017 World Bank Global Findex database estimated that some 200 million Chinese rural citizens remain unbanked, or outside of the formal financial system and are thus unable to join the mobile payment platforms that WeChat and Alibaba host. Other sources say close to 70 per cent of rural Chinese remain offline and unable to use mobile payments. As these digital platforms attempt to become the default form of payment, China is facing a critical challenge to get its unbanked citizens brought up to financial inclusion standards. There are communities that are cash-only and new invoicing systems transitioning to cashless ones without consulting rural communities or individuals, would make buying and paying for agricultural equipment, seeds, and other purchases for farming impossible.

Even as regulators and finance analysts worry about these gaps, Alibaba and Tencent remain determined to push cashlessness further into everyday life and they are making rural China another area to conquer. Alibaba, which grew its revenues via the Taobao shopping site and supply chains, is coming to an end of a 2014 to 2019 10 billion Renminbi spending spree to build e-commerce service centers in rural China. Tencent, on the other hand, relies on WeChat's role connecting migrant workers to family members in rural areas to get more mobile payment users onboard. Traditionally close family ties in China are also used to cajole older people to join cashless platforms, by encouraging children to recruit parents and elders into getting the apps and teaching them how to use them.

For Alibaba and Tencent differences in the use of payment apps between urban and rural areas are not much of a problem, as long as urban users keep the money flowing through their respective apps. They lose nothing substantial when lower-income, lower-technology, or unbanked users struggle to participate, because mobile transactions are still a massively growing sector. However, regional branches of the PBoC do worry, because lower spending and Renminbi circulation reflects poorly on different provinces' economic numbers - and, eventually, on the economic health of the whole country.

How Chinese individuals, businesses, and communities can adapt to the prevalence of ubiquitous cashlessness will determine survival in a burgeoning but unequal digital economy. If China goes cashless without widening the opportunities to participate, the end result may exacerbate economic inequality in China even further - and leave rural provinces frustrated even as the country's biggest corporations thrive, the report concludes. ■

EUROPOL LOOKS AT INTERNET CRIME

Before discussing the findings of IOCTA, and just by way of contrast, it may be useful to keep one figure from another agency of the European Union in mind. The European Central Bank released figures about counterfeit Euro banknotes in the first half of 2018: 301 000 counterfeit banknotes were withdrawn, 83 per cent of which were € 20 and € 50. There were 21 billion Euro banknotes in circulation, with a total value of € 1.1 trillion. The number of counterfeit banknotes decreased by 17 per cent compared to the last published figure in 2017.

For the fifth year in a row, Europol has produced the Internet Organised Crime Threat Assessment (IOCTA), which aims to provide a comprehensive overview of the current, as well as anticipated future threats and trends of crimes conducted and/or facilitated online.

There are four crime-priorities examined in the report: cyber dependent crime, child sexual exploitation online, payment fraud and online criminal markets. For the purpose of this article, we shall be looking primarily at payment fraud.

In online payment fraud there are two categories: Card present fraud and card not present fraud. Card-not-present fraud dominates payment fraud but skimming - the copying of card details to create counterfeit cards - continues and remains a common issue in most of the EU, although it is stable in most countries with only one member country reporting an increased number of cases. As in previous years, skimming continues to decrease as a result of geoblocking measures. Skimmed card data is often sold via the Darknet and cashed out in areas where Europay, MasterCard and Visa (EMV) implementation is either slow or non-existent.

The Europol report recommends that law enforcement and private industry should participate in the growing number of joint action days successfully tackling fraud involving non-cash payments. Global Airline Action Days, e-Commerce Actions and European Money Mule Actions (EMMA) all rely on close cooperation and collaboration between law enforcement and the private sector and the increasing numbers of participants only add to their success. Despite the likelihood that further EMV adoption will result in more card fraud moving to Card Not Present (CNP) fraud, implementation of EMV should continue.

Member States also reported the use of counterfeit cards originating from outside the EU, mainly from the US and India. In several Member States, criminals used these counterfeit cards to conduct multiple cash withdrawals within a relatively short time frame.

CARD-NOT-PRESENT FRAUD

As the number of online transactions within the e-commerce industry continues to rise, so does CNP fraud. One Member State stated that CNP is the “single biggest area of concern in terms of number of fraud complaints”. The EPC also indicates how CNP is one of the strongest drivers in payment card fraud.

It is difficult to accurately report the scale of the problem, as many victims report the fraud to their financial institution rather than to law enforcement. Often law enforcement has to rely on financial institutions for statistical data. There is also a lack of comprehensive insight into the availability of compromised card data on the Dark Net.

Regarding the different sectors and CNP fraud, reporting by member states is fragmented, preventing any definitive statements with respect to an increase of such frauds. With respect to the retail sector, for fraud relating to physical goods there is a fifty-fifty split between member states reporting an increase and reporting fraud levels remaining stable. In the virtual goods category, the majority is reporting an increase, while other member states are reporting CNP fraud with respect to virtual goods to have remained stable and even one member state as payment fraud decreasing.

With transport, the fraud related to airline tickets appears stable, as nearly all member states have reported. Some have even noticed a decrease in the number of cases connected to airline tickets, a likely consequence of the successful Global Airline Action Days.

In October 2017, 61 countries, 63 airlines and six online travel agencies took part in the 10th edition of the Global Airport Action Days (GAAD) at over 226 airports around the world, coordinated by the EC3 at Europol.

Throughout the week of action, 195 individuals suspected of traveling with airline tickets bought using stolen, compromised or fake credit card details were detained in this major international law enforcement operation targeting airline fraudsters. Several people were caught trying to traffic drugs from Latin America to Europe, frequently flying back and forth using fraudulently purchased tickets.

FUTURE THREATS AND DEVELOPMENTS

In January 2018, the Second Payment Services Directive (PSD 2) came into force. PSD 2 may introduce new opportunities for additional forms of cybercrime. PSD 2 obliges financial institutions to grant third party access to their payment accounts following the permission of their customers. This

means that third parties will have access to the account information of the consenting consumer. APIs, or openly available application programming interfaces, provide access to applications and govern how they communicate with one another. The introduction of open APIs makes banks dependent on the security of the third parties using these APIs. This leads to a number of threat scenarios. First of all, if the third party suffers a data security breach, then the banks' clients can also be exposed. Second, banks may receive fraudulent requests from compromised third parties. For example, a perpetrator may hack a third party and impersonate the company to issue a fraudulent request to the bank.

One of the central issues arising out of open banking revolves around the concept of screen scraping which allows third party providers (TPPs) to access customers' interfaces and collect relevant data to gain access to a bank account. While aimed at improving consumer experience, screen-scraping is susceptible to man-in-the-middle attacks and other forms of fraud. Given the number of security-related concerns, the European Commission has decided to ban screen scraping from September 2019 as part of PSD 2's regulatory technical standards. Until then, however, the issue of screen scraping persists and it is up to the countries how to handle the intermediary period.

CNP FRAUD EXPECTED TO INCREASE AS EMV COMPLIANCE SPREADS

As with many other forms of crime, EMV adoption will not lead to the eradication of payment fraud, but will most likely introduce a shift to CNP fraud. This has already occurred within Europe, where EMV was adopted earlier. The same is expected to take place in the USA.

INSTANT PAYMENTS MAY REDUCE DETECTION INTERVENTION OPPORTUNITIES BY BANKS

The introduction of instant payments also reduces the opportunities for financial institutions to intervene with a transaction. This lowers barriers for criminals when they try to commit fraud. As a result, while instant payments may not lead to new forms of fraud, they may lead to a new challenge in monitoring and detection capabilities for financial institutions. This can in turn lead to a higher fraud rate. This introduction of SEPA instant payments comes from the European Payment Council. The idea is that a transaction from one bank to another should take a maximum of ten seconds.

UK CARD FRAUD IN FIGURES

In its Internet Organised Crime Threat Assessment, Europol does not provide any detailed figures. However the financial industry trade association UK Finance provides very detailed figures although they apply only to the UK. Here are some numbers for 2017, that may serve as a means to judge the scale of payment fraud across Europe, although in both the use of digital payments and e-commerce, the UK is probably one of the more "advanced" countries.

Fraud losses on UK-issued cards totalled £566.0 million in 2017, an eight per cent decrease from £618.1 million in 2016; the first decrease reported in six years. At the same time, total spending on all debit and credit cards reached £755 billion in 2017, with 18.3 billion transactions made during the year. Losses from counterfeit cards decreased significantly, from £ 36.9 million in 2016 to 24.2 million in 2017.

Overall card fraud losses as a proportion of the amount we spend on our cards decreased during 2017, falling from 8.3p per £100 spent in 2016 to 7.0p per £100 in 2017 (in 2008 it was 12.4p for every £100 spent).

The clear majority of card not present fraud involves the use of card details that have been fraudulently obtained through methods such as unsolicited emails or telephone calls, or via digital attacks such as malware and data hacks. The card details are then used to undertake fraudulent purchases over the Internet, phone or by mail order. In 2017 there were 1,399,031 cases of CNP fraud, leading to a loss of £ 409.4m. ■

NEWS

Orell Füssli announced on October 1st that the company has appointed a new Head of the Security Printing Division. Dr Michael Kasch will take office as the new Managing Director of Orell Füssli Security Printing Ltd on April 1, 2019. Dr Kasch has many years of management and industrial experience in security printing. He will succeed the present co-heads of the division, Philipp Seewer und Dr Dieter Sauter. Mr Seewer will stay in the company and will manage the direction Operations within the Division Security Printing. Dr Sauter has decided to leave the company. Orell Füssli Holding Ltd wishes to thank Dr Sauter for his tireless efforts on behalf of the company in recent years.

CEO Martin Buyle will head the Security Printing Division ad interim until Dr Michael Kasch takes up his position.

MACHINE LEARNING EXPOSES VULNERABILITIES IN FINGERPRINT AUTHENTICATION

In November this year, a press release from New York University Tandon School of Engineering discussed the threat of partial fingerprint-based authentication systems being hacked by means of a "Master Print". The implications for fingerprints on ID documents are not clear, but there the level of security is bound to be higher.

Fingerprint authentication systems are a widely trusted, ubiquitous form of biometric authentication, used in billions of smartphones and other devices. Yet a new study from New York University Tandon School of Engineering reveals a surprising level of vulnerability in these systems. Using a neural network trained to synthesize human fingerprints, the research team evolved a fake fingerprint that could potentially fool a touch-based authentication system for up to one in five people.

Just like a master key can unlock every door in a building, these "DeepMasterPrints" use artificial intelligence to match a large number of prints stored in fingerprint databases and could thus theoretically unlock a large number of devices. The work of the research team was decribed in a reserch paper at the IEEE International Conference of Biometrics, where it won the Best Paper Award.

The work builds on earlier research led by NYU Tandon professor Nasir Memon, who coined the term "MasterPrint," and described how fingerprint-based systems use partial fingerprints, rather than full ones, to confirm identity. Devices typically allow users to enroll several different finger images, and a match for any saved partial print is enough to confirm identity. Partial fingerprints are less likely to be unique than full prints, and Memon's work demonstrated that enough similarities exist between partial prints to create MasterPrints capable of matching many stored partials in a database.

The new research took this concept further, training a machine-learning algorithm to generate synthetic fingerprints as MasterPrints. The researchers created complete images of these synthetic fingerprints, a process that has twofold significance. First, it is yet another step toward assessing the viability of MasterPrints against real devices, which the researchers have yet to test; and second, because these images replicate the quality of fingerprint images stored in fingerprint-accessible systems. They could potentially be used to launch a brute force attack against a secure cache of these images.

"Fingerprint-based authentication is still a strong way to protect a device or a system, but at this point, most systems don't verify whether a fingerprint or other biometric is coming from a real person or a replica," said lead-author Bontrager. "These experiments demonstrate the need for multi-factor authentication and should be a wake-up call for device manufacturers about the potential for artificial fingerprint attacks."

The paper, DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, is available at https://arxiv.org/pdf/1705.07386.pdf ■

NEW RULES FOR SCHENGEN INFORMATION SYSTEM

The Schengen Information System is the most widely used and efficient IT system of the EU in the area of freedom, security and justice. The system contains more than 76 million alerts. In 2017 it was accessed more than 5.1 billion times by member states, triggering more than 240 000 hits on foreign alerts (alerts issued by another country).

The Schengen Information System is being reinforced through updated rules to close potential gaps in the system and introduce several essential changes on the types of alert entered. On November 19, the European Council adopted three regulations on the use of the Schengen Information System, in the field of police and judicial cooperation in criminal matters, in the field of border checks, and for the return of illegally staying third-country nationals.

ALERT CATEGORIES

The draft regulations introduce additional categories of alerts to the system:
- alerts issued for inquiry checks, an intermediary step between discreet checks and specific checks, which allow for individuals to be interviewed.
- alerts on unknown suspects or wanted persons, which allow the introduction into the SIS of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist incidents and which are considered to belong to a perpetrator.
- preventive alerts for children at risk of parental abduction and children and vulnerable persons who need to be prevented from travelling for their own protection (for example, where travel might lead to the risk of forced marriage, female genital mutilation, ur trafficking of human beings).
- alerts for the purpose of return, improving the exchange of information in relation to return decisions.

It will, become possible to use facial images for identification, in particular to ensure consistency in border control procedures as well as DNA profiles for identification of missing persons in cases where fingerprint data, photographs or facial images are not available or not suitable for identification. ■

SECURE FACE IDENTIFICATION VIA SMARTPHONE

Veridos, the joint venture of two international ID solution providers, Giesecke & Devrient and Bundesdruckerei, has released a new mobile solution - VeriGo True ID - that allows citizens to easily access eGovernment services using smartphone-based face authentication.

This solution links the person to a digital identity, enabling citizens to access a variety of services remotely, such as applying for a new passport, renewing official documents or registering a birth. The technology allows citizens to easily verify their identity via face recognition. It is no longer necessary for them to visit the relevant office in person, instead, they can simply download the smartphone app and access the desired service from wherever they may be. This increases accessibility in remote regions while also cutting costs for governments.

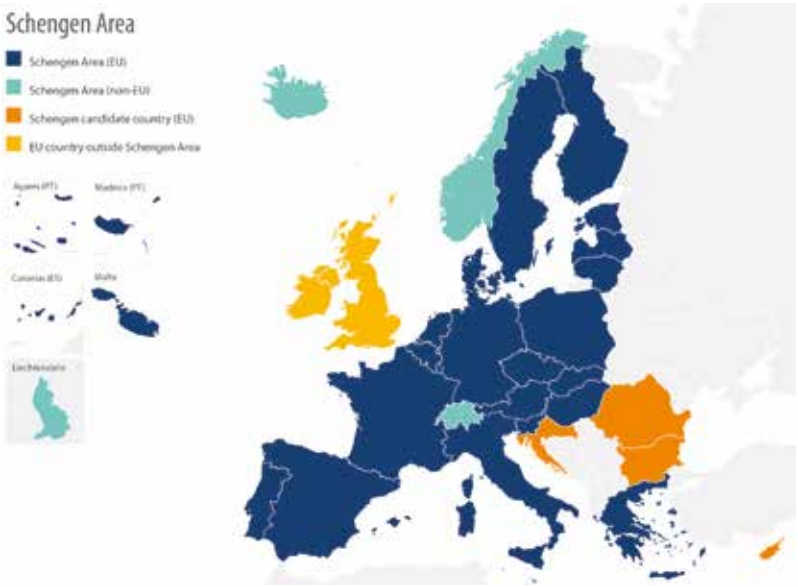
TECHNOLOGY

The mobile face authentication solution consists of a mobile app for face detection and a server-side matching service. It is not necessary to enroll in advance to access the service, as the matching is done against an existing national biometric database. Liveness detection helps to prevent spoofing attacks. The VeriGO TrueID solution can be seamlessly integrated into an existing authentication server and works on all commonly used smartphones on a BYOD (bring your own device) basis.

FACE AUTHENTICATION

Biometric face recognition is a secure and convenient way to validate an identity. The technology uses a unique human feature, authenticating the person as an individual. Unlike traditional secret-based systems, such as passwords, a biometric feature cannot easily be shared with others – willingly or otherwise. It could not be simpler, either: all citizens have to do is look into the camera of their smartphone. ■

COUNTING THEM IN, COUNTING THEM OUT: THE SCHENGEN ENTRY/EXIT SYSTEM



Almost a year ago, on 29 December 2017, the Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) as well as the amendments needed to integrate the new Entry/Exit System into the Schengen Borders Code entered into force. It will take until 2020 for the system to be operational. What will EES bring and what are the challenges?

The use of biometrics for border control in the EU is not new, but it takes time to apply any system. Only relatively recently the EU has adapted the Schengen Borders Code and made it mandatory to read and verify the ePassport chips. There are other systems that aim to control access to the Schengen area. The Visa Information System (VIS) has been operational since 2015 in Member State consulates, and its consultation is now compulsory for visa-holders entering the Schengen area. In addition, since February 2013, the concept of Smart Borders has been introduced. It's an ambitious package of legislative measures drawn up in consultation with the European Parliament. As part of the Smart Borders Package, the Entry/Exit System will be the next step. This means that from 2020 on all borders into the Schengen area will become biometric.

By introducing the Entry/Exit System, the European Union aims to contribute to the modernisation of the external border management by improving the quality and efficiency of the external border controls of the Schengen Area. The system will help to reinforce internal security and the fight against terrorism and serious crime and also help Member States dealing with ever increasing numbers of travellers to the EU without having to increase the number of border guards.

Nationals of non-EU countries – so called "Third Country Nationals", or TCN for short - whether they need a visa or are visa-exempt - will have to register with four fingerprints and a facial image when entering Schengen countries through land, sea and air borders. The biometric data will be stored in the EES together with the identity data and other information taken from the travel document. Each data record resembles an electronic stamp (thus replacing the previous manual stamping procedure) and will be used to calculate the legitimate duration of stay within the Schengen area: Once the EES is introduced, it will become much easier to verify whether the permitted duration of a short stay (maximum of 90 days within a 180- day period) is exceeded. The national security authorities will be automatically informed by the database if the person concerned has not left the country by the set date. Therefore, it will be easier to spot those who overstay visas and to fight document and identity fraud. But as it is perfectly legal for a TCN to enter the Schengen area e.g. in Spain and leave it in Finland, the system has to work flawlessly in all member countries.

After adopting the relevant legislation, the EU gave itself 36 months for the system to be operational. This is a tight schedule not only for the electronic system, the building of which was entrusted to eu-LISA, which is working together with the member states, but for implementation on the borders of the national member states. (eu-LISA is the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice headquartered in Tallin, Estonia.) The complete system consists of the central European register, a biometrics background system and the integration into the national border control and security systems.

In a recent interview, Frank Steffens, Principal in the Homeland Security division of Germany's secunet explained the need for the EU to act: He said that continuing with the present system of manual stamping of passports is not an option, particularly considering the constantly rising number of visitors from third countries and the numbers of migrants and refugees that arrive at the Schengen borders. Enforcing the higher level of security is a big challenge for everyone: The new handling process for Third Country Nationals would become significantly more complicated and potentially more time-consuming due to the biometric data collection at the stationary border control counters. This would inevitably lead to longer waiting times for all travellers. Due to the longer wait times, airports are likely to

reach their capacity limits, especially as passenger numbers continue to rise. This would predispose passengers to being dissatisfied, which in turn increases the pressure on security organisations, airports and airlines.

It is therefore essential to create an infrastructure that takes into account both the depth of control and the flow of passengers while facilitating the capturing of biometric data at the counter and achieving the technically much more complex connection of the airports – across several levels – to the central EES.

If a border control strategy is developed that is optimally adapted to the EES processes and applications – which also includes the stationary counters – the time required for the control process should remain virtually unchanged, despite the capturing of biometric data and the extensive checking performed. This is ensured by automation and process optimisation at key points, for example self-service kiosk systems, where travellers from third countries can carry out parts of the required and frequently time-consuming steps during the control process themselves by capturing their fingerprints and facial image, before proceeding to the border control counter. This speeds up the time-consuming process of data collection and document checks. EU citizens and, under certain conditions, also TCN, can use eGates (or ABC-gates) to perform the border crossing process themselves within a very short time. Also, at the counter, applications that have been developed specifically for border control can visualise the check results from various systems at a glance.

WHO CAN ACCESS DATA?

As in any large-scale biometric ID system, it matters who can access the data. This will be tightly controlled and will be limited to the member states, specifically their border guards and consular officials dealing with visas who will have evidence-based support to carry out visa policy. Law enforcement authorities in member states not directly involved in border control and Europol will also have access for criminal identification and criminal intelligence. The EES database will support the identification of terrorists, criminals as well as of suspects and victims of crime. It will provide a record of travel histories of non-EU nationals including crime suspects, perpetrators or victims of crime. It would thus complement the information in the SIS.

Data collected in the self-service kiosks at airports will be checked against the databases of the Schengen Information System (SIS) and Interpol's SLTD (stolen and lost travel documents) database. EES will also give information to border guards on refusals of entry of non- EU nationals and enable refusals of entry to be checked electronically.

WHAT ABOUT PRIVACY

In Spring last year, when the EES was still in the discussion phase in the European Council, the first critical voices appeared. "The scheme poses a serious risk for the fundamental rights to privacy and data protection of everyone travelling to and from Europe. But it won't prevent irregular migration," said Estelle Masse, senior policy analyst at digital rights organisation Access. The scheme is estimated to cost as much as €1 billion. That is an awful lot of money to spend for "nothing more than better statistics," she added.

A frequent criticism concerned the time the data, biometric and otherwise, is being kept in the system. The European Association for the defence of Human Rights (AEDH) in a posting on 28 November 2017 raised the question of data retention. It said: "Data from third country nationals who have respected the authorized length of stay will have their data kept for three years. .... Thus, for those who visit the Schengen area at least once every three years, their data will be permanently kept." The post continued "AEDH regrets that no compromise has been found between border control and the protection of personal data and regrets in particular that the proposal of the Social Democrats to reduce the storage time of data to 180 days was not retained."

WHO IS IN AND WHO IS NOT

The Entry/Exit System applies to the Schengen area and it was proposed by the European Commission, voted into existence by the European Parliament and adopted by the European Council. However, the Schengen area does not only consist of EU member countries and not all EU member counties are part of the Schengen area. Iceland, Lichtenstein, Norway and Switzerland are associate members of the Schengen area but are not members of the EU. The Azores, Madeira, and the Canary Islands are special members of the EU and part of the Schengen zone although they are located outside the European continent. Ireland and the United Kingdom have not joined the Schengen area, because they have opt-outs, while Romania, Bulgaria, Croatia, and Cyprus are required to join and are expected to do so soon.

It seems clear that UK nationals will be treated as TCNs (if and) when the country has left the European Union, while the position of Irish travellers is not quite clear, but it is difficult to imagine that the Irish will be subjected to the EES, especially in view of the current Brexit negotiations which center very heavily on the question of the Irish/UK border. ■

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®