# PHYSICAL TO DIGITAL:

## A REVOLUTION IN DOCUMENT SECURITY

### A White Paper

Ian Lancaster
Francis Tuffy
John Winchcombe

Published by

Reconnaissance International Ltd

10 Windmill Business Village
Brooklands Close
Sunbury-on-Thames
TW16 7DY
United Kingdom

Tel: +44 (0) 1932 785 680
Fax: +44 (0) 1932 780 790

Email: publications@reconnaissance-intl.com
Website: www.digitaldocumentsecurity.com

Although all the information contained herein is obtained from sources believed to be reliable, we accept no legal liability of any kind for the publication’s contents or for any omissions, errors and their consequences.

Reconnaissance International Ltd acknowledges products, services and company names referred to in this publication, some of which are trade names, service marks or registered trade marks.

# Executive Summary

There is a revolution underway in the secured document field, as society migrates from using physical secured documents, such as banknotes and identity cards, to the use of smartphones and electronic payment cards for financial transactions and as carriers of our identity credentials.

There is a perception that this revolution is well underway and that the transition from physical to digital is inevitable, unstoppable and irrevocable. The drivers are user convenience and provider cost savings, allied to the technical community's belief that it can deliver a new way of doing things. Perception trumps reality for now, though, as cash is still used for most retail purchases globally and passports are still required to enter a territory. Nonetheless, this transition is inevitable, so there is a need to consider the impact and implications of this change.

Physical documents are tangible, familiar, and with security and authentication features built in. Moreover, there are a thousand years of history and experience in the world of banknotes, passports and other secured documents, and a key driver for specifiers and designers is security and document protection. In this physical world, professional document examiners develop a sixth sense, a feeling for the document which comes with familiarity and practice.

The result is reflected in the low counterfeiting levels for banknotes and passports (eg. 0.003% of euro banknotes in circulation and 2% of passports worldwide), which compares to, say, the World Health Organization's estimate that worldwide 10% of medicines are fake. More pertinently, the rate of fraud using payment cards is a large multiple of the banknote counterfeit rate – over 300 times more in the eurozone.

Digital financial transaction systems and identity credentials, for comparison, have barely a 20-year history. This field is technology driven, starting with the development of near field communication (NFC) chips on phones and the 2004 launch of Alipay in China, followed by the the launch of the iPhone in 2007. This 'we can do it' attitude leads to the large number of incidents of hacking, system crashes and identity theft which affect millions – sometimes hundreds of millions – of users, often jeopardising their key personal information.

Identity becomes a key factor in this move to digital systems, requiring users to establish their identity and then repeatedly prove it. This involves biometrics, encrypted digital signatures, hash codes, two-factor signatures, self-sovereign ID, encrypted apps, encrypted phones and much more. But all of this depends on the algorithms in the systems. Do we trust these algorithms too much? Is there a role for human senses in examining and authenticating digital identity and financial transactions?

An immigration official can look at and scan a passport and look at the person presenting it. A retailer can check a banknote with their eyes, their fingers and simple equipment – but this takes time. When digital solutions are created, the primary goal is a more convenient product. Security brings friction, eroding that all-important convenience valued by the consumer. Security is required but is currently a secondary consideration in the development of these digital systems.

Digital identity is being introduced across health systems, driver's licences and national ID cards, facilitating more efficient health care and easing the passenger experience, enabling kerb-to-seat progression without showing any documents at an airport. Significantly, though, no immigration agency allows the same convenience for arriving international passengers, who all have to show a passport or ID card, sometimes to a machine, sometimes to a person, but always with the person there as backup to the machine.

This white paper asks whether the way forward in this transition, this revolution, is to look for ways to draw on the best of both worlds, the physical and the digital. Can the commitment to security and protection that drives the physical secured document field be inculcated among digital system developers and adopters – and if so, how? Reconnaissance aims to stimulate and facilitate this important discussion through its newsletters, conferences and other publications.

# Contents

# Introduction: The Digital Document Revolution

*"Our reluctance to question the power of an algorithm has opened the door to people who wish to exploit us."*

*Hannah Fry*[1]

We are currently living through a revolution. It's not a national revolution, like the French or Russian revolutions, nor is there an obvious Robespierre- or Lenin-type leader or figurehead for this revolution. This revolution is global and amorphous, driven by a widespread consumer desire for convenience and simplicity on the one hand and the realisation by digital systems developers that they can fulfil that desire on the other.

A revolution is intrinsically disruptive, and this one is disrupting the way we manage our financial transactions and how we confirm who we are. We are in transition from the traditional use of physical secured documents such as banknotes and passports, to the use of digital methods of payment and identity confirmation. We are moving from a world in which we can see, touch and smell banknotes, passports, identity cards, driving licences and so on, to a virtual world in which we use smartphones and other digital devices to pay for things and to confirm our identity.

But is it a revolution that leaves us and our data safe and secure?

We are moving from a world in which people can examine and inspect a document to check its legitimacy (in order to be confident it can be trusted), to one in which we have to trust that a device, such as our smartphone, is doing what we think it's doing, that the data it's using is accurate and secure and the decision it makes – or leads us to make – is correct and appropriate.

Are we right to invest that much trust in these new methods of making payments and showing our identity? Or should we pay heed to Professor Hannah Fry's view that, in failing to question the algorithms that are doing this work for us, we open the door to hackers, fraudsters and other criminals?

## Scope

This white paper examines this transition in security documents from the physical to the digital. We consider:

- How far has it gone and what is its future?
- What are its implications and – crucially – how safe is the data held and used in the digital world?
- Are we merely users of these systems, or is there a role for us in ensuring they and the data they use are secure? What might that role be?
- Is anything needed to enhance the safety and security of these digital methods and if so – what?

The stimulus for this white paper is the perception that this revolution is well advanced, with many retail payments no longer involving cash and many of us carrying our driving licences, health or social security identities on our smartphones.

In fact, at the global level neither is true – cash is still king and physical ID documents are still the norm – but many people, especially in developed countries and even among security document specialists, share this false perception.

[1] In 'Hello World: How to be Human in the Age of the Machine', Penguin Random House 2018, ISBN 9780857525246

Nonetheless, the irrevocable trend is towards the digitisation of payments and identity, and that trend is accelerating, with more consumers using what are now termed 'mobile wallets' to make retail payments, and issuers of identity documents actively considering how to move away from physical (ie. paper or polymer) to digital ID credentials.

This white paper therefore aims to clarify where we are at present and to indicate the issues that arise in this transition from physical to digital, while acknowledging the likelihood of digital methods becoming more prevalent in the years ahead.

At the 2018 Optical Document Security Conference the transition from physical to digital was described as a ‘watershed in document security’[2]; are we approaching that watershed? Have we already crossed it? How safe are our financial transactions and our personal data in these digital systems? How do they compare with the security and safety of the physical document world?

## A word of caution

This white paper explores the issues and poses questions; we don’t claim to have the answers!

# How and Why Physical Document Security Works

### *“Fingerspitzengefühl”*

What a fascinating and apt German word for the world of document examination, although it’s practically untranslatable! Literally it means 'the feeling at the tips of your fingers', but it’s used to refer to the intuition, the sixth sense, that we develop when we are very familiar with something that we encounter every day.

A professional, trained document inspector – such as a bank teller or an immigration officer – handles hundreds, if not thousands, of banknotes or passports every day. They have fingerspitzengefühl, a sense, a 'fingertip feeling' for the look and feel of these documents, so they quickly know if a document they’re handling is 'not quite right'. They may not immediately know why, but the chances are that a more detailed examination will reveal some aspect or component of the document that is fraudulent.

This interaction between the document and the examiner has been developed and refined over many centuries. The first government-backed paper banknote was issued in China in 1023 AD, when Emperor Chen Tsung established a government agency to issue a paper means of exchange. It took Europe over 600 years to catch up, when Sweden issued a paper banknote in 1661, but then other countries followed suit as they realised the convenience of banknotes: Britain in 1695, and France during its revolution in the 1790s[3].

## Countering Counterfeit Banknotes

This development quickly saw the corollary of counterfeit banknotes, which in turn led to the incorporation into banknotes of designs and components to make it more difficult to counterfeit notes and easier to detect them. Historically, difficult to make or source paper was used, and some special features were incorporated into the printed design; now, they are also added to the substrate and the printed note. The outcome is that today’s banknotes may have tens of anti-counterfeit or counterfeit detection features built in, from the obvious (for inspection by humans) to the very non-obvious, the latter only being detectable with laboratory equipment.

Banknote printers have a similar longevity. OK, most don’t have a thousand-year history, but there is a wealth of experience in security printing from many state-owned and commercial printers who have been producing security documents, including banknotes, for 200 years or more.

As with banknotes, so with passports. The word 'passport' was first used for a document enabling safe passage across national borders in England in 1540, but the passport as we know it today as a standardised identity document originated with the League of Nations in the 1920s. The invention of photography some 90 years earlier was a critical factor in enabling the production of a document to confirm the identity of a specific person.

[2] Physical vs Digital: A Watershed in Document Security? Ian Lancaster, Optical Document Security Proceedings 2018

[3] Historical banknote information is from Don Cleveland on the International Bank Note Society website - www.theibns.org

What has developed over these centuries of experience in design, development, production and examination of security documents is a thorough awareness of the need to fight fraudsters, whether they be counterfeiters who attempt to recreate a document or those who alter a document to change its value or holder's identity. Protection is probably the first thing a specifier or designer thinks of when they sit down to create a new banknote, passport or identity card.

## The Security Hierarchy

One commonly recognised outcome of these centuries of experience is the hierarchy of security. As Figure 1 shows, this means incorporating security features into the document, which are intended for increasingly sophisticated examination, from unaided human senses (Level 1) to laboratory equipment (Level 4), via simple handheld tools and more sophisticated portable tools.

For banknotes, the examination starts with the public (who are typically fairly lackadaisical about examining their cash) or a retailer. The next level is a trained examiner, such as a bank clerk, who uses their *fingerspitzengefühl* before passing a suspect note to someone more specialist who has tools – such as a simple magnifying glass or ultra-violet light – to help them examine covert features, and so on to the forensic laboratory.

It's similar for passports, driving licences and other ID cards – except that the public probably don't examine their ID items, so we go straight to Level 2 – examination by law enforcement or immigration officials.

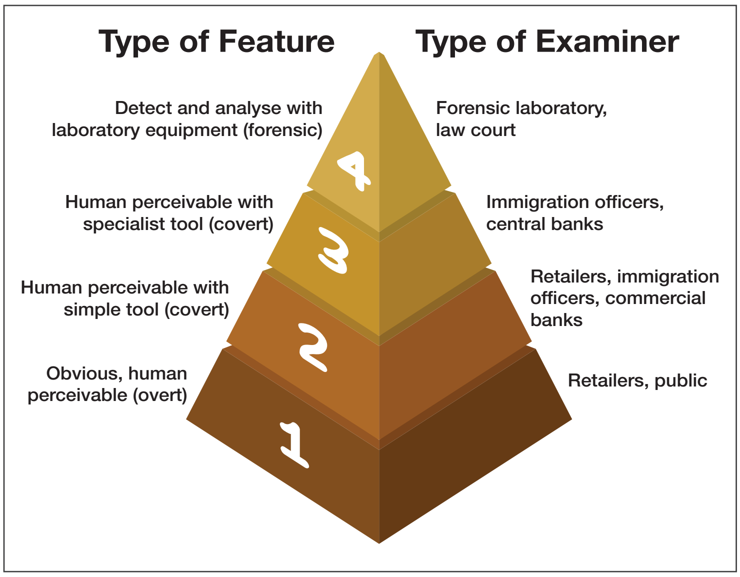

Type of Feature
Type of Examiner
Detect and analyse with laboratory equipment (forensic)
Forensic laboratory, law court
4
Human perceivable with specialist tool (covert)
Immigration officers, central banks
3
Human perceivable with simple tool (covert)
Retailers, immigration officers, commercial banks
2
Obvious, human perceivable (overt)
Retailers, public
1

Figure 1: the Hierarchy of Security.

This is an established and effective system where each level adds more complexity, requires more expertise and more sophisticated tools. The top level provides proof that should stand up in a law court if the fraud perpetrators are prosecuted.

## Some Counterfeit Statistics

The result is a very low level of counterfeiting of government-issued secured documents. In 2018, according to the European Central Bank, some 563,000 counterfeit euro banknotes were taken out of circulation; that's three-thousandth of one percent (0.003%) of the 22 billion euronotes in circulation. The comparable rate for US dollars, the most used note internationally but which is not so well protected, is estimated by the US Treasury at between 1% and 2.5.[4]

Of course, it's possible that there are undetected counterfeits in circulation, but the consensus view in the law enforcement community is that this is extremely low and wouldn't significantly change these figures.

[4] US Department of Treasury

Compare these percentages with other much-used items that are known to be counterfeited but don't have the rigorous approach of the banknote world; for example, the World Health Organization's estimate that ten percent (10%) of medicines worldwide are counterfeit, ie. a counterfeit rate 3,333 times higher than euro banknotes.

Rates of passport counterfeiting are similarly low, although exact statistics are hard to come by. An indication of the difficulty of counterfeiting passports is the number that are stolen or 'lost'. Media headlines refer to a huge number of 'fake' passports, but the reality is that most of these are stolen (including blank passport booklets stolen in transit) and fraudulently altered. Interpol estimates that in 2015 (latest available figures) 40 million passports were lost or stolen. That is 2% of the approximately 2 billion passports in use worldwide, a relatively high rate because it is much easier to steal and alter a passport than it is to create a good fake from scratch.

Sadly, the same cannot be said for other forms of identity, such as driving licences and social security cards. The 9/11 attacks prompted the US authorities to take steps to improve the security of driving licences issued by each state (in the absence of a national identity card, state-issued driving licences are the de facto ID card in the US), but the states successfully fought against having common security features as they wanted to retain their autonomy.

It is easy to source fake ID cards on the web, including US driver licences. They are adequate, perhaps, to kid a bartender that you're old enough to buy an alcoholic drink, but it's doubtful that they would pass inspection by a traffic cop or immigration officer.

## Examination is Key

The quality of the examination is a key component in successful detection of fraudulent documents or cards. This is where human senses have a role, especially as used by professional, experienced document examiners. Human senses, especially when trained, are remarkably attuned to detecting variations in a familiar item.

When that item is designed for security, to protect it against copying or alteration, and the person examining it knows its inbuilt security features, detection of counterfeit or altered documents is almost certain, which is why 99.99% of circulating euro banknotes are not counterfeit.

Remember these figures for document counterfeiting when reading about digital hacking and data theft…

## Key Questions

The bottom line is that there is huge experience in the security document sector in designing, producing and examining ID documents and financial transaction documents. So as digital methods become more common, key questions that need to be asked are:

- Do digital methods match the security and detection built into the physical document world?
- If not, how can they be improved?
- Should we abandon the use of human inspection?
- If not, how do we combine the best of both worlds?

# Digital Systems and Data Security

*"Passwords, phone numbers, addresses and other PII (personally identifiable information) that authenticate users' identities when logging in can be easily cracked or stolen using specialized malware."*

*Who Are You? PYMNTS.com*

Does the security of digital methods of financial transactions and identity confirmation match that of the well-established traditional methods that use physical documents?

If not, can it be improved?

These are the critical questions in this age of revolution, in this transition from the physical to the digital world.

## The Game-Changers

Attempting to answer those questions, we start with the history of this digitisation, for which there are two game-changing events:

1. The invention of what became known as the World Wide Web by Tim Berners-Lee in 1990, which enabled this world of digital financial transactions and ID credentials;
2. The launch of the Apple iPhone in 2007 as the first easy-to-use, touch-controlled smartphone. (The Blackberry preceded the iPhone by eight years – launched in 1999 – but its main appeal was as a pocket-size voice and email communications device.)

Neither of these was driven by an intention to replace banknotes or passports; the first was Berners-Lee's response to the need to manage the large amounts of data at CERN, while the iPhone was Apple's move into the mobile phone business, deliberately showing off what it could do with the technology. So in neither case was security a driving force.

Other notable landmarks, though, were more directly aimed at financial transactions, including:

- AliPay's launch in China in 2004;
- Nokia's launch of the first NFC (Near-Field Communication)-enabled phone in 2006;
- WeChat's launch of WeChat Pay in 2013, to compete with AliPay;
- The launch of ApplePay – the first integrated, simple-to-use phone-based payment system *in the West* – in October 2014 (just over five years ago at the time of writing).

The Web and smartphones have proved to be truly disruptive innovations. The dominance of mobile wallet payments in China has even prompted the country to launch its own official digital currency – expected very shortly, a mere seven or so years after the launch of WeChat Pay (by the time you read this it might have been launched).

# The Digital Systems Drivers

As we mentioned in the Introduction, what's driving this transition to digital systems is partly a human desire for convenience and our growing expectation that our actions will have almost immediate results. But we need to examine the other side of that coin, the side which is providing this convenience:

- What drives the developers of these systems and the writers of code to put them into practice?
- And how do they perceive their role in protecting the hard-earned money and the identity credentials of their customers?

The simple answer to the first question is 'technology'. This field is technology driven; there is a new iPhone launched every year, and it is a similar case with Samsung and other Android phone manufacturers. Moore's law[5] that processor power doubles every year applies: these phones are introduced because they are better than the predecessor generation. 'Better' meaning more computing power, more memory, higher resolution cameras, larger and higher resolution screens, new capabilities and new apps to take advantage of all these improvements. Not to mention the rising speed of phone networks and expansion of wifi coverage.

We see that the mobile wallet (also referred to as the digital wallet – the ability to make payments using a phone) has a 15-year history. There are of course security procedures built into all of these proprietary systems, but this is not a driver of development as it is for the security document community.

# And so to Digital ID

The digital ID field is even younger. The development of better cameras, memory and speed is allowing the adoption of smartphones for identity confirmation as carriers of driving licences and citizens' ID credentials. Several countries and US states are developing and testing mobile phone-based driving licences and IDs, while in Estonia it has been legal to use an encrypted digital signature instead of a written signature since December 2000.

Indeed, Estonia is one of the countries most committed to the adoption of digital ID credentials – if not the most committed. Over 2.5 million people in the Baltic states use its Smart-ID credentialing system, including 38% of the adult population in Estonia (420,000 users). It is worth noting that a key driver for adoption of the Smart-ID card is that it also serves as a pass for public transport. It is significant that this new system, Smart-ID, was launched in 2017 as a response to vulnerabilities found in the country's Mobile ID system that could have led to the theft of users' identities.

[5] Gordon Moore, co-founder of Intel

## Problems, Problems…

This was a close shave for Estonians, but there are numerous examples of online identity and financial theft, often serious enough that they are reported in the mass media, not just the specialist media. In addition, there have been many cases of systems crashing, making it impossible for people dependent on their credit cards or smartphones to conduct any financial transactions. To give just a few examples:

- In July 2019, Capital One bank suffered a data breach which affected around 100 million US citizens;
- In 2019, 165 million records containing personally identifiable information (PII) were breached in the USA alone, according to the Identity Theft Resource Center[6];
- Credit-check company Experian reports that 40% of consumers worldwide have been targets at least once for online financial fraud or identity theft;
- Visa's European credit card system crashed in June 2018, making it impossible for customers to use their Visa debit or credit cards for many hours;
- At the time of writing, the Travelex online currency exchange websites have been offline for almost two weeks following a ransomware attack (ie. 'pay us and we'll restore your service') which threatens to steal and release the PII of millions of customers;
- Following system crashes at TSB, NatWest and other UK banks, an October 2019 report by the House of Commons Treasury Committee said that customers are left 'cashless and cut off' due to an unacceptable number of IT failures – some of which have cut-off customers from their bank for several days or even longer.

## The Hackable 'Cloud'

It is worth pointing out that these are thefts from or hacks of the places where our data is stored. Those promoting online systems refer to storage in 'the cloud', implying an ethereal, intangible entity which thus cannot be illicitly penetrated. But the reality is that our data is transmitted over the internet (via cables and satellites) to huge server farms, buildings that contain thousands or even hundreds of thousands of servers making and recording our transactions or our identity. These very physical resources are certainly well-protected, with back-ups and redundancy built in, but they have been hacked, as have the internet network connections to them, as the above examples reveal.

*So for 'cloud' read 'networked computers'.*

These computers, data stores and the connecting networks need protecting, and as with the hierarchy of protection in the physical document world, so there are numerous layers of protection in the digital world. Hash codes, PKI (public key/infrastructure), two-factor sign-in, SSI (self-sovereign identities), encrypted apps and protected server farms – all of these and more are deployed to secure our financial and identity data in this digital domain.

Note, though, that these security processes all work *within* the digital domain; there is no interaction with human beings.

There are numerous collaborative development projects underway to establish standards and improved systems for data protection, including the EU-funded Olympus[7] project and ISO's emerging mobile driving licence standard. These all show that there is recognition of the need for security within the digital domain, even though the original impetus may have been – and in hardware terms, still is – technology driven.

[6] Idtheftcenter.org

[7] Oblivious identitY Management for Private and User-friendly Services

Nonetheless, these systems remain vulnerable and fallible, a fallibility which border control authorities at least seem alerted to. These authorities are introducing document-free, facial recognition passage from kerb to airplane for departing passengers, such as at Singapore's Changi airport, Beijing's new Daxing airport and JetBlue's pilot scheme at Boston Logan airport. Yet none of these airports have a similar document-free system for arriving international passengers, nor are any being planned. Border agencies still require examination of identity credentials for arriving passengers, to ensure the document matches the holder, even though this is often machine examination rather than human examination. But even with machine verification of passports and ID cards at airports, any issue leads to a fallback to an immigration officer, who will examine the document and the face of its holder to ensure they match and are legitimate.

## Human Senses

This introduces us to a key difference between the security procedures for physical documents and digital 'documents': the use of human senses as an examination resource. In the digital systems currently being used for financial transactions or identity credentialing, there is no scope for human examination of their security; when a traffic cop views a driver's licence on his or her phone they're not interrogating its legitimacy – they're simply confirming whether or not the driver has a valid licence. Similarly, when a customer uses a smartphone to pay for something in a shop, neither s/he, the retailer nor either of their banks are examining the transaction; they are simply watching it go through.

But perhaps there should be some human interaction in these systems? Are we indeed too trusting, too reluctant to question the power of the algorithms that are enabling these transactions and ID confirmation?

When an experienced person examines a physical document with which they are familiar they are doing so not only with their senses but also with their brain, their memory; they are engaging with the document and its security features. Perhaps this is a factor which contributes to the much higher rate of dollar bill counterfeiting compared to euro counterfeiting, given that so many dollar bills are transacted outside the USA.

There's an important strand of neurophysiology that establishes the link between our eyes (seeing) and our brains (mind) which results in perception. Hermann von Helmholtz (1821-1894) was the first to empirically study the physiology of perception; he is referenced in Richard L Gregory's (1923-2010) seminal book *Eye and Brain*, which describes how we perceive using these two organs, while Magdelen D Vernon (1901-1991) wrote explicitly in *The Psychology of Perception* that 'seeing is not the same as perceiving; there's a need to engage the mind to see then perceive'.

The opposite happens when we use our smartphones as 'security documents'; we trust, we disengage, we don't pay attention to what's happening 'under the skin'.

We therefore make ourselves vulnerable to those who would do us harm by stealing our identity or our money.

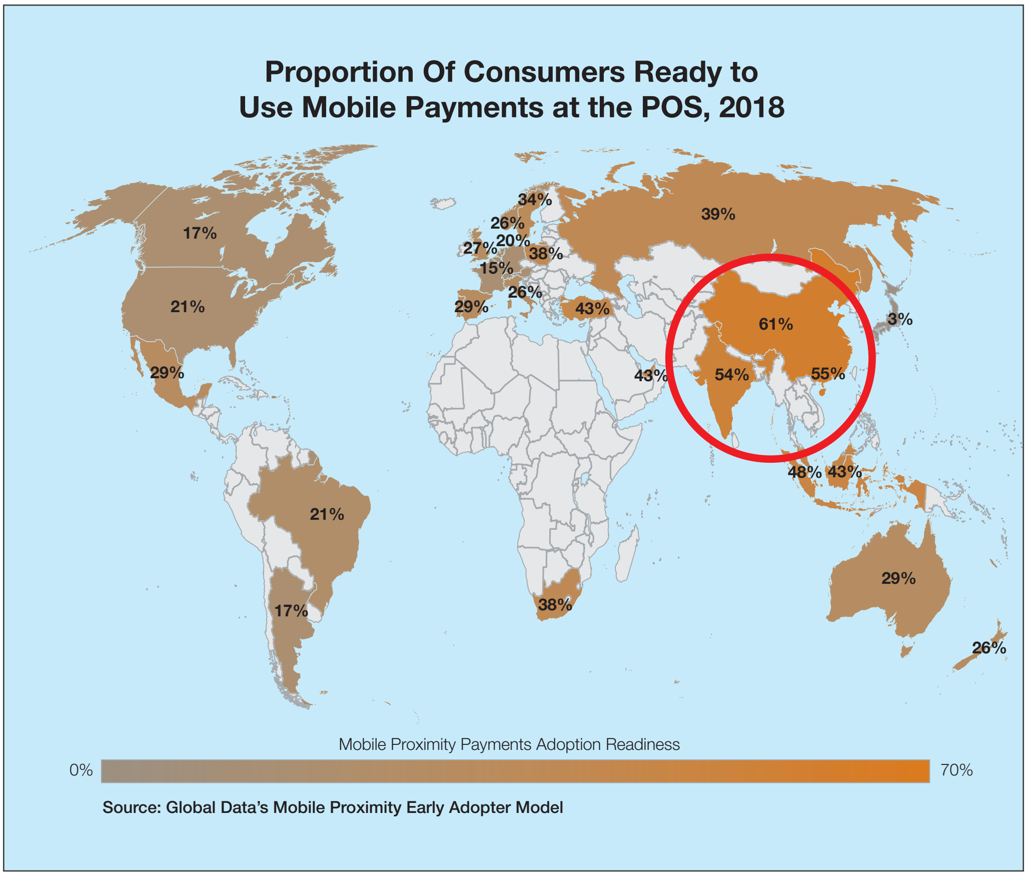
# Financial Security and Authenticaton

*“Convenience and security are uneasy bed fellows”*
*Garry Sidaway, NTT Security*

What is going on in consumer payments at the moment? Is it a revolution or simply technology amending the current model? How does security and authentication fit into this story?

Nearly 85% of all retail transactions today are still made with cash, representing around 60% of retail transaction value[8]. Despite that, few would deny that the world is changing as digital increasingly displaces the analogue world. Figure 2 shows the country-by-country willingness of shoppers to use mobile payment methods, revealing the dominance of smartphone payments in China.

This can be characterised as a continuation in the evolution of payment methods, which has seen society move from cash (still in use, of course), to cheques (17th century but now out of favour), to cards (1950s to present) and now digital payments and digital currencies.


Proportion Of Consumers Ready to Use Mobile Payments at the POS, 2018
17%
21%
29%
21%
17%
34%
26%
27%
20%
38%
15%
26%
29%
43%
39%
61%
3%
43%
54%
55%
48%
43%
38%
29%
26%
Mobile Proximity Payments Adoption Readiness
0%
70%

Source: Global Data’s Mobile Proximity Early Adopter Model

Figure 2: the willingness of consumers to use phone-based payment methods.

[8] thefutureofcash.com

## The Vulnerability to Fraud in this Paradigm Shift

We characterise this as a revolution, not simply evolution, because the characteristics of the digital payment world are so fundamentally different to those of the physical payments world. Digital represents a paradigm shift from physical payment methods.

What is certain is that the two newest of these transaction methods are the most vulnerable to fraud – as shown, for example, in the UK, where, according to the Bank of England, there are currently 3.8 billion banknotes in circulation with a face value of £70 billion; in 2018 472,000 counterfeit notes were taken out of circulation, with a face value of £10 million (in the first half of 2019 the figures were 228,000 and £5 million). ie. counterfeits represent 0.0012% by quantity, 0.014% of value.

Compare this with the Card Payments statistics from UK Finance. In 2018 there were almost £800 billion-worth of card transactions in the country, but there was £671 million-worth of card fraud – ie. 0.08%, which is a rate of fraud over six times higher than that for cash. It is important to note that 'card-not-present' (CNP) fraud represents 76% of the total. If the criminal can pass themselves off as the owner of the card, money can be stolen.

The difference in the rate of fraud between banknotes and payment cards in the eurozone is even more stark. The European Central Bank reports that payment card fraud in the zone in 2016 totalled €1.8 billion, which is one-tenth of one percent of the total card transaction value of €1.8 trillion[9]. This is over 300 times greater than the 0.003% of euro banknote counterfeits, while Europol reports that CNP accounts for 66% of the card fraud.

For an African comparison, the South African Banking Risk Information Centre’s 2018 crime report[10] showed card crime for South African issued cards increasing 18% to R 873 million ($58 million). The increase across credit and debit cards was almost identical. As in the UK, CNP accounted for just under 80% of the total.

In 2018 there were 23,466 incidents across banking apps, online banking and mobile banking amounted to R 263 million in gross losses, a rise of 75.3%. This broke down as

| | |
|---|---|
| • Mobile banking | R 29 million |
| • Online banking | R 129 million |
| • Banking app | R 105 million |

## Identity is All

It is clear that in electronic transactions, whether card or app-based, the key challenge is identity.

If you pay with cash, the cash is assumed to be yours and the physical exchange is straightforward. The link between value and the bearer is 'presence' and not 'identity'. A digital transaction is more complicated because there is no link between the value and the identity of the user.

[9] Source: European Central Bank

[10] Sabric.co.za/stay-safe/card-fraud/

Nonetheless, the move away from cash is happening, and in some places it's happening fast. In China, Alipay and WeChat Pay have made mobile payments an everyday event and they are spreading fast around the world with banking licences in the region and into Europe. Apple Pay is a minority player in comparison. Similarly, in Sweden the Swish payment app is sweeping cash away; 80% of consumer transactions are card or Swish, meaning only 20% are made with cash.

Some central banks and commercial companies are recognising and trying to take advantage of this trend. Facebook's proposed Libra digital currency is a radical step for an internet operation (and despite initial enthusiasm from banks and card companies this is fading so much that Libra may never take off), but China and Uruguay have announced the launch of digital currencies (the preferred term, not cryptocurrency), while many other central banks have announced studies into the issuance of such currency.

## Convenience a Driver

Convenience is one of the key drivers for a consumer, but we see that convenience and security are uneasy bed fellows. Security has a tendency to introduce 'friction' that slows down the transaction process. To date the payments industry has not wanted that friction since it might slow down the changeover to the new payment tools. The scale of the losses though, is so significant that the EU has introduced new requirements to counter these losses as part of its 2015 Payment Services Directive (PSD2).

The EU Strong Customer Authentication (SCA) legislation requires two-factor authentication for payments over €30. This means the use, for example, of a PIN code for a contactless payment or a separate authentication code sent to your phone to be used alongside your card details if paying online. Merchants no longer have a say as to whether they require second-factor authentication from their users. Moreover, every fifth transaction below that €30 threshold will be challenged, as well as when the combined value of transactions exceeds €100. The deadline for the implementation of the SCA legislation is now 31 December 2020 (a delay from the original September 2019).

## The Non-Monetary Value of Cash

With this trend to digital payments we have to examine the issue of resilience. We've seen the impact of some system failures in the banking and card sector. In much of the world, if there is a power outage of more than a day or so, then the disruption will be very significant. ATMs won't work, but the whole payment infrastructure will also fail along with the entire retail system. The reliance on power for lighting, heating/cooling and security will have an immediate effect in addition to the stock control, accounting and payment systems. If it is a communications failure, whether back-end, front-end or in between, the impact can be managed or even delayed. Cash can bridge that gap so long as it is for a short period, up to 48 hours perhaps – as long as there is cash available in the system.

Digitisation also raises the possibility of denying some sectors of society their ability to participate in their local economy. People are unable to use smartphone-based payment systems if they don't have this necessary gadget. That includes:

- People in many parts of the world where smartphone penetration is relatively low (eg. 24% of the population of India has a smartphone[11]);
- The elderly, many of whom don't understand how to use smartphones or no longer have the dexterity to do so and haven't mastered voice control;
- People who can't afford a smartphone;
- People who have a smartphone but live or work in areas with poor network coverage;
- People who have neither a bank account nor payment cards;
- People who simply don't want all their transactions recorded (which includes criminals, but there are also legitimate reasons for transaction anonymity);
- The one-seventh of the world's population who don't have any formal identity document.

Let's not forget that cash is a great leveller; everyone has access to it (in larger or smaller amounts) and it allows anonymity as well as fast transactions.

## Conclusion

Payments are changing. Cash is being used less for transactions, replaced either directly by cards or indirectly by mobile payments linked to cards. The rate of innovation and change is in danger of leaving some people behind and creating significant risk should the electronic payment system fail for some reason, leaving people unable to pay.  Another risk is the vulnerability of these systems to hacking and other methods of data misappropriation, with all the attendant dangers of identity and financial theft that result.

In addition, the regulatory landscape is struggling to keep up and criminals are exploiting the new paradigm of payment being about value linked to identity rather than value linked to presence.

This brings us back, of course, to how governments and businesses can secure identity with confidence, the proof of identity and how it can be proved at the point of transaction. Perhaps here the physical meets the digital to allow the future to happen.

[11] Pew Research Center

# Digital Identity or Digital ID Credentials?

- Every day millions of travellers get home faster because they can move quickly through ports of entry and exit using their digital identity;
- Tens of millions of patients get better treatments because their doctors can gain access to their digital medical records;
- And billions of consumers can purchase goods from across the world, choosing from a seemingly infinite showroom using a username and password.

All of these processes are conducted with relative ease by asserting that you are who you say you are by demonstrating your credentials against a pre-existing digital record.

By digitising data, you translate information into a format where it can be read by a machine and operated on by an algorithm. This is the basis of the advantage of digital identity over its analogue counterpart but also its potential vulnerability, because whilst a machine is highly efficient at confirming the truth, or otherwise, of a user's credentials, it is not so good at determining the provenance of the credentials. It may also be vulnerable to the theft of this digitised personal data.

We will look at examples from a range of sectors where a system uses a digital credential to allow access. In our current phase the main commercial driver is user convenience, which leads to the ongoing tension between efficiency and security that is being played out today… and which will be for some years to come.

## The Mobile Driver's Licence

The driver's licence has long been established as a useful tool of law enforcement. The trend of migrating a driver's licence onto a smartphone is well advanced. In Wyoming, one of the US states that is piloting mobile drivers' licence (mDL), the system displays the personal data of the driver (name, address, date of birth) and other data (date of issue, restrictions and rights) in a driving licence format that is comparable to its physical counterpart *except that it contains none of the physical security features that might be used to authenticate the card.*

These physical security features tap into the human tools that any document inspector naturally carries with them: the raised laser engraving which creates a tactile response, translucent elements that create a visual response, and diffractive components that invite the inspector to view the document from different angles. With the use of simple portable tools such as a magnifying glass or a UV light other higher levels of security can be deployed.

Interestingly, to give confidence to the driver that they are maintaining control over their data, the enforcement officer has to provide evidence that they have authority to view the data and that it will not be shared beyond the specific purpose of the enquiry. Before the licence holder releases certain types of data[12] they can use the camera on their smartphone to read a QR code on the officer's ID badge. Only after the code has been authenticated will the data be released to the device associated with the credentials.

[12] www.gemalto.com/govt/traffic/digital-driver-license

At the moment, the mDL is being piloted to replicate the traditional functions of a physical licence but plans for extending its use to other identity verification tasks outside law enforcement are in the pipeline. Health insurance enrolment and online purchases are just two of the applications where the US mDL might be used. This would give it the status of a digital breeder document upon which other digital security might rest. With the onus on convenience, what safeguards will be put in place to ensure verification of the online application process for future mDL applications?

With such dependence on the driver's licence as a means of establishing identity in the USA it is no wonder that additional safeguards have been put in place. In an effort to prevent driver's licence fraud, the faces of more than 120 million people have been collected into state-level driver's licence searchable photo databases – about a half of the licensed drivers in the USA. The FBI already has agreements in place that grant it access to the driver's licence databases of ten US states and many more share information with state, local and federal authorities through so called 'fusion centres'[13].

## Towards a Digital ID Card

Outside the USA, proving your identity to government agencies is less dependent on the driver's licence and more on the national identity (ID) card, with some countries moving towards a digital version of this card.

South Africa is one of the countries moving in this direction. The current South African ID card has replaced the green bar-coded identity book that was used as proof of identity when applying for voter registration, a driver's licence travel documents or when opening a bank account[14]. The card combines many of the physical features that protect the authenticity of the card itself with the digital security that controls access to the data.

But for South Africa's Home Affairs National Identity System (HANIS) the direction of travel is away from the physical and toward the digital. Director General Apleni, speaking to BiometricUpdate.com at ID4Africa2017[15] , made the case that technology in the form of iris and voice biometrics not only improves security of the ID card but reduces corruption and fraud in the country.

The promotion of digital technology solutions over physical checks is also evident in South Africa's Home Affairs process for applying for a visa, where face and fingerprint digital data is recorded as a part of the application[16], as it is in several other countries, including the USA.

## Personal Data at Risk

But with security researchers continuing to find vulnerabilities in electronic identity systems it may seem premature to place so much confidence in technology solutions. In November 2018, during a test of software used to authenticate an identity using the embedded RFID chip on the German identity card, SEC Consult identified a security vulnerability that allowed an attacker to impersonate a user on certain online service platforms. In this instance, SEC Consult[17] gave the German authorities prior warning before going public with their findings and a patched version of the software was created.

[13] www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html

[14] www.gemalto.com/govt/customer-cases/south-africa

[15] www.biometricupdate.com/201705/evolving-partnerships-drive-south-africas-digital-identity-program

[16] www.vfsglobal.com/dha/southafrica/faqs.html

[17] sec-consult.com/en/blog/2018/11/my-name-is-johann-wolfgang-von-goethe-i-can-prove-it/

There was no such easy fix in the well-reported vulnerabilities of the Estonian eID card (see Digital Systems and Document Security, above). The fix for this entailed suspending the certificates associated with 750,000 cards and updating them with new credentials.

Enrolment in a fully digital ID system has the potential to reduce the likelihood that a fraudulent document will be intercepted, because once the documents that validate the identity are used in the application process there is little chance that they will be interrogated again. Your digital credentials will now be established and all you have to do to assert them is to present your username and password. The chance that a fraudulent birth certificate, marriage certificate or other physical breeder document will be detected is related to the frequency of inspection, which essentially drops to zero.

## Digital Health

Electronic Health Records (EHR) offer the prospect of providing accurate, up-to-date and complete information about patients at the point of care. Their use is being heavily promoted in the USA by government[18] through a series of financial incentives to medical professionals.

The transfer from physical to digital records is particularly attractive when you consider the lifetime of the record which will be, by definition, at least the lifetime of the patient. During that time the accumulated data will be enormous and if stored on paper it will be vulnerable to flood, fire, theft and misplacement. To give some context to the amount of data stored on a patient's medical record throughout their lifetime, one estimate puts the amount of data gathered per patient per year[19] at around 80 megabytes, which is roughly equivalent to 20,000 A4 pages of text.

So, the benefits of moving to EHR are clear but not without risk. These risks fall broadly into two categories:

- The housekeeping of transcribing paper-based documents into a digital format –quite overwhelming but manageable;
- The increased risk to privacy and security now that the record is digital (which is the bigger problem).

Whereas the paper document is archived in a single physical location, the digital version can be transferred with ease. This certainly makes it easier to 'accompany' the patient should they relocate or have a spell in hospital, but massively increases the scale of the potential harm should the record fall into malevolent hands. Again, in the USA, the medical health records (physical and electronic) of patients are protected by the Health Insurance Portability and Accountability Act (HIPAA), of which the Privacy and Security Rules[20] can impose penalties of up to $50,000 per violation; at the time of writing there have been a handful of prosecutions brought under this act.

Medical identity theft, though rare, can be devastating. The abuse falls mainly into two categories:

- Someone assuming the identity of another person to gain access to medical services;
- Health records stolen *en masse*.

In a well-known case a medical office worker stole the electronic records of over 1,000 patients, selling them to a relative who made nearly $3 million by filing medical claims[21]. Of course, the physical nature of paper records limits the extent of any theft but with the transition to electronic records, it seems reasonable to assume that we will witness an increased scalability of this fraud.

[18] U.S. Department of Health and Human Services Centers for Medicare & Medicaid Services 42 CFR Parts 412, 413, 422 et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule

[19] geekdoctor.blogspot.com/2011/04/cost-of-storing-patient-records.html

[20] www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[21] The IATA-ICAO Tension www.bu.edu/jostl/files/2015/02/Hiller_Web_171.pdf

The Chinese government is also encouraging the switch to online medical records, proposing to make hospital records available through a centralised system. Most hospitals in the country have negligible protections for their digital patient records, so making these available through a central system means they will be vulnerable, but the government project calls for security systems to be written after the records have been centralised.

## The IATA-ICAO Tension over Travel Documents

The tension between efficiency and security is perhaps most stark when considering travel documents. The One ID programme currently promoted by IATA advocates a near-future where passengers enrolled in the programme 'can further streamline their journey with a document-free process based on identity management and biometric recognition'[22]. The key drivers for One ID are, firstly, user convenience – with a single identification being recognised and accepted at all travel touchpoints during the traveller's journey; the traveller is freed from repetitive processes, resulting in less queuing. A close second to user-convenience is cost reduction – with IATA claiming that One ID 'will improve staff productivity by reducing time spent on manual ID checks'.

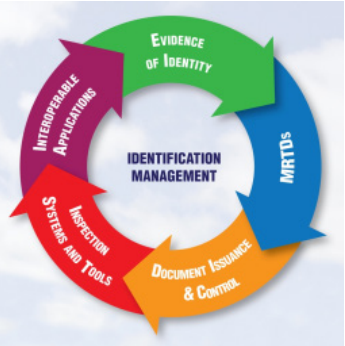

Evidence of Identity
MRTDs
Document Issuance & Control
Inspection Systems and Tools
Interoperable Applications
Identification Management

Figure 3: ICAO's schematic for TRIP.

ICAO's Traveller Identification Programme (TRIP) takes a more holistic approach to the different elements of traveller identification management, going so far as to cite that 'credible evidence of identity, involving the tracing, linkage and verification of identity against breeder documents to ensure the authenticity of identity'[23] should be a key element of the overall TRIP strategy.

Whilst ICAO does not want to halt the inexorable progress of technology through the assertion of digital credentials, it sees advantages in a period of integration with the existing processes of manual inspection of physical documents. This philosophy is perhaps best captured in the title of the recent 15th Symposium and Exhibition on the ICAO TRIP – 'Bridging the Physical-Digital Document Divide'[24].

In each of the cases above, the primary purpose of creating and recording personal data digitally is to improve convenience for service users and providers and it seems undeniable that that trend is set to continue.

But there is a risk that further adoption of digital identity may be greeted with push back until key issues of trust, privacy and security can be addressed. Could this be an opportunity for commercial entities with knowhow and experience in the security arena to guide users in the proper balance between physical and digital safeguards to ensure that security is built-in and not merely a bolt-on?

[22] www.iata.org/whatwedo/passenger/pages/one-id.aspx
[23] www.icao.int/Security/FAL/TRIP/Pages/default.aspx
[24] www.icao.int/Meetings/TRIP-Symposium-2019/Pages/default.aspx

RECONNAISSANCE

# DIGITAL DOCUMENT SECURITY™

**5–7 OCTOBER 2020**

**Vienna, Austria**

Explore the transition from the physical document world to the world of digital financial transactions and identity credentials, while also looking towards the application of next-generation technologies in this important field

digitaldocumentsecurity.com

**Key Dates:**

**01 April 2020** - Summary Submission Deadline

**03 July 2020** - Last Day Early Booking Discount

**04 September 2020** - Audio-Visual Presentation Deadline

**05 October 2020** - Conference Start

# The Way Forward?

So where are we in this transition and can we identify the positives and the negatives of this switch towards digital systems? More specifically, can we not only identify any negatives but can we take steps to negate them?

Before considering those questions, let's remind ourselves of our current reality:

- China and Sweden may be well on the way to becoming cashless societies, but the reality in most of the world is that 85% of retail transactions and 60% of retail transaction value globally is still in cash;
- Singapore Changi, Beijing Daxing and some other airports allow document-free departure passenger experience, but no airport in the world allows non-domestic arrivals to enter without a passport or similar ID card (counting the EU's Schengen area as domestic).

So the reality is that while some countries are very far down the road to the use of phones or contactless cards for retail purchases, most people in most countries still depend on cash.

Similarly, while there is much discussion, research and some pilot projects into the use of mobile ID, only in Estonia is the switch to mobile or digital ID much advanced.

As we enter the third decade of the 21st century, physical banknotes and physical ID credentials remain the norm, with inspection of these documents by people and machines remaining the essential step in detecting fraudulent documents.

But for how long?

There is absolutely no doubt that there is an inexorable trend towards the digital. Some will always favour cash – for its anonymity if nothing else – but the relentless global expansion of Tencent and Alipay, as well as the weight of Silicon Valley giants like Apple and Google, will see more people relying on the networked micro-computer (more usually referred to as a smartphone, but 'micro-computer' is a more accurate designation) in their pocket or handbag.

Meanwhile, the International Standards Organization (ISO), the American Association of Motor Vehicle Administrators (AAMVA) and the European Commission are drafting standards or guidance for digital ID credentials, and the International Civil Aviation Organisation (ICAO) is looking into document-free travel.

Yet the old caution of *caveat emptor* (buyer beware) applies. Consider the success of human senses in detecting fraudulent physical documents and compare this with the proven vulnerabilities of digital systems, as shown by the unremitting stream of reports of hacks and data theft – Travelex's ransomware problem being only the latest major example.

We need to enter this new digital world with our eyes open, with our senses aware and with our suspicions honed.

We need to inculcate in the developers of digital systems the same awareness of protection, the same intrinsic commitment to document and data protection, that the physical document community has acquired from its 1,000-year history.

The challenge is to make sure this is achieved; to make sure that the first thing a developer considers is not 'how do I do this?' but 'how do I do this so it is secure?'.

Reconnaissance can't give you the answers as to how this happens, but we hope to do our bit to facilitate the asking of the questions and the exploring of the issues. So watch for information about the Digital Document Security Conference in Vienna on 5-7 October 2020 and look out for our resource publication – due for publication in late 2020 – on the whys and hows of the transition from physical to digital security documents. And read our regular newsletters which set out the latest developments in physical and digital document security. We are a conduit, a forum, a vehicle for discussion and exchange of information and ideas. But our driver is the security of data – our data, as individuals, as consumers and as members of the public.

RECONNAISSANCE DIGITAL DOCUMENT SECURITY™

www.digitaldocumentsecurity.com