Rethinking digital identity

Michael Salmony

Received (in revised form): 14th February, 2018

equensWorldline SE, Hahnstr. 25, 60528 Frankfurt am Main, Germany
Tel: +49 172 6867163; E-mail: michael.salmony@equensworldline.com

Michael Salmony

Michael Salmony *is Executive Adviser at equensWorldline SE. He is an internationally recognised leader on business innovations, especially in the digital and financial services space. He is a board-level adviser to major international banks, industry associations and European decision-making bodies, as well as national and international boards. He is also a keynote speaker at international events who makes regular media appearances on the subject of advances in finance and has been quoted extensively in various publications around the world.*

Abstract

Massive cyber breaches and identity frauds are daily news. Users experience endless frustration with countless passwords and registration procedures. Governments suffer from poor online acceptance and merchants experience high fraud costs despite massive IT investments. Perhaps it is time to rethink the topic of identity. This paper argues that we should move from verifying the full 'identity' of a person or company to very specific 'attribute verification'. This should be done not only for people and companies but also for devices, apps, bots and more. The paper advocates the use of intelligent data-driven authentication and a shift away from the current dependence on government-issued documents, faxes/utility bills, user ID/passwords and rigid two-factor procedures. It argues that the future should be based upon pseudonyms rather than full identification and will describe the very few occasions when full anonymisation is actually necessary. The paper proposes a federated model that connects the many current silos of organisations providing attributes with the many organisations that wish to use them, employing an open four-corner model instead of today's point-to-point interconnections. Finally, it provides arguments why banks could and maybe should play a more active role in this space, notably to realise benefits for all in the emerging Open Banking and platform economy.

Keywords: identity, authentication, pseudonymity, eIDAS, GDPR, privacy, bank-ID, attribute verification, four-corner model

INTRODUCTION

> 'If you solve authentication, everything else is just accounting' (Ross Anderson, Professor of Security Engineering, University of Cambridge)[1]

In the last few years there have been massive cyber breaches and rampant identity fraud.[2,3] In response, everyone now suffers the daily chore of dealing with countless user IDs and passwords, each with their own format rules, and completing endless forms on the internet. It is time for modern identity solutions that are secure, simple-to-use, scalable, private and pervasive; in other words, '3SPP authentication' (pronounced 'triple S-P-P').

A 3SPP authentication system benefits from the following features:

- *Secure:* Authentication should use modern technology, not 1970s passwords, and employ a distributed, federated system rather than a centralised infrastructure, ensuring it is not vulnerable to a single point of attack.

Journal of Payments Strategy & Systems
Vol. 12, No. 1 2018, pp. 40–57

- *Simple-to-use and situative:* Authentication must find the right trade-off between convenience and security. There are times for friction-free payments (eg when buying coffee or paying for a car journey via an app) just as there are times when multi-factor authentication is the right choice (eg when buying an expensive television). Simply put: the user experience must be balanced with the risk management of the merchant/government/bank.
- *Scalable:* Authentication must be highly reliable in huge volumes across all countries, services and platforms. At its core, this is a high-scale transaction business.
- *Private:* Authentication should reveal no more data than is necessary and only to those parties that need said data — and only where the user has explicitly consented.
- *Pervasive:* Authentication requires a reusable interconnected solution under a common framework across all channels, geographies and devices for government, banking and commerce.

The options for realising the above goals will be explored in the following text.

THE NEED FOR A FEDERATED APPROACH

Current EU initiatives such as eIDAS seem largely focused on government and public sector issued identities and how to make them interoperate across Europe. However, the time is ripe to think beyond this (Figure 1). Instead of the current isolated silos from government and industry, what is needed is:

- a *federated* system,
- where *multiple* identity providers (government, commercial entities, social media, mobile operators, banks etc) verify the rights of access,
- which can then be used by *multiple* relying parties (government services, online platforms, internet of things (IoT) etc) under an open but secure identity regime.

This will involve many parties and industries. Some will provide verification of attributes; some will want to have attributes verified; others will provide the interconnecting services and organise the rules between these parties. This will be a diverse ecosystem that will require much alignment

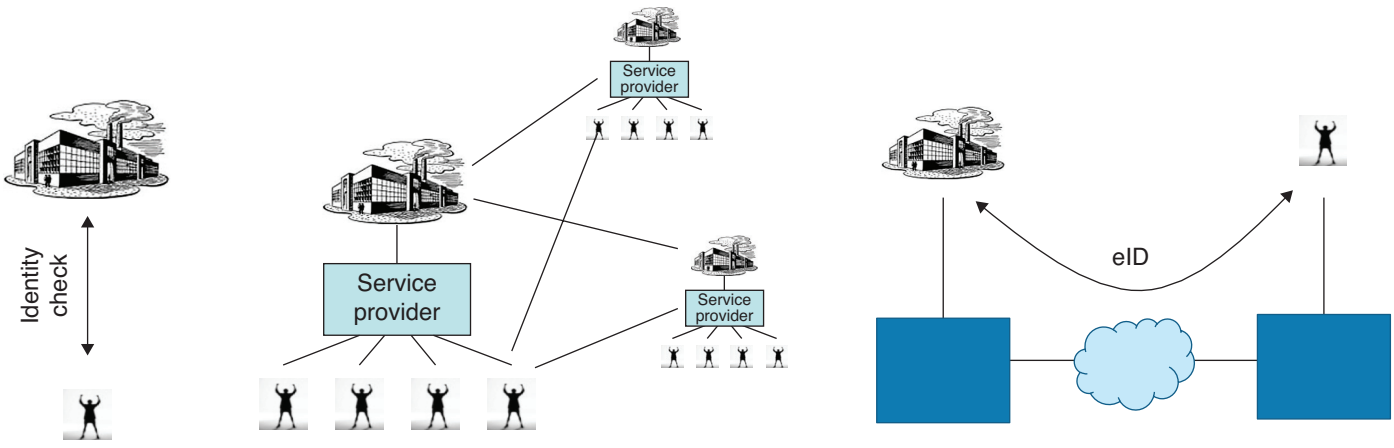
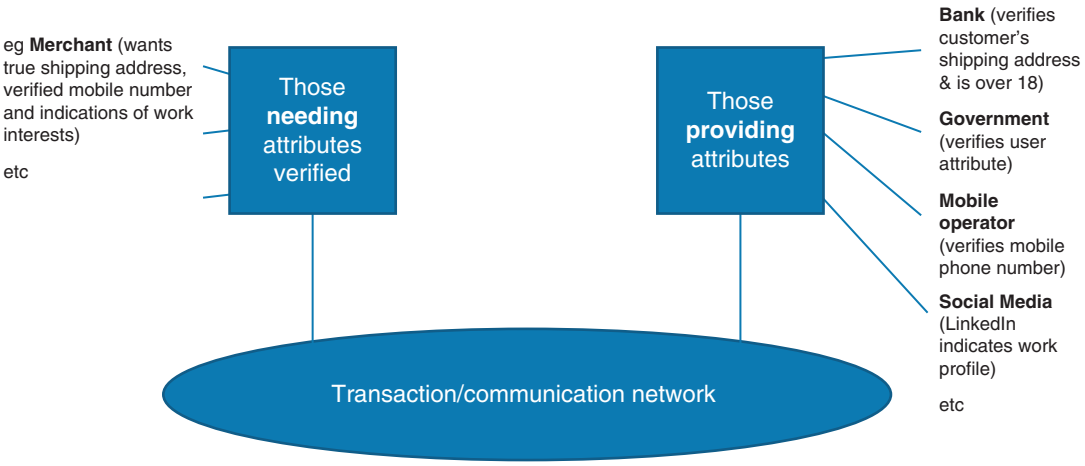


Figure 1: The evolution of authentication
Source: equensWorldline 2018

Figure 2: Federated authentication scheme



Source: equensWorldline 2018

and coordination. However, as with many other complex ecosystems that span several parties (eg worldwide e-mail, international payments), it can be done successfully if there is sufficient need and opportunity.

Many parties are already playing significant roles in the identity sphere. Indeed, all online services, physical point-of-sale (POS) solutions and e-government services require some form of registration/identification/authentication, and many service providers (notably the social media, mobile telecommunications industries and countless technical solution providers) are stepping up to provide these services. In addition, as this paper will explore, there are also roles for banks in this emerging multi-party ecosystem.

MODERN TECHNOLOGY: AN INTELLIGENT RISK-BASED APPROACH

Clearly, it is prudent to employ modern technology rather than 1970s-style user ID and password combinations (as is largely the case today) or rigid two-factor[4] authentication where intelligent, risk-based authentication is the exception.[5]

Someone who buys their coffee at the same local outlet every morning can enjoy a simpler authentication process than someone who buying an expensive television in a place far from home. These smart solutions use — if the user is happy to allow this — information about a person's habits, location, devices,[6] and maybe even social media profiles, using smart analytics to provide risk-based seamless recognition (which the customer likes), massive fraud reduction (which the banks like) and much reduced transaction abandonment (which merchants like). Indeed, when it comes to 'data'/'user'-based authentication, thousands of businesses around the world are now turning to the mature solutions offered by providers such as ThreatMatrix, equensWordline, iovation etc.

FORGET IDENTITY — THINK PSEUDONYMITY

Importantly, it is worth noting that one should not actually be talking about 'identity' at all. Formally speaking, 'identity' is a term used to identify a natural or legal *person* (see, for example, eIDAS Art. 3 'Definitions' §1[7]). Indeed, the topic can no longer be restricted to people and companies, as one must also identify/authenticate programs (apps, robots), devices (IoT) and more.

Figure 3: Why does the cigarette machine need to know the customer's name and bank account details? Why does the hotel, which keeps a copy of guests' passports, need to know their ethnicity, date of birth, or the visas of the countries they have visited?

Source: equensWorldline 2018

Very rarely is a real name or true personal identity actually necessary. *Pseudonymity* is not just a better way forward, it is also germane to the matter of improving privacy.

A cigarette vending machine may be under legal obligation to verify that the customer is over 18 (Figure 3); however, the customer's name and bank number is none of its business. Likewise, the many businesses that take copies of people's passports do not need to know their ethnicity, place of birth, nor the visas of the countries they have visited. What is required is an *attribute* — not an identity. Vending machines that require users to insert a driver's licence as proof of age or hotels and car rental companies that take copies of people's passport are in contravention of the EU General Data Protection Regulation (GDPR) as they have access to far more personal data than they require. These simple physical examples surely apply also to the countless online services that regularly request data much beyond what is required and must henceforth surely be illegal.

ATTRIBUTE VERIFICATION INSTEAD OF IDENTITY

If one considers that both physical and online services will in the future be limited to requesting only the attributes they really need, they will have no excuse for requesting more (especially not an entire physical identity) once they have a proper 3SPP solution in place.

Attribute management, which preserves the principle of data minimisation as opposed to identity (which reveals the whole individual), may best be realised using a handle or pseudonym. A pseudonym can take many forms in practice: it may be a simple virtual handle/alias/avatar or a digital cryptogram/token or a physical chip or other form factor. What is important is that use of the pseudonym is uniquely controlled by the user without revealing his identity, as does a passport.

Should the real person employing the pseudonym attempt something unlawful, like posting racially-offensive content or illegally accessing bank accounts, then law enforcement (and no one else) can trace the pseudonym back[8] to the perpetrator's real physical identity.

By law, only the state issues documents verifying real personal identities, and access to real identities should largely be restricted to the state.[9] Only in a very few cases is it essential to know exactly who a person is,[10] such as in the event of marriage, imprisonment or crossing a state border. These are all state-controlled

actions. Non-state actors, and even most other government services, are largely best served with non-identity pseudonyms.

> 'Pseudonymisation is gaining traction among modern electronic identification systems as a privacy enhancing technique that can significantly reduce risks of personal data misuse.'[11]

ANONYMITY

At the other end of the scale (Figure 4), true anonymity (ie without any possibility of tracing back to the real individual) is sometimes demanded. Again, however, there are only very rare cases where this is truly justified, or even legal:

- A well justified case for true anonymity can, for example, be found for an internal company satisfaction survey. The management needs to convince staff that the data will be collected anonymously and reliably assure everyone that no individual employee's answers will be identified. The impossibility of tracing the answers back to the individual is fundamental to securing valid, open feedback.
- The topical cases of personal abuse (#MeToo) and corporate whistleblowing may also appear to be justified areas for anonymity. However, to also protect the rights of the individual/company being accused, it is important to allow the facts to be verified by an independent body, and hence the source must be identifiable to a neutral party.[12] Again, a pseudonym protects the individual's identity but allows law enforcement to connect to the real person if needs be, making it the better solution.
- In payments, a public debate on a true online cash equivalent — with anonymous exchange as in physical cash — is still ongoing. However, many open questions, not least about the potential for money laundering, suggest this idea will never see the light of day. Nevertheless, some argue strongly that there is a role for *pseudonymous* cash.[13,14,15] This is to balance the demand for individual privacy, also in the areas of digital fund exchange, with the need for law enforcement to expose the identity of parties in the event of misuse. However, the past history of this topic is strewn with the corpses of high-investment failures (eg Mondex), indicating that any future for pseudonymous cash may be thorny.
- More generally in the areas of banking, truly anonymous online payments are clearly forbidden under due diligence and know your customer (KYC) regulations, as well as regulations designed to prevent money laundering and the financing of terrorist activities. Instead, the true personal identity of the payer and payee must be reliably verified and law enforcement able to step in if terrorists are financed. Allowing fully anonymous online payments would put bankers in prison.

In general, Europol notes, not surprisingly, that 'The growing misuse of legitimate anonymity … poses a serious impediment to detection, investigation and prosecution'.[16]

Thus, with very few niche exceptions (eg anonymous employee surveys), the call for true anonymity is difficult to justify.[17]

Figure 4: Scale of personal identification — the future is in the middle

Source: equensWorldline 2018

With this in mind, the large body of future authentication will do well to revolve around pseudonymity. The other extremes — true full personal identity and true unresolvable anonymity — may be the exceptions.

POTENTIAL ROLE OF BANKS: THREATS, ASSETS AND OPPORTUNITIES

There is, of course, no God-given right to banks in this space. Indeed, this key space of identity and attribute verification will be very heavily contested by many industries. There will even be some well-justified opposition to banks providing identity services.[18]

In addition, some conservative banks may actively prefer not to enter this space. Fears around liability, concerns regarding business cases, organisational inflexibility, IT demands, and a general preference for sticking with familiar processes etc, will make some banks reticent. However, those banks that choose not to engage must be clear that they risk being further intermediated (and thus losing more contact with the customer and seeing less data), being further relegated to a role as commodity provider, further leaving the position of trusted party to others, while letting others benefit from the new business models and enjoy the new revenue streams.

The more forward-thinking banks see the unique opportunities here. First, they see that they hold key assets that can be leveraged: maybe the best hard data, maybe the best network, maybe the most robust infrastructure and maybe the most credible role as trusted partner. These assets can then be employed for new value propositions to customers, for business models (also based on the new open application programming interface (API) economy) and to save costs. These aspects will be addressed in the following.

If the user gives informed consent to release selected data on/about his account, then banks can provide hard verification of attributes (eg age of user, home shipping address, whether his television licence has been paid for etc) based on KYC processes and transaction history. This is in contrast to many other industries (notably the very active social media) which can typically only provide indicative information (eg 'seems to be quite interested in politics', 'said she was over 18'). Of course, both hard and soft data will be valuable to online services — but the hard data, combined with other external data sources, will be the main basis of the new data-driven economy, as one already sees in the most successful emergent FinTech/RegTech/InsurTech/PayTech models.

The banks not only have key hard data, but also a unique network (built for payments) that interconnects people and companies across the world. The federated 3SPP approach linking multiple attribute providers with multiple services requestors, will likely be based on a four-corner-model (see Figure 2) that is familiar to banking and payments and is another key asset that banks have, indicating that this may be a real opportunity to leverage existing investments and infrastructures.

Considering that the financial services industry is the most heavily cyber-attacked industry,[19] it is holding up well compared with other sectors (see Figure 5).[20] This is due to the industry investing particularly heavily in IT security, new technologies and privacy and being highly regulated and monitored. The industry is, of course, not invulnerable,[21] but the European banking industry in particular has an above-average record with respect to withstanding cyber crime and protecting user data.[22] All stakeholders should welcome the input from such a security/privacy-conscious and robust industry.

In view of all these assets, it is no surprise to see a number of banks (both individual

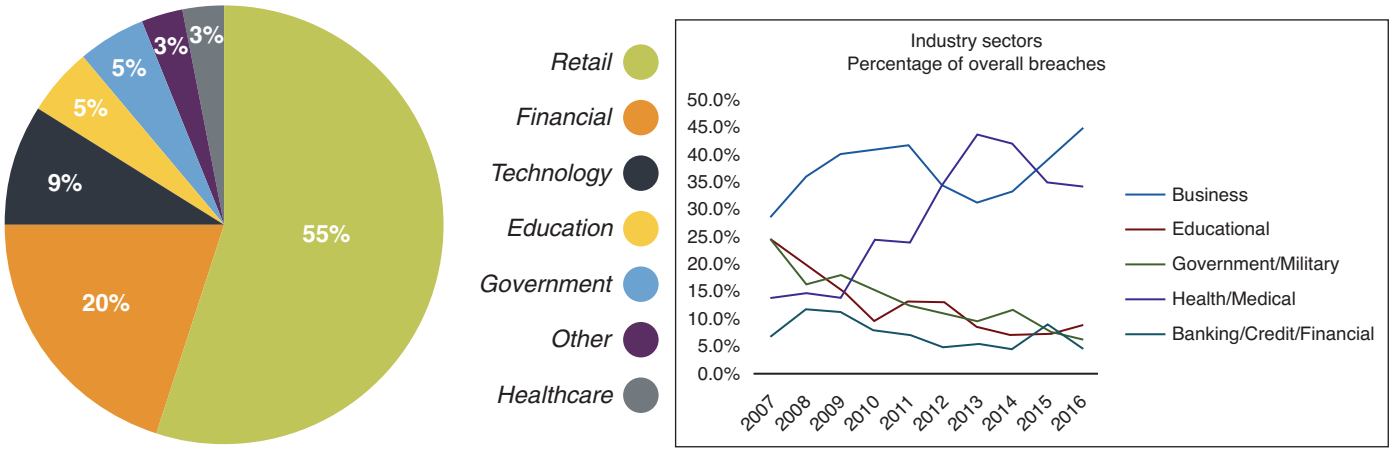


Figure 5: Data records stolen/lost by industry
Source: Almansi, A. (2015) 'Financial Sector Cybersecurity: who's in charge?', available at: http://pubdocs.worldbank.org/en/370701446574212560/pdf/Aquiles-Almansi-Cyber-Security-Implications-for-the-Financial-Sector.pdf (accessed 10th January, 2018); Identity Theft Resource Center and CyberScout (2016) 'Data breaches increase 40 percent in 2016, finds new report from Identity Theft Resource Center and CyberScout', available at: https://www.idtheftcenter.org/2016databreaches.html (accessed 10th January, 2018).
According to the above, the financial services industry had 'only' 4.8 per cent of the breaches and lost 'only' 0.2 per cent of the records, and continued to be the most robust industry sector.

institutions, such as Barclays, and whole geographies, such as the Nordic countries) and payment-related services (eg Klarna, PayPal, Swish, iDeal) already embracing this new opportunity to move from core banking/payment/accounts to higher-value authentication services (from age verification to full legal online contract signing) for third parties.

These forward-thinking players typically see it first as a *strategic* opportunity to win back their position as the customer's main trusted partner against the onslaught of other platforms now offering very non-private online 'identity' services.

Secondly, it can be a new *commercial* opportunity. Although one cannot in all likelihood charge end-user consumers, the corporate case for providing identity services to mobile operators, online services, mobile solutions and governments is very different. Providing companies with reliable authentication solutions makes for good business: the business-to-business margins are much better than for payments and the volumes are much bigger too (every day, people log on/identify themselves to corporates, governments and online services many more times than they make payments — and when IoT devices and mobile apps start needing identification, then this volume will surely explode).

The new services also allow more information to be gathered about the customer, yielding data which can be used for further commercial services of benefit to the customer.

Finally, it is an opportunity to leverage existing infrastructures (worldwide interconnectivity) and investments (KYC, online security methods) for further valuable services. In this context, 3SPP could be used to reduce the cost of compliance. By reusing shared infrastructure and maybe also reusing some properly verified attributes from other service providers, smart banks are able not only to help others but also to reduce their own costs with respect to due diligence and

KYC activities, and regulations designed to prevent money laundering and the financing of terrorist activities.

BANKS MUST OPEN UP UNDER OPEN BANKING/PSD2 ANYWAY

New authentication services towards third parties are already being provided by forward-thinking banks (eg CA, ING, BBVA, Nordea, Fidor) under Open Banking.

This comes as part of the move towards the connected API economy. Smart banks, knowing that the Second Payment Services Directive (PSD2) requires them to open up with standard/free APIs anyway,[23] will also offer commercial value-added APIs to provide bank-verified age ID, bank-verified shipping-address ID etc[24] (see Figure 6) as new business propositions. This generates value and revenue and helps to put them in an offensive position that embraces the business potential of the regulations, rather than a defensive position of basic compliance.

Once the Open Banking paradigm is truly embraced, there will be many more APIs (see Figure 7) beyond what is required by compliance (ie beyond just PSD2 APIs for payment initiation services (PIS), account information services (AIS) and payment instrument initiation services (PIIS)). Merchants are actually asking for *value-added* APIs where the payment is not just initiated (PIS) but actually executed with some confidence (the focus of the Euro Retail Payments Board PIS 2017[25]), or that recurring payments are managed, or that funds can be reserved for later use, or that payments can be returned, and much more.

Beyond payment initiation there will be the — likely much more disruptive — potential of access to transaction data. This

Service	Acronym	Parameters in	Result out	
Payment initiation	CAPS-PI	from IBAN, to IBAN, amount, [QoS] TPP cert	CT initiated w best effort [guarantee, real time, …] /insufficient funds/other error	Mandatory APIs under PSD2
Sufficient funds	CAPS-SF	IBAN, amt, reserve time, TPP cert	yes/no, reserved until <timestamp>	
Balance information	CAPS-BI	IBAN, TPP cert [all accts=y] [past=n days/all]	balance[s], [past statements]	
Account verification	CAPS-AV	IBAN, TPP cert	yes/no account exists	Optional identity APIs for added value
Identity information	CAPS-II	type of info requested, TPP cert	age verification, identity verification, postal address, mobile number, …	
Sign service	CAPS-SS	IBAN, doc/mandate, TPP cert	confirmation (eg mandate number) or fail code	
…	…	…	…	

Figure 6: Mandatory and commercial identity APIs under Open Banking
Source: Salmony, M. (2014) 'Access to accounts: Why banks should embrace an open future', *Journal of Payments Strategy & Systems,* Vol. 8, No. 2, pp. 157–171.

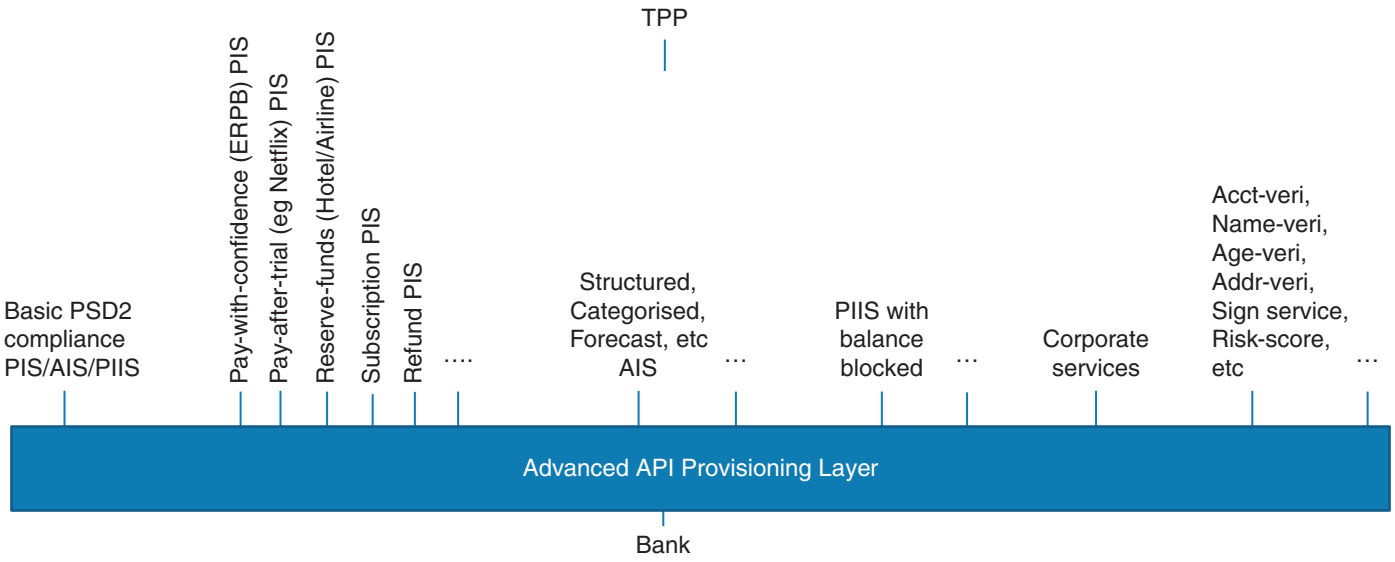


Figure 7: Value-added APIs, beyond PSD2 compliance, with commercial services that FinTechs, merchants and corporates really need (sample authentication APIs shown on the right)
Source: equensWorldline 2018

will again offer opportunities to go beyond what is required by legislation (ie PSD2 AIS API with just a 'screenshot' of the recent transaction history), but instead offer value-added structured/categorised data in XML for direct use by FinTechs.

One of the main beneficiaries of Open Banking may not necessarily be the retail customer — which is the current focus — but the corporate. This is just the same as in the discussion around 'Instant Payments', where again the biggest advantage may be to corporates,[26] rather than private end users as originally envisioned. Therefore, one can expect to see many commercial APIs being offered by banks to corporates, as they know they will be ready to pay for the added value.

Finally, in the context of this paper, forward-thinking banks will also open up a number of 'identity' APIs to allow merchants, FinTechs, apps, devices etc to verify whether a user really does own an account (without the current absurd method of sending a microtransaction), whether they are over 18, that their shipping address is correct etc, and even maybe offer yet more advanced services for signing and risk management.

The potential for banks and their users in Open Banking is truly endless.

All in all, one can see that there are many arguments — which many organisations are beginning to embrace — for banks and payment organisations to enter the authentication and identity domains.

DIVERSITY AND LINEARITY OF TRUST

As a final thought on another common subject in the identity community that may need to be revisited, this paper takes a closer look at the linear scale of trust. In eIDAS, for example, there are three linear levels of 'low', 'substantial' and 'high', corresponding to the confidence with which an individual is really identified, again associated with increasing verification 'factors' being employed.

This does not work when relying on attributes, as these cannot be put in a linear order.

As shown earlier, the future lies not in the verification of individuals but in the authentication of attributes:

- is she over 18?
- is he a student?
- is he employed here?
- has he paid his television licence?
- does this company have sufficient funds?
- can this robot open this door?
- is that really the company's address?
- is this application allowed to see my transaction history?
- should this speaker read out my balance
- … and so forth.

Such attributes cannot be meaningfully placed on a linear scale and must be managed without natural precedence.

However, although identities and attributes cannot be set out on a linear scale, there are some useful areas for linearity of trust. For example, linear confidence levels on attributes are increasingly being served by providers. Just as the linear (0–100 per cent) credit score reveals a confidence in a customer honouring his debts, this principle of a linear scale is being increasingly applied to other attributes. For example, social media channels rate the likelihood that a person is interested in a topic, while mobile operators serve a likelihood that a phone is in the vicinity of a particular location. The relying parties can then base their higher-level services upon these confidence levels.

By and large, however, trust is not linear. Regulation itself enforces some non-linearity, which may even be widely different within a single geography. Before PSD2 and GDPR harmonised the rules, in some Nordic countries personal data could not be digitally shared at all (even with user permission); in other Nordic countries, salaries (usually one of the most sensitive personal data elements) are published on the internet. Those are extreme poles of view in the same area and demonstrate a surprisingly wide range and non-linearity in such a narrow geographical region. Observations indicate that some diversity will continue even after general harmonisation of legislation through PSD2 and GDPR.

Of course, the widest variability is generally observed between geographies. This is due to regulation often being a reflection of a society's attitudes — and attitudes and cultures typically vary across countries and continents. Single individuals will, of course, differ, but to take one example, the scale of 'how much control people want', is typically highly disparate between Germanic and Latin countries.[27–29] In the context of authentication, this means that in some geographies, there may be a preference for verifying every transaction explicitly and having every payment checked by the bank,[30] while in others, the preference is for a more *laissez-faire* approach that prioritises a simple, convenient and smooth user experience with the minimum intermediate steps. Either preference should be respected and accommodated.

From these few examples one can plainly see that defining a common identity framework across Europe will be a challenge. There is significant cultural, regulatory diversity and the habits that people have formed are very different. Thus, a flexible approach like 3SPP, which allows different federated solutions to interoperate across different geographies and cultures, again seems a winning way forward.

Looking beyond Europe, the diversity in culture, habits and regulation is even more pronounced.

In Europe there are largely agreed on potentially global, free market, privacy-observing approaches. In China, by contrast, many external providers are blocked, local digital champions cultivated, and state-run identity solutions[31] rolled out with individuals' activities heavily monitored throughout.

While the citizens of Europe are largely reticent about central governments storing

biometric data, India has set up the complete opposite: the largest biometric system in the world — the Unique Identity Authority of India (https://uidai.gov.in), which contains the data of around 1.2 billion people.

All this diversity means that those that dream of a globally harmonised approach[32] will sadly but surely encounter severe challenges in the foreseeable future. It is currently too early to predict whether the long-term tendency will be towards world-wide alignment or whether cultural and political diversity will continue to fragment further. This topic merits further research and monitoring.

This is compounded by the fact that these diverse tendencies across the world are not static. Some attitudes (and hence regulations) are indeed very much in flux. In the USA, for example, people's attitudes towards privacy have traditionally been more liberal than in Europe.[33] There has also traditionally been a marked cultural reticence against control by any government.[34] However, after 9/11, Wikileaks, Snowden and other events, the attitude towards privacy/identity/government may be changing, and one can possibly see an emerging tendency towards a more controlled view on privacy.

In summary, the wide range of cultural mores across the world has led to different attitudes, regulations, habits and ultimately very different technical implementations. This interesting, colourful universe of human diversity cannot be hammered flat into simple linear scales. However, a flexible approach which respects this diversity and the fact that attitudes and regulations and technology — and eventually even habits — change, will provide a safe view towards the future.

SCENARIO: THE 'TERMINATOR'

To make the above considerations a little more tangible, the paper now provides an example of how the 3SPP approach could work in practice.

Consider a new digital service offering: the 'Terminator'. It allows a user to cancel conveniently any recurring contract online. Example subscriptions include magazine subscriptions, insurance, mobile phone contracts, public transport cards, streaming television/music feeds, cloud hosting services, an initially free trial that now incurs a fee etc.

Users are already employing such services by the millions to reduce their monthly expenses or to change to better service providers. However, such services today (eg truebill.com, aboalarm.de, online-kuendigen.at, comparison websites, even Emma in Figure 8) still require a good deal of manual labour: logging on to the termination site, logging on to the site of the service to be cancelled, downloading files of the data required, uploading the data back up to the comparison and termination sites, and finally, the downloading, printing and mailing of the legal document for termination.

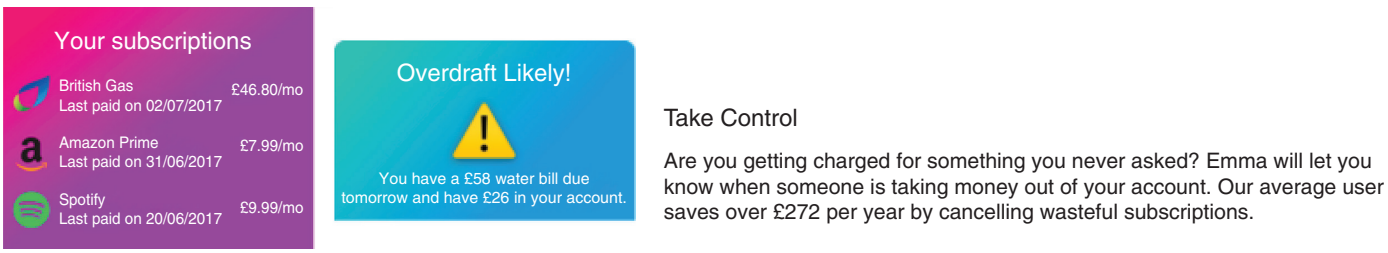


Figure 8: Managing subscriptions
Source: emma-app.com

A discussion regarding how to automate the full process (eg submitting and tracking the actual legal cancellation notice) is well beyond the scope of this paper, as is the current state of the industries involved. However, much benefit could be reaped were the termination service to improve the sign-on and authentication experience using advanced methods in a federated system.

Such a concrete future scenario could look like this:

> A millennial woman about to leave for work asks Alexa [the virtual assistant for Amazon's smart speaker] to read out her current bank balance. She finds this is lower than expected, so she opens her mobile banking app during her commute in order to review the last few transactions on her account. She sees that a number of subscriptions have been debited and thinks it is time to ditch the ones she is not using. She asks Siri [Apple's virtual assistant] to remind her in the evening to sort this out. Back home after work she goes to her Mac and invokes Terminator to scan through all her subscriptions (repeated direct debits) on all her accounts (bank, card, PayPal, etc). This comes up with a surprisingly long list of gym memberships, music streaming services, care packages for pets she no longer has, travel insurances already covered by her new business credit card and more. She puts a 'tick' against all the superfluous subscriptions and instructs Terminator to send a cancellation immediately to all these services she no longer uses. The cancellation notices[35] (properly legally formulated, with the right termination clauses/timings/etc) are generated automatically by Terminator. Next month, she can see from her increased bank balance that all unwanted subscriptions have indeed been cancelled.

This is a complex scenario with many actors[36] and, as such, a full description of every last step of the automated solution is beyond the scope of this paper. Nevertheless, a brief look at the first few steps is sufficient to identify a number of ways to improve the user experience.

For each of these steps, some authentication is necessary: she will not want Alexa to read out her bank balance to anyone else, she will need to identify herself to the cat care service, etc. If each of these steps involves a full, rigid two-factor authentication procedure, the benefit of the service will likely never be realised.

Using 3SPP, however, the flow could be as follows:

- Alexa senses that the user's Android smart watch is in close proximity and recognises the user's voice so has sufficient confidence that the true user is really present and thus reads out the balance to her. Alexa is on the bank's 'white list' for read-only data (eg reading out balances/transactions but not for initiating payments) so the device has access without requiring further credentials.[37] It is also common for this user to make this request at this time of day over this device from this location, further enhancing the confidence that she wants this action to be done. Obviously, all these permissions (Alexa–watch connection, proximity recognition, white-listing, monitoring of 'usual' behaviour) have been set up previously, explicitly verifying her consent.
- During its installation, the mobile banking app was linked with the physical mobile phone, the SIM card, etc and monitors continuously that the phone has not been tampered with. As this is all in order and as the user opened the phone using her fingerprint, the app can show the recent transaction history on the screen.
- Back home after work, she invokes Terminator for the first time, so this new service must be legitimised towards her online banks, her insurance providers, etc.

- First, Terminator must access her primary bank account, so the bank asks her to verify her consent for this. Her bank displays on the Apple Mac screen the message 'Do you agree that application Terminator on this Mac at this location may view direct debits of the last 30 days from this account until further notice?'. The user can press cancel, or modify (eg to limit Terminator's bank access to one day only until further notice) or ask for further information or, if everything is fine, hold her face to the camera on her Apple iPhone X for 3D facial recognition to verify the consent. The bank notes how, when and for how long the consent was given.
- This consent can be revoked by the user at any time.
- Terminator needs to verify that the user is over 18 as she needs to have the legal maturity to terminate contracts. Therefore, Terminator invokes her bank's age-veri-id API in the background to confirm this attribute/property. (The bank receives a small fee from the company Terminator Ltd for this.)
- Six months ago, the user signed up for a free trial of pet care services under the pseudonym of Molly2014 — this protects her true personal identity but allows the service, that has since started to charge a monthly fee, now to be cancelled.
- The process continues with the user being asked to interact only when it is *necessary* (ie for new actors, when she requests something unusual) and to give her *assurance* that nothing is done without her explicit consent.

Note that nowhere is a government-issued document involved and nowhere is the personal identity of the user revealed. There are no passwords, no user IDs and no 'factors': the user is asked only if there is a real need.

This is an open approach where solution providers — large and small — will compete heavily against each other to provide the most *convenient* and most *secure* user experience. These two demands are no longer at odds with each other, but can both be realised simultaneously and flexibly, according to the users' preferences with modern technology. This is a world with true opportunity also for small nimble new players and increased competition to provide the best solutions, and not only for dominant[38] online platforms.

Although not everything around this scenario can be covered in depth in this text, it would appear that with behavioural analytics, judicious use of guided interactions and modern technology, it is possible to realise an experience that is simultaneously:

- secure (background multi-dimensional verification that device is authorised, has not been tampered with etc);
- simple-to-use and situative (fingerprint and further biometrics, only interact when necessary);
- scalable (there is nothing in the architecture to prohibit wide deployment);
- private (no single social media or bank has all information — instead, it is distributed and federated); and
- pervasive (across all devices, platforms, service providers).

SUMMARY AND RECOMMENDATIONS

In summary, the time may be right to think more about secure, simple-to-use/situative, scalable, private and pervasive '3SPP' authentication. Banks could and maybe should play a key role in this space to protect customers from cyber crime and online fraud and to make their lives easier and truly enable the online and offline economy.

As hypothesised at the outset, this paper has shown that it is time to radically rethink the topic of authentication. As summarised in Table 1, the focus should be on verifying targeted attributes only instead of revealing

Table 1: Old thinking vs the possible way forward

Old thinking	*New thinking*
Identity is issued by a government and can be used by (another) government Basis is a physical identity document	It is largely not about identity — 'You' are not anybody else's business — To reveal the full identity is to act against the data protection principle of data minimisation and its use is illegal according to GDPR — Use pseudonyms, handles, alias instead — Very rarely is there a case for true anonymity
The goal is to identify a person with various levels of reliability	It is about rights management — Properties (over 18, allowed to access etc) are verified — not the person These rights are not linear — they cannot be put on a scale of low to high It is not limited to people — Programs, apps, robo-advisers, devices also need to have their access rights checked
Each company issues identity primarily for its own use Some point-to-point interoperability	Several providers offer rights verification — Not one provider with some interoperability — Need for any-to-any connection Four-corner model — A proven scalable model in payments and banking
Largely user ID/password technology Extra security through rigid two-factor authentication, with few complex exemptions (and exceptions to exemptions)	Technology using data and analytics — Only ask user if you really have to — 'Right' friction (two-factor authentication is the exception)
Regulator lays down in great technical detail the rules for authentication (description of factors, number to use, exceptions, thresholds, etc)	Principle based, technology-neutral, proportionate, evidence-based regulation — specify only the goal
Banks operate their own KYC silos at great cost	Banks find new strategic role as trusted party and generate more revenue than in payments[39]

Source: equensWorldline 2018

whole identities; attribute verification extends beyond people to include software and devices; the many providers of attribute verification should be connected with the many parties that want to rely on them; the connection is best done not with point-to-point silo interconnections but using the tried-and-tested four-corner model; pseudonyms should be used; rigid two-factor and user ID/password technologies should be replaced with intelligent modern risk-based methods that balance convenience and security; and everyone should be generally be more connected and smart about the topic.

How can one realise the above new approach? Collaboration is essential to make this happen. If we all believe that there is a better way than using government-based identity documents which reveal at once our age, ethnicity, name, blood group, travel history to every hotel clerk; if we believe there is a better way than deploying countless user IDs and passwords; if we believe there is an

opportunity for smart risk-based authentication which is both secure and convenient; if we believe that we must move away from countless silos with little or no interconnection; if we want a future-proof infrastructure that is scalable; if we want our online world to be safe and if we want to make life harder for those that try to impersonate and defraud us, then we must act — *together.*

This naturally leads to the following actionable recommendations for the concerned stakeholders:

- *Regulators* — lay out principle-based, technology-neutral, proportionate, evidence-based legislation. Trying to define rigid authentication rules and attempting to be the chief technical architect of the industry is not a role that a regulator can fulfil successfully. In general, the focus should be on letting the industry do its work. There are enough commercial incentives and legal motivations for the market to move as described. Legislation should only be considered to catalyse multi-side markets (where parties may otherwise be waiting on each other) or in the case of proven market failure.
- *Banks* — consider embracing the opportunities, also on the topic of identity and authentication. If banks do no more than simply comply with legislation, they will incur only costs and not realise any commercial or strategic benefits. Banks are increasingly becoming proactive digital players, partnering with advanced companies, generating new revenues, setting themselves up in a new position as a partner of trust and privacy. The alternative is to be intermediated and reduced to a commodity provider. The only way is forward.
- *Industry* — may see an advantage in setting up a federated 3SPP solution. Instead of every bank investing in silo solutions to solve largely the same problem as everyone else, consideration should be given to building a shared infrastructure for the benefit of all.
- *All of the above* — work together. Collaboration is essential. In this regard it is important to think of all stakeholders, especially the end users (who may also need some help and education — see below).
- *Users* — may need help to appreciate that security is also their responsibility, and help to understand what they need to do. Banks, governments, merchants are doing their utmost to keep users safe, but users must also invest some time and money and, for their own interests, must see this topic as of primary importance, as they themselves have said in various surveys.
- *Research* — keep coming up with new technologies that make people's lives easier and safer. The pace of change is astounding and should be kept up relentlessly as people are hungry for more.
- *FinTech* — find new commercial models that employ new technologies and partner with banks and industry to leverage these in the market. Modern technology for authentication now provides a win-win (easier to use *and* more secure), whereas past approaches were a trade-off. This yields better experiences for users, enhanced security and new commercial opportunities.
- *The European Central Bank (ECB)* — a catalyst may be needed to speed up the process. In principle, this could come from any actor in the market. However, as the financial services industry has such key assets here (trust, KYC, four-corner-model, high-volume international transaction business, growing API industry, FinTech partnerships, secure authentication etc) one could consider whether that catalyst might profitably come from this side of the market. A powerful innovation driver such as the ECB, with a mandated role as 'facilitator' and 'enabler' and to leverage and build on the 'smooth operation of the payments system' — here not in the role of oversight or regulator — could consider kick-starting an initiative. The ECB could, for example, consider bringing together key actors to

explore the potential of a new approach towards identity. This would surely benefit the whole European market and not just for financial services. Some may possibly see this as slightly beyond the core remit of the ECB by formal interpretations, however the trend towards value-added services (transaction data, identity, etc) around/based on payments, seems most welcome if not inexorable. In any case, it would surely be good to have the banking industry finally seen as a wider benefactor of society.

It is thus hoped that this text has provided some stimulation in the debate surrounding modern, flexible identity (which, as discussed, is not actually about identity…).

References and Notes

(1) Anderson, R. (2012) 'Risk and privacy implications of consumer payment innovation', paper presented at The Changing Policy Landscape Symposium, 29th–30th March, Kansas City, MO.

(2) 'Identity fraud reached the highest level since records began 13 years ago', '88% of identity frauds occurred online', 'one in every two crimes now a fraud or cybercrime — surpassing all traditional crime like burglary, robbery, etc'; see CIFAS (2017) 'Fraudscape 2017', available at: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2017 (accessed 10th January, 2018).

(3) 'In 2016 a record 421 billion data records were stolen — 3 million data records are lost or stolen every day', 'identity theft counts for 64% of all data breaches'; see Global Cyberalliance (2017) 'Identity Theft and Cybercrime Statistics', available at: https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html (accessed 10th January, 2018).

(4) OTP, as the name implies, typically uses a password as one of the factors. Although a 'one-time' password, this suffers the same deficits of any password-based system. Also, the choice of two factors seems largely arbitrary: when I buy a coffee at the same time and place every day, one or two factors seems more than sufficient, but when I buy a house, maybe seven steps/credentials/verifications are not enough. The whole approach with rigid 'factor' authentication appears worthy of reconsideration.

(5) 2F as originally laid out by ECB's SecuRe Pay — was published in January 2013 and based on the state-of-the-art of the early 2000s. Most recently, it has been largely adopted by EBA's PSD2 RTS and will likely apply from late 2019. Thus, in an environment where technology moves at breath-taking speed, solutions are being enforced approximately ten years later after they are state-of-the art.

(6) Of course, the mobile phone plays a key role here as it is pervasive, provides key fraud triggers (unusual behaviours, device changes), has secure environment (SIM card, sometimes TEE), has some key social attributes (users notice loss of phone much quicker than loss of card — and report it much quicker too) and unique attributes (remote disablement, location identification, biometrics) — see 'Strong Mobile Customer Authentication under PSD2: Comparisons and Considerations' white paper, to be released at Mobile World Congress Barcelona, March 2018.

(7) 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market', *Official Journal of the European Union*, 28th August, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:257:FULL&from=EN (accessed 10th January, 2018).

(8) The true identity can be found because of the chain of trust back to where the pseudonym was created (eg on mobile phone which was registered at purchase). Likewise, a car number plate is also a pseudonym: to the public it is just a string of letters and numbers — but for the police it is a means of reliably identifying the holder, if needs be, by tracing the plate code back via the car licence procedure to the identified registered owner.

(9) The true identity may be revealed to few selected key private sector services (opening of a bank account, obtaining a mobile contract, forming a company, buying a house) where law enforcement must be able to truly identify the individual when there is misuse. Again, true identity is only needed for law enforcement.

(10) Selling a car or a house, leaving a will, attaining right of attorney and other legal acts at a notary currently require personal identification. Whether this will always need to remain so is another question. It is conceivable that the right (ownership attribute) of the car could in the future be transferred via a digital token of ownership rather than the traditional means of government-issued documentation. This visionary view would of course require the deep revision of existing legal and government processes and is thus far too ambitious at this stage. Let us fix the lower-hanging fruit on online identity first.

(11) Tsakalakis, N., Stalla-Bourdillon, S. and O'Hara, K. (2016) 'What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation', paper presented at Open Identity Summit, Rome, 7th July.

(12) Whistleblowers that seek to expose government, law enforcement, etc will of course seek to remain fully anonymous as they will rightly not see the third parties they accuse as neutral.

(13) This marries *unforgeability* ('only authorised entities like banks are able to issue valid digital coins'), *untraceability* ('the relationship between a

digital coin and a user is untraceable') and even *unlinkability* ('different coins spent by the same user are unlinkable') and *unframeability* ('no user or shop can be falsely incriminated'). Chaum, D. (1982) 'Privacy protected payments. Unconditional payer and/or payee untraceability', offprint, CWI Amsterdam.

(14) Chaum, D. (1983) 'Blind signatures for untraceable payments', in: Chaum, D., Rivest, R.L. and Sherman, A.T. (eds) 'Advances in Cryptology', Springer, Boston, MA, pp. 199–203.

(15) Knapskog, S. (1988) 'Privacy protected payments — realisation of a protocol that guarantees payer anonymity', in 'Advances in Cryptography — Eurocrypt 88', Springer, Berlin, pp. 107–122.

(16) Europol (2016) 'The Internet Organised Crime Threat Assessment 2016', available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (accessed 2nd January, 2018).

(17) A case in point is the avalanche of anonymous comments found on the internet, which seldom add to the sum of human wellbeing and education. It is thus encouraging to see current political initiatives to curb 'fake news' and some of the online mis- and dis-information. Indeed, the topic of identity may help here to ensure that content providers are identified and must stand by their statements and their consequences.

(18) Opposition may occur as a result of some reputational damage banks have incurred due to customers not wanting their bank to know too much about them, hence banks may not always be the right players. Also, in developing countries or in states where the government wishes to retain full control, banks may not be the identity providers of choice.

(19) As cyber criminals tend not to publish their statistics, one can only employ a common-sense argument such as 'Suttons Law'. This is named after the bank robber Willie Sutton whose response to a reporter's enquiry why he kept robbing banks was simply 'because that's where the money is'. Common sense therefore dictates that in the online world too, most attacks will be targeted at where the money is — hence banks are the most heavily cyber-attacked industry.

(20) Compare even the worst the bank breaches (see next footnote) with other industries such as Sony's reputed loss of 100 terabytes of data or Yahoo's recent loss of 3 billion accounts. This latter breach was actually not revealed externally for four years — a situation unimaginable for regulated banks which are heavily and constantly monitored. According to CIFAS, 'Despite high volumes, identity frauds against bank accounts have reduced' — a trend that no other industry has seen. See: CIFAS (2017) 'Fraudscape 2017', available at: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2017 (accessed 10th January, 2018).

(21) Spectacular breaches, especially in the USA — Equifax (145.5 million accounts), JPMorgan Chase (83 million accounts), Heartland Payments Systems (134 million accounts), Global Payments, Inc. (1–1.5 million accounts), Citigroup (360,000 accounts), show that no industry is protected from cyber crime and data breaches.

(22) Note the lack of European breaches in the above list and the early introduction of security measures in this geography, such as Europol's statement (ref. 16, above) that 'EMV (chip and PIN), geoblocking and other European industry measures continue to erode card fraud within the EU, forcing criminals to migrate cash-out operations to other regions'.

(23) Salmony, M. (2014) 'Access to accounts: why banks should embrace an open future', *Journal of Payments Strategy & Systems*, Vol. 8, No. 2, pp. 157–171.

(24) Note that multiple attributes can be verified with one single call. Instead of multiple API calls, the relying party could provide a list of attributes that it wants verified and simply receive a yes/no answer back — for example, the attribute verifier confirms whether the data supplied by the user ('I am over 18 and live in London SW3 3BP and have two children') are correct, or not. This is more elegant and privacy sensitive than asking several times for each individual attribute.

(25) Euro Retail Payments Board (2017) 'Final Report of the ERPB Working Group on Payment Initiation Services', 15th November, available at: https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf?483e4d28242cd84322850a01e549d116 (accessed 10th January, 2018).

(26) Salmony, M. (2016) 'The future use of instant payments — from infrastructure to novel applications' in Mosen, M, Moormann, J. and Schmidt, D (eds) 'Digital Payments', Frankfurt School of Finance and Management, pp. 57–82.

(27) Huijser, M. (2010) 'The Cultural Advantage', 4th edn, Nicholas Brealey Publishing, Boston, MA.

(28) Trompenaars, F. and Hampden-Turner, C. (1993) 'Riding the Waves of Culture: Understanding Cultural Diversity in Business', Nicholas Brealey Publishing, Boston, MA.

(29) Hofstede, G. (1991) 'Cultures and Organizations: Software of the Mind', McGraw-Hill Education, New York, NY.

(30) For example, PayPal, Swish (SE) and iDeal (NL) each enforce redirection away from the merchant to the authentication service and are among the most successful online payment services in the world. They are perceived to give the users control and confidence, prevent fraud and have massively improved adoption of e-commerce. Others, by contrast — including the European Commission's revised PSD2 RTS Art.32 §3 — consider redirection an obstacle to the provision of online services.

(31) Botsman, R. (2017) 'Big data meets Big Brother as China moves to rate its citizens', available at: http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion (accessed 10th January, 2018).

(32) A global approach which the world surely needs. An effective digital identity would ideally need to match the increasingly global nature of commerce (as with the card schemes and over-the-top players like Amazon, Google, Facebook, etc) and increasingly global life.

(33) Except, for example, in Illinois with its restrictive 'Biometric Information Privacy Act', 740 ILCS 14/1 et seq. ('BIPA'). Also in the USA there are variants in legislation and attitudes change as privacy is seen to be violated.

(34) Contrast this, for example, with attitudes in Germany where the population traditionally values privacy highly and is usually quick to ask for the government to take control in case something is perceived to be going awry.

(35) Via signed e-mails/PDFs, scripted online web cancellations, automated faxes or old-school paper letters.

(36) We do see in this example that value chains are becoming ever more complex with multiple becoming involved in a single transaction. This indicates that it may be necessary to have an approach that works across multiple players (in this example Android, Apple, Amazon and many more small solution providers). This is an interoperability challenge but has many advantages, not least minimising the privacy-relevant data available to each player. The future can surely not be digital giants that know everything — it must be federated.

(37) The user herself may wish to set preferences with respect to how many steps are required to gain access to account balances on Alexa, in this example. In particular, control and security conscious users might wish to demand additional steps beyond a minimum threshold set by the service provider. Such users typically also wish to instruct transport apps to show the bill for the journey after a quick TouchID verification as the journey ends *before* the payment is made — rather than having the fully automated/transparent/no-friction process that others value so highly. Conclusion: user choices and preferences must be respected with sensible minimum defaults set.

(38) This is not always the case with current regulation, for example in PSD2 SCA RTS. The one-click checkout that merchants and customers love (but which in future is only permitted under contract) will likely only be available to the big players. Amazon cannot afford to talk to all the many small banks and ING cannot afford to talk to all the many small merchants across Europe. However, the two big players (ING, Amazon) will likely do a direct deal/contract to have the great one-click experience for *their* customers, rightly leveraging each others' huge user base. Thus, one-click will likely *not* be viable for the small players (merchants, FinTechs, banks) but will be the privilege of the large players. This is not the bank's or Amazon's fault — it is a natural (unintended) consequence of the regulation. Also, only big players can afford to employ the very sophisticated (needing, for example, IBM Watson) analytics to achieve the rigidly defined and highly demanding regulated fraud targets. Thus, rigid regulations such as this — although nobly aiming to improve competition (small players vs quasi-monopolists) — may end up actually achieving the opposite. The literature has proved many times that 'less is more' in regulation. See, for example, Haldane, A. (2012) 'The Dog and the Frisbee', in 'Proceedings of the Economic Policy Symposium, Jackson Hole, WY, 30th August – 1st September', pp. 109–159.

(39) Which is already a good business now with huge volumes, good revenue, stable growth regularly above GDP, see for example:

- 'In 2016, the global payments industry accounted for 34 percent of overall banking revenues — up from 27 percent just five years earlier' ... 'a $2 trillion-dollar industry by 2020' (McKinsey (2017) 'Global Payments Report 2017', available at: https://www.mckinsey.com/industries/ financial-services/our-insights/global-payments- 2017-amid-rapid-change-an-upward-trajector (accessed 10th January, 2018));

- 'Global non-cash transaction volumes grew 11.2% during 2014-2015 to reach 433.1bn, the highest growth of the past decade, and above predictions' (see CapGemini (2017) 'World Payments Report 2017', available at: https://www.worldpaymentsreport.com/ (accessed 10th January, 2018));

- 'The value of global payments transactions stood at $420 trillion, or 5.5 times global GDP' (Boston Consulting Group (2017) 'Global Payments 2017', available at: http://image-src. bcg.com/Images/BCG-Global-Payments-2017- Oct-2017_tcm9-173047.pdf (accessed 10th January, 2018)).