Financial Services in the Digital Age

How Strengthened Digital Identity Will Open Markets, Drive Innovation and Deliver Growth

By Sergey Filippov

Dr Sergey Filippov is associate director of the Lisbon Council. Previously, he served as assistant professor of innovation management at Delft University of Technology in the Netherlands.

The author would particularly like to thank Andrus Ansip, vice-president of the European Commission for the digital single market, who spoke at the *High-Level Conference on a New Leap in the eIDAS Journey: New Trust Services for a Digital Single Market*, where this digital insight was launched. Special thanks as well to Andrea Servida and the hard-working group at the task force legislation team (eIDAS) for a generous critique of the ideas and recommendations. As always, any remaining errors of fact or judgment are the author's sole responsibility. The opinions expressed are those of the author alone, and do not necessarily reflect the views of the European Digital Forum or any of its associates.

The European Commission – led by President Jean-Claude Juncker – has prioritised completion of the digital single market – and it's not hard to see why.[1] Some estimates suggest that linking European consumers in a single, online marketplace – where shoppers in Slovenia could browse online stores in Estonia, and a trip to the bank would be as easy as a few clicks of a mouse – could raise the gross domestic product of the European Union by 4% – adding more than €500 billion of additional commerce per annum to a continent urgently looking for an economic boost and desperately seeking new jobs.[2] The European Parliament has estimated non-completion of the digital single market could cost EU countries as much as €75 billion per annum in lost revenue and unnecessary transaction costs.[3]

Increasingly, visions of linking the continent together online are stumbling on a recurring problem: the lack of reliable, interoperable identification and online authentication procedures, or e-Identity, as it is sometimes called. To be sure, many European companies and services – such as Air France-KLM, BlaBlaCar and Spotify – have worked around the problem by allowing log-in with popular

1 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *"A Digital Single Market Strategy for Europe,"* Brussels, 06 May 2015, COM(2015) 192 final http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192

2 Marco Hafner, "Why the EU Single Market Is Still an Incomplete Jigsaw," *The RAND Blog*, 16 February 2016. http://www.rand.org/blog/2016/02/why-the-eu-single-market-is-still-an-incomplete-jigsaw.html

3 European Parliamentary Research Service, *The Cost of Non-Europe in the Single Market III – Digital Single Market* (Brussels: European Parliament, 2014). http://www.europarl.europa.eu/RegData/etudes/STUD/2014/536356/EPRS_STU(2014)536356_REV1_EN.pdf

social networking services like Facebook, LinkedIn and Twitter.[4] But this system has advantages and disadvantages. The advantage is that – without much fanfare – Facebook, LinkedIn and Twitter have rolled out popular, pan-European platforms whose basic usage is not in any way limited to or defined by national borders; these are pan-European platforms in the truest sense of the word, and that has clear advantages for the future of the European digital single market. But the disadvantage is that Facebook, LinkedIn and Twitter are hardly robust "identification" systems; customers like the services, but as presently constituted they hardly set an identity standard strong enough to sustain, say, cross-border banking or electronic commerce.

'Visions of linking the continent together online are stumbling on a recurring problem: the lack of reliable, interoperable identification and online authentication procedures.'

In the meantime, the European Union is taking decisive action. The all-important "trust services chapter" in the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, or eIDAS, came into force on 01 July 2016.[5] Among other things, it requires that e-signatures recognised in one EU member state be accepted in other EU member states as a valid signature – once the e-signature has been approved at the member-state level and listed in a national "trusted list of certification service providers." This is a colossal step forward. These days, most European countries have autonomous national electronic identification (eIDs) schemes, which diverge widely in scope and format. These systems have been helpful for solving national online authentication problems, but have left the EU fragmented along national borders.[6] Prior to 01 July 2016, only some countries recognised digital signatures signed by citizens or businesses in other EU countries on official documents, which forced much of the potential cross-border economy to remain offline in the analogue world of paper, ink and snail-mail. This created huge bottlenecks, led to unnecessary duplication on many transactions and complicated important procedures, forcing them to be duplicated as many as 28 times. But even more damagingly, it slowed down deployment of the European economy's most important asset: the emergence of a coherent, single market of 508 million consumers, united by a single set of rules in a truly European digital single market. And it discouraged citizens and businesses from taking full advantage of the most-productivity boosting tool the world has ever seen: the Internet and online transactions.[7]

Put simply, helping people and businesses to transact business online will give an important boost to the European economy. But doing this will require trust – and vision. In this game, the technical has become political, and more and more policymakers are realising that European citizens and businesses are urgently awaiting faster, more decisive action in this area. Governments must use

4 This is known as OAuth/ SAML – an open authorisation standard commonly used at international level, allowing Internet users to log into third-party websites using their online profiles without exposing their password.

5 Technically, the eIDAS regulation came into force on 17 September 2014. The all-important "trust services chapter" become operational on 01 July 2016. Since 29 September 2015, EU member states with an eID system can "notify" other EU member states of the existence and parameters of that eID, and recognise eIDs from other member states on a voluntary basis. From 29 September 2018, EU member states will be required to issue and recognise full e-ID systems and to recognize the eIDs of citizens from other EU member states. and accept the eIDs of other member states that have notified them.

6 Any customer authentication by commercial organisations is underpinned by a national identification system that all EU member states have in one form or another. National identity cards are issued to their citizens by the governments of all EU member states except Denmark and the United Kingdom. At present, there is a huge diversity in terms of their appearance and design, their validity as a travel document, requirement to be in possession of an ID card and other technical divergences. According to the European Commission, as of 2015, 14 member states had functioning eID schemes, seven were planning to introduce eIDs, and seven did not have any plans.

7 Paul Hofheinz and Michael Mandel, *Uncovering the Hidden Value of Digital Trade: Towards a 21st Century Agenda of Transatlantic Prosperity* (Brussels and Washington, DC: The Lisbon Council and Progressive Policy Institute, 2015). http://www.lisboncouncil.net//index.php?option=com_downloads&id=1184

Seven recommendations

1. Make the European eID system fully interoperable ahead of the 2018 deadline.
2. Make cross-border eID recognition tools and solutions under the eIDAS available to the financial sector on a voluntary basis.
3. Strengthen the regulatory alignment between the eIDAS regulation and financial sector-specific rules.
4. Explore greater cross-border and cross-sector use of private sector-based solutions in advanced e-Identification, including broader use of the high-standard banking sector-developed identification procedures.
5. Share and promote best practices: successful measures for distance verification in the financial sector that are legal in some EU member states should be accepted in other EU member states.
6. Implement a voluntary single contract for cross-border retail financial services to facilitate building of a common market in retail financial services.
7. Avoid diverging implementation of the fourth Anti-Money Laundering Directive. Apply anti-money laundering, counter-terrorism financing and "know-your-customer" criteria consistently across the EU.

their power to ensure widescale rollout of easy-to-use and fully interoperable pan-European e-Identity standards – using a tried and tested technique of weaving together a European quilt through mandatory interoperability rather than allowing individual member states to foment and enforce uninteroperable, effectively protectionist national standards. This effort could take on two aspects. First and foremost, it should be built on competition: effective online certification procedures should compete to ensure better, easier use for customers and safer, less-costly-to-install customer verification procedures for service providers. But it should also aim at insuring that good, reliable procedures are available to a broader range of potential customers, making successful e-Identification a relatively easy, cheap to install solution for shops and services wishing to sell their goods online. Done well, this can have a tremendous catalysing effect. It could serve as a boost to the online market much as the Global System for Mobile Communications (GSM) standards did for telecommunications two decades earlier.[8]

> 'Lack of online verification procedures slows down deployment of the European economy's most important asset: a coherent, single market of 508 million consumers.'

8 Jacques Pelkmans, "The GSM Standard: Explaining a Success Story," *Journal of European Public Policy*, 8(3): 432-453, 2001. http://www.tandfonline.com/doi/abs/10.1080/13501760110056059. Stephen Temple, "Chapter 23 – Could Europe Create Another GSM Success?," in *Inside the Mobile Revolution: A Political History of GSM* (stephentemple.co.uk, 2010). http://www.gsmhistory.com/chapter/chapter-24-could-europe-create-another-gsm-success

Fortunately, there are some bricks upon which an important and powerful European solution could be built. The banking sector itself is well on the way towards establishing secure, reliable online verification procedures, and it is a core argument of this paper that those online verification procedures – and others that will be developed in coming years – could themselves form a stronger backbone for greater cross-border online commerce.

The eIDAS regulation could easily form the nucleus of a larger, more broadly needed reform to give Europe better standards for online interoperability throughout the economy. We believe that

Banking industry identity solutions

NemID is a common login solution for Danish Internet banks, government websites and some other private companies. NemID is managed by the Nets DanID A/S company and came into use on 01 July 2010. Everyone in Denmark who is over 15 years old and has a CPR-Number (the Danish personal identification number) is eligible for a NemID that can be used with their bank as well as public institutions. Anyone over 13 years old may use a NemID for Internet banking. Users of NemID are assigned a unique ID number that can be used as a username in addition to their CPR-Number or a user-defined username. For more, visit https://www.nemid.nu/dk-en/about_nemid.

BankID is a personal electronic ID used in Norway. The solution is developed through BankID Partnership, which is a collaboration between the Norwegian Financial Services Association and the Savings Banks Association. BankID is a public key infrastructure (PKI) solution, and supports both authentication and signing. The solution consists of a central infrastructure and multiple client versions in different forms. In addition, BankID for mobile phones now offered by all mobile operators in Norway. Over 2.9 million Norwegians use BankID, mainly for access to network services from Norwegian banks, but also for public services. BankID, along with MinID, is the most widespread electronic identity solution in Norway. For more, visit https://www.bankid.no/en/about-us/.

TUPAS is a digital authentication method created by the Federation of Finnish Financial Services, a de facto standard for digital identification in Finland. It is used by all major Finnish banks, as well as by the Finnish government to log into the Social Insurance Institution of Finland and the Finnish Tax Administration. Commonly the identification is done using a password and a list of single-use passcodes or a passcode device. For more, visit https://en.wikipedia.org/wiki/TUPAS.

Based in Trondheim, Norway, and founded in 2007, **Signicat** is the first and largest identity assurance provider in the world, providing regulated markets with the technology to create mutual trust between organisations and their potential customers. With Signicat, service providers can build and leverage existing customer credentials to connect users, devices and even "things" across channels, services and markets transforming identity into an asset rather than an obstacle. Service providers can rapidly grow market share, easily acquire new customers, and ensure compliance with financial, privacy and data protection regulations including anti-money-laundering and know-your-customer checks. For more, visit https://www.signicat.com.

the tools and methods proposed in the eIDAS regulation provide a strong, technical basis for a further, deeper restructuring – one where the eIDAS method becomes a coherent and broadly adopted mechanism for conducting online transactions throughout Europe, setting an important (but voluntary) standard for digital identity, available at low cost to all participants, and competing on quality and ease-of-use with other, private-sector-led initiatives in this fast-growing area. We call on European governments and financial institutions to band together and urgently deliver a powerful, single-market friendly solution to this problem, and particularly for digital and online banking. Europe's economy needs it. And citizens are demanding no less.

MyBank is an e-authorisation solution which enables safe digital payments and identity authentication through a consumer's own online banking portal or mobile application. MyBank creates a direct link between a customer's online bank account and the online business's bank, which eliminates the need to collect and store personal data. Customer identity and confidential data are protected. Immediate authorisation of payments reduces risk of fraud and charge-backs. MyBank offers identity verification services allowing consumers and businesses to confirm their identity through their online account in order to complete online purchases or subscribe to digital services, in a safe and trusted manner. For more, visit https://www.mybank.eu.

GOV.UK Verify is a new way of proving identity online, making it possible for services to allow people to do more complex, risky transactions entirely online. The programme is growing a diverse and competitive market by taking a standards-based, federated approach. Rather than having a single provider, GOV.UK Verify allows users to choose from a list of certified companies that all work with the same published standards and principles. All certified companies go through a rigorous onboarding process to make sure that their solutions are secure, meet the standards and are well designed. At the moment, there are eight GOV.UK Verify certified companies. They are Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail, SecureIdentity and Verizon. For more, visit https://identityassurance.blog.gov.uk.

iDIN in the Netherlands

On 08 March 2016, Betaalvereniging Nederland, an association of the largest Dutch banks and payment providers, launched a pilot stage of iDIN. iDIN allows customers of one participating financial institution to identify themselves with another participant in the pilot, using the safe and secure authentication of their own bank. Moreover, the Dutch Tax Authority participates in the pilot too. iDIN operates in parallel to other customer authentication methods such as DigID for the Dutch public services. Persons may choose their authentication method themselves – either iDIN, or DigID or alternative. The intention is to extend this pilot to e-commerce stores and insurance companies. As such, iDIN is supposed to become a universal digital identity for Dutch citizens and residents – to access public, financial and other commercial services and products online. For more, visit http://www.betaalvereniging.nl/nieuws/pilot-idin.

Making eIDAS work in the financial and commercial sectors will require collaboration between European and national authorities. We recommend the following seven-step programme:

1. EU member states should move more decisively to make the European eID system fully interoperable ahead of the 2018 deadline for full implementation. The ultimate objective is the smooth, almost unnoticeable presence of a high-level, secure e-identification system available to all customers with the click of the mouse and boasting an online standard whose security assurance level is clearly mappable against a set of objective, outcome-oriented criteria.

2. The cross-border eID recognition tools and solutions under the eIDAS regulation – designed and obligatory for the public sector – should be expanded and offered to the private sector on a voluntary basis, and specifically for use in online financial services, where a high standard for correct digital authentication is *de rigueur*.[9] Financial institutions are encouraged to voluntarily accept this new tool as a way of seamlessly knitting the sector more closely together across borders. Engagement between the financial sector and national electronic identification schemes should be developed in the eID area, though the system should remain voluntary, with rival systems competing to offer higher levels of security and better ease of use.

3. Regulatory alignment between the eIDAS regulation and the financial sector-specific rules – in particular, the fourth Anti-Money Laundering Directive (4AMLD) and the Revised Payment Services Directive (PSD2) – should be strengthened. At the European level, co-legislators should explicitly recognise the use of electronic signatures and eIDs in the text of the amended 4AMLD. The European Commission should specifically address the risks involved in cross-border customer identification and electronic authentication in the report on the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (to be drawn up by June 2017), taking into account that electronic identification (as embodied in the eIDAS regulation) is in many ways more secure than most paper-based identification procedures. At the national level, EU member states transposing 4AMLD and PSD2 into their national legislation should consider their overall fitness with the eIDAS regulation. The European Commission should support the ongoing transposition, making the consistent transposition of the directives its top priority.

> ‘Helping people to transact business online would give an important boost to the European economy.’

9 Recital 17 of the eIDAS regulation states clearly “member states should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many member states at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any member state should be available to private sector relying parties established outside of the territory of that member state under the same conditions as applied to private sector relying parties established within that member state. Consequently, with regard to private sector relying parties, the notifying member state may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.”

4. National authorities should consider and explore federated solutions and embrace a "make once, use many times" approach, with active private-sector input and engagement. Strong, verifiable digital identification solutions used by banks could be used to access other online services, including digital public services, and vice versa. In this scenario, banks – which already boast some of the highest identity authentication procedures in the world – could act as identity assurance services providers themselves, taking on an important function in online transactions. This will have a mutually reinforcing effect on both financial services and eGovernment. The systems themselves can remain autonomous, but the authentication standards applied should be fully mappable against an explicit and outcome-based framework, setting out clearly stated levels of assurance.

'The technical has become political.'

5. Successful measures for distance verification in the financial sector that are legal in some EU member states should be accepted in other EU member states. New technological solutions for identification of new customers, such as video calls permitted by regulators in one EU member state, should be accepted and legal in others. Sharing of best practices should be promoted across borders. Innovative pilot activities on cross-border digital identification in the financial sector relying on the use of eID should be promoted and closely studied.

6. An interoperable, cross-border electronic identification and authentication system is a first and very emblematic step towards building a common market in retail financial services. A more fundamental issue is contract law. Despite some measure of legal harmonisation across the EU, there are still legal differences across the EU member states that need to be bridged in order to promote cross-border retail financial services and facilitate the uptake of cross-border transactions. One of the possible solutions is a voluntary single contract for cross-border retail financial services.

7. Avoid diverging implementation of 4AMLD. The anti-money laundering, counter-terrorism financing and so-called "know-your-customer" criteria need to be applied consistently by national regulators and supervisors, preventing a fragmented regulatory landscape in Europe.

'European citizens and businesses are awaiting faster, more decisive action.'

This Digital Insight is divided into three parts. Part I sketches a brief overview of the current solutions and approaches used for customer identification and authentication in the financial sector, the most advanced part of the economy when it comes to effective, verifiable e-Identity. Part II looks at the current regulatory framework that governs electronic identity, customer authentication and e-signatures in financial services online sales and operations, specifically focusing on the eIDAS regulation and its alignment with sector-specific legislation. Part III concludes with a set of proposed policy solutions. Our aim is to contribute to the formulation of better solutions – including effective regimes that will open markets and allow ambitious providers to deliver more and better financial services to a broader range of customers, and create an overriding vision for an effective cross-border e-identification and e-signature system.

I. Customer identification and authentication in the financial sector

The potential for cross-border retail financial services in a common European market is huge. One in three Europeans live in regions bordering other member states; and 13.6 million EU citizens live in another EU member state. And yet, fewer than 3% of European consumers purchase banking products such as credit cards, current accounts and mortgages from another member state. When it comes to consumer credit, Europeans buy only 5% of their loans from abroad.[10] The reasons are numerous – ranging from cultural and linguistic ones, to regulatory ones. But one rather technical – but also deeply political – cause is the lack of a universal online digital service that would give a high enough level of identity assurance.[11]

For the purpose of this paper, we will look at digital identity primarily in the financial sector, where existing technology is most advanced and the need for secure identification most acute. Specifically, we will examine current practice in this key sector from two sides: 1) initial identification when a new client wants to open a bank account, known as "onboarding" in the financial jargon, and 2) continuous electronic authentication, with a qualified electronic signature or similar mechanisms, which customers use to gain access to financial services online.

Presently, the first stage, onboarding, often requires the physical presence of a prospective customer wishing to open a bank account. This process also includes residential requirements – the customer needs to provide and confirm his or her permanent home address. Such rigid interpretation of the rules known as "know your customer" is extremely burdensome for many in the digital age. People often need to visit a bank branch, identify themselves face-to-face, present reference documents, have their identity card photocopied and put a handwritten signature on a contract. Many people living in remote and rural areas find it difficult to visit the nearest bank branch and are de facto deprived of access to formal financial services. And when an individual would like to open a bank account in a bank based in the country other than the country of his residence, and even physically present themselves at a bank branch, he or she may be turned away due to residency requirements.

> 'Governments should weave together a European quilt through mandatory interoperability rather than dictating a single European or national standard.'

10 European Commission, *Key Facts on Consumer Finance*. http://ec.europa.eu/finance/finservices-retail/docs/policy/151210-factsheet_en.pdf

11 European Commission, *Green Paper on Retail Financial Services: Better Products, More Choice, and Greater Opportunities for Consumers and Businesses*, COM/2015/0630 final. http://eurlex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:630:FIN

These cumbersome, analogue-age procedures have direct financial implications, too. According to some estimates, in the UK alone, the total costs of identity assurance processes currently exceed £3.3 billion [€4.2 billion at the 2016 exchange rate], made up of £1.65 billion [€2.1 billion] inside organisations and another £1.65 billion [€2.1 billion] of consumers' time costs.[12] The process differs across the continent in terms of what documents are requested. For instance, can a driver's licence be accepted as a proof of identity, or as valid address proof? There are certain exceptional cases, too. In the UK, the national ID card ceased to be a valid legal document for confirming identity on 21 January 2010, and the national identity register has been destroyed. Potential clients need to submit alternative identification documents.

'Online certification procedures should compete to ensure better, easier use for customers and safer, less-costly-to-install customer verification procedures for service providers.'

STORK 2.0

Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0) was a three-year long EU-funded project that ended in September 2015. The STORK 2.0 consortium consisted of 55 organisations from 19 EU member states and associated countries (Austria, Belgium, Czech Republic, Estonia, France, Greece, Iceland, Italy, Lithuania, Luxembourg, Netherlands, Portugal, Slovenia, Slovakia, Spain, Sweden, Switzerland, Turkey and the United Kingdom). Together, they drove the project and built a common, comprehensive and long-term vision of eID in Europe. STORK 2.0 built upon its predecessor, STORK, an EU-led project to establish interoperability of different approaches at national and EU level, eID for persons, eID for legal entities. STORK 2.0 was a step forward towards the creation of a fully operational framework and infrastructure for electronic identities and authentication in the EU. STORK 2.0 pilots – ranging from eLearning and academic qualifications, to public services and eBanking – demonstrated interoperable services that eID can offer in real-life settings. These pilots are underpinned by common specifications, standards and building blocks, operating across borders in different sectors. Importantly, STORK 2.0 methodology seeks to maximise take-up of its scalable solutions by both public and private sectors with a strong commitment to open specifications and long-term sustainability. Within three-and-a-half years, STORK 2.0 has accomplished major achievements, such as a set of common specifications for cross-border interoperability eID platforms, commercial packages with manuals, guidelines and common code and a new attribute quality authentication assurance framework. STORK2.0 serves as the basis for eIDAS technical specifications. CEF (Connecting Europe Facility) eID and the EU co-funded Large Scale Project e-SENS (Electronic Simple European Networked Services) work together to address the integration of the functionalities of STORK 2.0 in the eIDAS technical specifications. Learn more about STORK2.0: https://www.eid-stork2.eu/.

12 Alan Mitchell and Jamie Smith, *Economics of Identity: The Size and Potential of the UK Market for Identity Assurance* (London: The Open Identity Exchange / Ctrl-Shift, 2015). https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/

Digital identification to combat fraud

In the ever connected and digitised world, criminals use technology to exploit vulnerabilities, both in the physical and digital worlds. Bank accounts have been opened and people's lives have been ruined by people taking on their identity and committing crimes. The weakest link in the criminal chain is often identity documents, such as passports. Interpol's Stolen and Lost Travel Documents database presently contains 54 million records from 170 countries; and many of these documents are being fraudulently used by terrorists, drug smugglers and human traffickers to travel the globe. Back in 2010, this situation led then Interpol Secretary-General Ronald Noble to characterise passport fraud as the "biggest threat facing the world." According to credit reference agency Experian, in the UK, at least 89 in every 10,000 applications for a current account in 2015 were made by an imposter compared to 77 in every 10,000 applications in 2014. And almost half of all fraud was attempted by people who had stolen an identity, compared to less than a third in 2014. Technology makes it possible to forge documents. And it is this very same technology that allows it to combat fraud, starting from incremental improvements in the integrity of existing documents to radically new forms of identification, such as biometrics – that cannot be lost or stolen. To be sure, electronic identification and authentication bring their own risks and challenges that need to be carefully managed. However, with proper cybersecurity measures and policies in place, the risk of eID fraud is much smaller than that of forging paper-based documents. For more information, visit https://www.theguardian.com/money/2015/jul/02/current-accounts-overtake-mortgages-as-of-choice

As for the ongoing electronic authentication, most banks have introduced one system or another, depending on the needs and responsibilities of correct identity assurance, with combinations of different factors providing different functionalities. They employ a wide variety of technology-based solutions, in compliance with the existing legislation, offering safe, secure and convenient authentication to bank clients. Most commonly, these systems are based on the multi-factor authentication principle – a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism. Typically, it should combine at least two of the following categories: knowledge (something they know, e.g. password), possession (something they have, e.g. a bank card or token), and inheritance (something they are, i.e. biometric identification). The use of at least two categories is put forth in the guidelines on securing online payments across the EU, released by the European Banking Authority in December 2014.

'The banking sector itself is well on the way towards establishing secure, reliable online verification procedures.'

Many banks have issued hand-held smartcard readers to their customers to support different electronic payment applications using a chip authentication programme. Others use security tokens, such as physical contactless tokens and mobile device tokens. Rather than distributing physical authentication gadgets to their clients, other banks widely use the mobile communications channel to support a customer

authentication procedure. They offer either dedicated mobile applications, or text-message-based solutions to deliver a one-time password to a registered customer's mobile device. The above solutions satisfy two requirements – knowledge and possession.

These systems are typically bank-specific, i.e. can be used only to use the services offered by the issuing bank. Some banks incorporate national identification systems, developed by public authorities, to their systems. In this case, customers are able to electronically identify themselves, access their bank account and perform financial operations using their national (electronic) ID cards. In this case, the state de facto provides a guarantee that the person identifying herself or himself with an electronic ID card is the right person. Additionally, the digital certificate on the smart eID serves for the encryption of the transferred data, authenticating its origin and therefore it can serve for e-signatures with contractual validity.

'The electrical signals emitted by a person's heart, known as electrocardiogram, are unique and a vital signal of the body and cannot be faked.'

Regarding the third category – "inheritance" (electronic fingerprinting, and iris, voice and face recognition) – it is increasingly used in the public sector by governments. The growing availability of biometric-based authentication on consumer mobile devices provides an opportunity for mobile application developers to use them as part of a multi-factor authentication process, too. Here, however, a delicate balance needs to be struck between convenience and privacy. For instance, fingerprints used for customer authentication – on their mobile devices – must be stored and processed in strict accordance with data protection rules. The benefits for consumers are sizeable. In the long term, technologies like iris recognition would greatly reduce the risks of fraud through identity theft, if implemented correctly.

An even more futuristic solution is the use of electronic wristbands to measure customers' heartbeats to authenticate and verify their identifies. The electrical signals emitted by a person's heart, known as an electrocardiogram, are unique and a vital signal of the body, and cannot be faked. As such this technology is superior even to fingerprints or iris scans.[13]

Digital identity is a constant daily need in the financial sector. Banks have gained rich experience in day-to-day electronic authentication. In contrast, the use of digital solutions for onboarding remains limited due to a number of reasons, most prominently, regulation. The tools and solutions under eIDAS make it potentially possible for banks to digitise onboarding too, and offer a fully end-to-end digital experience to their users.

13 Julia Kollewe, "Halifax Trials Heartbeat ID Technology for Online Banking," *The Guardian*, 13 March 2015. https://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking

II. Ensuring alignment between eIDAS and financial sector-specific legislation

Adopted in 2014, the all-important trust services chapter of the eIDAS regulation came into force on 01 July 2016 in all EU member states. It aims to deliver a predictable pan-European regulatory environment related to electronic identification and trust services; specifically, giving qualified electronic signatures the same legal effect as handwritten signatures everywhere in the EU. As is, as of 29 September 2015, EU member states can already notify and recognise "notified" eIDs from other EU member states. As of 29 September 2018, this mutual recognition will be mandatory. People and businesses will be able to use their national eIDs to access public services in other EU countries where eIDs are available. Ultimately, the regulation intends to create a common European space for electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.[14]

'State-supported standards for digital identity should compete on quality and ease-of-use with other private-sector-led initatives in this fast-growing area.'

Importantly, eIDAS does not intend to create "an EU eID," but rather to make existing eIDs interoperable. The EU member states that do not yet have fully functioning eID systems can leapfrog and design them in full conformity with the eID technical specifications under eIDAS. The regulation has a wide scope, covering the entire trust chain including sealing, validation, time stamping and central signing.

Although the primary focus of the eIDAS regulation is public services (regarding cross-border eID recognition), the European Commission sees wider benefits from it. For instance, the EU eGovernment Action Plan 2016-2020 mentions banking, finance, e-commerce and sharing economy as sectors where the potential of eID would be huge.[15] The eIDAS regulation should allow firms to more easily identify customers at a distance, strongly authenticate parties to payment transactions, allow safe and secure signing of contracts and enable e-signatures. The successful take-up of the eIDAS regulation may help remove a major barrier to the cross-border provision of retail financial services.[16]

The eIDAS regulation has the potential to transform the entire operations of many banks. This, however, will be possible if the sector-specific regulations are observed. By their nature, financial institutions are subject to very stringent regulation. The know-your-customer requirements of the existing anti-money-laundering and counter-terrorism-funding legislation are aimed at preventing identity theft, financial fraud, money laundering and terrorist financing. The know-your-customer rule requires due diligence information to verify the clients' probity and integrity, including fiscal and residential requirements. Effectively, it limits banks' ability to open and maintain business

14 European Commission, *Trust Services and eID*. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

15 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU eGovernment Action Plan 2016-2020: Accelerating the Digital Transformation of Government,* Brussels, 19.04.2016, COM(2016) 179 final https://ec.europa.eu/digital-single-market/news-redirect/30497

16 European Commission, *Green Paper on Retail Financial Services: Better Products, More Choice, and Greater Opportunities for Consumers and Businesses*, COM/2015/0630 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:630:FIN

e-Identity for financial inclusion

Access to a payment account has become a pre-condition for participating fully in economic and social life. Globally, more than two billion people are financially excluded. In the European Union, around 58 million consumers over the age of 15 still do not have a bank account, according to some estimates. The number of consumers without a payment account varies from 55% to less than 1% of the national population. The highest levels are reached in Romania (55%) and Bulgaria (47%), and the lowest in the Scandinavian countries (less than 1%). Adopted in July 2014, the Payment Accounts Directive (PAD) aims to help the EU internal market for payment accounts work well by ensuring that every EU resident has access to a basic bank account and by helping people switch payment accounts. In order to reduce financial and social exclusion, all consumers legally residing in the EU should have access to basic banking services, whatever their financial situation. With the rise in migration, PAD is also applicable to the refugees entering the EU – many of whom do not have any identity documents. Banks are facing a dilemma – balancing the need to comply with the provisions of PAD and the know-your-customer requirements. Cross-border digital identity solutions should help ease the access to financial services and improve financial inclusion. For more, visit http://ec.europa.eu/dgs/health_food-safety/pressroom/docs/bank-accounts-factsheet-03_en.pdf and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0092

relationships with customers at a distance.[17] In its strict interpretation, banks request physical attendance at their premises, where potential new clients would also present documentary evidence of residence and any other supporting documents.

The fourth Anti-Money Laundering Directive (4AMLD) was enacted on 25 June 2015. EU member states have up to two years to transpose it into national legislation, with 26 June 2017 as the ultimate deadline. Despite this formal deadline, the European Commission has called on member states to bring forward the implementation by six months to end of 2016.[18] The directive provides for a risk-based approach that allows for more flexibility in order to take into account national specificities and the circumstances of individual business relationships or transactions.[19] Article 15 allows "simplified customer due diligence" to "areas of lower risk." At the same time, Annex III listing factors and types of evidence of potentially higher risk includes "non-face-to-face business relationships or transactions," yet makes an exception for "certain safeguards, such as electronic signatures." Thus, digital identification using present-day IDs via video is deemed high risk.

> 'The cross-border eID recognition tools and solutions in the eIDAS regulation should be offered to the private sector on a voluntary basis.'

17 Ibid. This is an obstacle that has also been confirmed in the European Commission study on the Directive 2002/65/EC concerning the distance marketing of consumer financial services on the conclusion of cross-border contracts for financial services between suppliers and consumers within the Internal Market back in 2008.

18 European Commission, "Commission Presents Action Plan to Strengthen the Fight Against Terrorist Financing," *Press Release*, 02 February 2016, Strasbourg. http://europa.eu/rapid/press-release_IP-16-202_en.htm

19 Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

In the wake of the November 2015 Paris attacks, the European Commission adopted an Action Plan to strengthen the fight against terrorist financing.[20] According to the Plan, the European Commission is to propose a number of targeted amendments to 4AMLD, including proposals with respect to virtual currency exchange platforms and prepaid instruments. The Action Plans set "at the latest by the second quarter of 2016" as the deadline, and the amendments are expected to be unveiled on 05 July 2016. Following the imperative of the Action Plan, the European Commission proposes a harsher approach to anti-money laundering to combat terrorist financing. At the same time, the revision of 4AMLD provides an opportunity to recognise the use of eID solutions in the text of the amendment. Specifically, one may expect a reference to eIDAS as a framework for e-identification to be included in the text of the modified directive. It is important to note that this modification of 4AMLD comes at the time while EU member states are still transposing the original directive into national legislations.[21]

'Banks, which already boast some of the highest identity authentication procedures in the world, could act as identity assurance providers themselves.'

As 4AMLD (as well as its predecessor) is a directive, it could potentially lead to different national laws and interpretations in each EU member state, and hence, approved identity verification schemes could not be the same in all EU member states. Take a web video solution, or Skype calls for distant identity verification during customer onboarding, as an example. More often than not, the use of these new technologies represents a "grey area." It may be acceptable to supervisors for anti-money laundering purposes according to national implementing rules in one member state (e.g. Germany); and yet there is no guarantee that exactly the same solution would be deemed as lawful by supervisors in another country. Effectively, such regulatory divergence prevents banks from rolling out new advanced technological solutions and offering cross-border retail financial services to new customers.

Article 6 of 4AMLD mandates the European Commission to conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. A first report identifying, analysing and evaluating those risks at European Union level is to be drawn up by 26 June 2017. Thereafter, the report is to be updated every two years. The report will identify, *inter alia*, the areas of the internal market that are at greatest risk and the risks associated with each relevant sector. In addition to that, we encourage the European Commission to take a holistic, cross-sector view, specifically looking at the risks involved in cross-border customer identification and electronic authentication.

The revised Directive on Payment Services (PSD2) is yet another recently adopted EU directive relevant to electronic authentication in the financial sector. Enacted on 16 November 2015, it aims to contribute to a more integrated and efficient European payments market.[22] EU member states

20 European Commission, *Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight Against Terrorist Financing*, COM/2016/050 final, Strasbourg, 02 February 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050

21 The expectation is that the amendments to 4AMLD will be finalised in the course of the Slovak Presidency of the Council of the EU (before 2017). In the meantime, some EU member states proceed with the transposition of the original directive, while others took time out and are waiting for the final text of the directive.

22 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

The world of identity assurance and authentication mechanisms

Presently, there are five broad categories of identity assurance and authentication mechanisms:

1. Face-to-face contact: the most basic, traditional form of identity assurance involving a manual check of identity documents;
2. Username and password: organisation- or service-specific login details;
3. Single sign-on: an individual can login to one service using their accreditation from another (e.g. social media profile credentials);
4. Multifactor authentication system: secure authentication with at least two of the three elements – know, have and are;
5. Identity provider systems: federated identity systems with multiple identity providers with a "make once, use many times" approach.

Each of the categories has its own pros and cons, mostly in terms of a balance between costs, security and user convenience. Accessing news content online, available only to paid subscribers, can be done with username and password only. In contrast, by the nature of their business, financial institutions such as banks are required to adopt the highest standards of identity assurance. Presently, it is a multifactor authentication system. There is huge potential, however, in a transition towards certified (or government-led) federated identity systems. Digital identity assurance offers immense business opportunities in the digital age, with digital identity providers ranging from social media (Facebook, LinkedIn, Twitter) and postal services (Deutsche Post) to merchants (Amazon Payments), mobile network operators and banks. For more, see Alan Mitchell and Jamie Smith, *Economics of Identity: The Size and Potential of the UK Market for Identity Assurance* (London: The Open Identity Exchange / Ctrl-Shift, 2015) https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/

are required to transpose PSD2 into national law by 13 January 2018. Article 97 of PSD2 requires member states to ensure that payment service providers apply strong customer authentication. Specifically, to avoid divergence in approach, PSD2 mandates the European Banking Authority to draft new standards for the strong authentication of electronic payments by January 2017.[23] Common standards are important to avoid fragmentation and secure interoperability. They must be flexible enough to ensure that new ways to pay remain convenient and secure for consumers. Already today, the financial sector is exploring open universal standards, whose application should be lawfully recognized by the existing regulation.

The directive regulates payments executed by banks and payment institutions, and also, by third-party providers. These are services that collect and consolidate information on the different bank accounts of a consumer in a single place; other third-party providers facilitate the use of online banking to make

'The authentication standards applied should be fully mappable against an explicit and outcome-based framework, setting out clearly stated levels of assurance.'

23 Following the release of a discussion paper on future draft regulatory technical standards on strong customer authentication and secure communication under PSD2 on 08 December 2015, the European Banking Authority conducted an open consultation that ended on 08 February 2016. The paper formulated 20 questions. The EBA will assess the responses received, and use them as input for the development of the draft regulatory technical standards, which it will publish in summer 2016, for a consultation period of three months. Read more: https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2

Table 1. Regulatory alignment between eIDAS and sector-specific legislation

	Fourth Anti Money Laundering Directive (4AMLD)	Revised Payment Services Directive (PSD2)
Nexus with eIDAS	Business-to-Consumer: Identification of customers under 4AMLD, and opening and operating a bank account without face-to-face identity verification in a branch.	Business-to-Business: The eIDAS regulation offers a set of tools to match the requirements set in PSD2 in relation to strong authentication for online payments, particularly, for third-party providers, e.g. website certificates issued by a qualified trust service provider under an eIDAS policy.
Risk of inconsistency	eIDAS views e-identification as a new opportunity to facilitate the establishment of non-face-to-face business relationships. 4AMLD considers entering into relationships with customers not physically present in a bank branch as higher risk.	The use of eIDAS certificates may be complicated due to the liability regime not compatible with the liability regime under PSD2.
Follow-up actions	In line with the Action Plan for strengthening the fight against terrorist financing, the European Commission is preparing a modification of 4AMLD, in which the use of e-identification will be recognised.	European Banking Authority will continue its work on drafting the Regulatory Technical Standards by January 2017 in the context of PSD2.
Deadline for transposition	26 June 2017	13 January 2018

‘Successful measures for distance verification in the financial sector that are legal in some EU member states should be accepted in other EU member states.’

Leveraging the potential of blockchain

The blockchain – a revolutionary technology of a distributed public ledger – can potentially be leveraged for digital identity verification and customer authentication. Customer identity could be stored on a distributed ledger, not being under control of any institution. By their design, blockchain records are immutable – nobody can change a record, but can only append a new record. Due to the needed consensus among network nodes, and the potentially huge number of nodes in the network, it is almost impossible that anybody can change an existing record, unless it has control of most of the nodes. Today, over 40 of the world's leading banks, led by R3, a U.S.-based innovation firm, form a consortium partnership to design and deliver advanced distributed ledger technologies to global financial markets. Exploring the potential of the blockchain for digital identity verification is a very promising research avenue.

Internet payments. They all need to prove that they have certain security measures in place ensuring safe and secure payments. Authentication and verification schemes under eIDAS – such as website certificates issued by a qualified trust service provider – could potentially be applied for the authentication of third-party providers. And yet, the use of eIDAS certificates may be complicated due to the liability regime, which is not compatible with the liability regime under PSD2.

'Sharing of best practices should be promoted across borders.'

To sum up, to make eIDAS work in the financial sector, its regulatory alignment needs to be ensured with two sector-specific rules – 4AMLD and PSD2 (see Table 1 on page 16). There are synergies; and the eIDAS regulation has the potential to positively affect the financial sector, where obligations exist for security, reliable information and strong authentication of parties to a transaction. Specifically, the nexus and regulatory alignment between the eIDAS regulation and 4AMLD warrant serious consideration. In essence, while the eIDAS regulation presents e-identification as a new opportunity to facilitate the establishment of non-face-to-face business relationships, the tone of 4AMLD is more conservative. It holds that entering into relationships with customers not physically present in a bank branch is inherently high risk.[24] The expectation – and hope – is that the on-going amendment process to 4AMLD will recognise the use of electronic signatures and eID in the text of the directive.

Both directives and eIDAS are enacted, but the implementation and technical procedures for 4AMLD and PSD2 are still underway. The synergies between these areas – electronic identification and trust services, and sector-specific financial regulation – should be reaped and properly managed. It is important that EU member states transposing 4AMLD (and its forthcoming modification) and PSD2 into their national legislation should consider their overall fitness with the eIDAS regulation. Or, even more broadly, regulators and legislators need to think about digital technologies notionally, applying a "digital check" to all pieces of legislation and guided by the "digital-by-default" policy.

24 For a thorough discussion on this regulatory inconsistency, read: European Banking Federation, *Removing Regulatory Inconsistencies*. http://www.ebfdigitalbanking.eu/EBFDB_58.html

III. Solutions in the short and long run

As the European Commission acknowledged in two recent green papers – on the capital markets union and retail financial services – Europe's financial sector suffers from fragmentation along national borders. Cross-border digital identification is a crucial block for building a single market in financial services. If the single European market in retail financial services operates smoothly, European consumers will benefit from the breadth of competition, giving them greater choice, better services and lower prices. And for successful, innovative banks, embracing the digital transformation and seeking to offer the best value proposition, it will effectively offer a wider pool of clients from all across the Union.

'The successful take-up of the eIDAS regulation may help remove a major barrier to the cross-border provision of retail financial services.'

National eIDs should become a valid proof of identity for cross-border online onboarding. As for customer authentication, due to the heterogeneity of national eIDs in public services, the eID schemes under eIDAS can hardly be rapidly adapted to the realisation of strong customer authentication within payment services or account information services in all European countries. Thus, in the short term, a complete roll out of eID on a pan-European basis in financial services may not seem to be a realistic option.[25]

The eIDAS regulation is built on the principle of federated identity schemes while respecting domestic arrangements, which will be essential to scaling up eIDs. The same type of logic is applicable to federated identity solutions being deployed by banks in many countries on a voluntary basis (see the box on pages 4-5 and Table 2 on page 19 for an overview). Some of them are led by a group of national banks; others are done in collaboration with national authorities. Most of these systems are based on a residency criteria – one needs to legally reside in the country where this system is used.

This scheme is allowed under 4AMLD with specific conditions in place. They can be less risky than centralised solutions and deliver the required functionality. Importantly, new federated approaches could cut rising costs of identity assurance by 90%, as well as reduce levels of identity theft and fraud.[26] The case of the United Kingdom is telling. While the country doesn't have a national ID card system, the GOV.UK Verify scheme operated by public and private identity assurance providers offers a reliable identification solution.

The way forward is to ensure cross-connectivity of these national federated systems cross-border and, importantly, extend them to the onboarding stage, too. If a customer in Bank A in one member state has already opened a bank account and passed anti-money laundering checks, this digital identity could be transferred seamlessly to another bank (Bank B) – in the same or another member state, with the customer's consent. Customers will have access to their digital profile and will be able to retrieve it when needed to open a new bank account. The customer would not need

25 A view held by many, including the European Banking Federation. See, European Banking Federation, *EBA Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised PSD2,* 08 February 2016. http://www.ebf-fbe.eu/wp-content/uploads/2016/02/EBF_019489-EBF-Response-to-EBA-Discussion-Paper-on-SCA-and-secure-communications-under-PSD2-Final.pdf

26 Alan Mitchell and Jamie Smith, *Economics of Identity: The Size and Potential of the UK Market for Identity Assurance* (London: The Open Identity Exchange / Ctrl-Shift, 2015). https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/

Table 2. Examples of national federated digital identity systems

	Name	Launch year	Participating entities and available services	Underlying architecture
Estonia	e-Residency	2015	Public services, Internet banking	The service is open to foreigners; initial identification with nationals IDs
Denmark	NemID	2010	Danish banks, government websites and some other private companies	The service is based on CPR-Number (the Danish personal identification number)
Finland	TUPAS	2008	Finnish banks, public services (tax administration)	The service is based on Finnish personal identity number. It uses a password and a list of single-use passcodes or a passcode device
Italy	SPID (Sistema Pubblico di Identità Digitale)	2015	Public services	The service is additional and complementary to the national electronic ID card; provided by InfoCert, Poste Italiane and Tim (Telecom Italia)
Netherlands	iDIN	2016	Dutch banks and payment providers, national tax authority	The service is being developed and is to be used in parallel to DigID for the Dutch public services
Norway	BankID / MinID	2004	Public services, banking and insurance, commercial services	BankID is a Public Key Infrastructure (PKI) solution that supports both authentication and signing, storing the security elements on the mobile phone's SIM card
United Kingdom	GOV.UK Verify	2016	Government and commercial services	The service allows to substitute the non-existent ID card. Initial identification is done with UK passport, driving license or other valid documents. Accredited identity providers include, inter alia, Barclays, Post Office, Royal Mail and Verizon

to go physically to Bank B to complete all anti-money-laundering checks once again. The know-your-customer requirement will be satisfied, and for the customer, opening a new bank account will be a matter of a few clicks. Regarding the anti-money-laundering checks, all liabilities and responsibilities need to be clearly defined.

To be sure, the architecture will be underpinned by mutual trust and corresponding regulation. Fully operational, this federated solution will be open to all banks from all member states. In the first stages, however, it will be open for countries that already have eIDs and similar system of personal identification in place. This is similar to the Trust Services solution proposed in the eIDAS regulation, with the EU trust list of approved providers and services.

These federated systems should allow three-category verification, including bio-identification. In addition to that, the European financial sector can explore the possibility of a banking industry authentication standard or the use of open universal standards, such as OAuth/SAML.

'National eIDs should become a valid proof of identity for cross-border online onboarding.'

Ultimately, cross-border eID solutions should offer frictionless customer experience and cross-operability. It can be compared to the global chain of cash machines used by banks. Customers can use any cash machine with the same card (subject to certain conditions and restrictions). Pan-European solutions can be a long-run goal, and in the meantime, cross-border federated solutions should be explored. Following the successful completion of the STORK and STORK 2.0 cross-border programme (see the box on page 9 for more), the Connecting Europe Facility (CEF) has taken on the role to support roll-out of eID connectivity throughout Europe.[27] This has included the development of open-source software components, documentation, training and support. The CEF eID building block helps public administrations and private online service providers to easily extend the use of their online services to citizens from other EU member states, making national electronic identification systems interoperable.[28]

Once in place, this pan-European banking identity solution could potentially be used in other contexts where customer/ citizen identification and authentication are needed (e.g. e-government, other industries, other third parties). As holders of anti-money-laundering/ know-your-customer-proven data, banks could leverage this intangible asset and add a function of digital identity provider to their operations. They are in an ideal position to deliver digital identity solutions for both the private and the public sector. New revenue streams could be identified; they will help cover the costs associated with the pan-European banking identity service.

As progressively the single digital market and the cross-border provision of retail financial services – powered by digital identity solutions – become a reality, this development will unavoidably raise a number of much wider questions, particularly in relation to contract law. What jurisdiction's contract law will govern the relations between financial institutions and their clients residing in other member states? How will the right to judicial redress work in cross-border operations?

27 The eBanking Pilot within the Stork 2.0 project https://www.eid-stork2.eu/pilots/ebanking/index.php/en/. The first technical reference implementation for eIDAS cross-border eID interoperability framework is based on STORK results. See: https://joinup.ec.europa.eu/software/cefeid/description

28 Learn more about CEF eID building block: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

Table 3. Overview and comparison of digital identification solutions

	National federated schemes	Cross-border federated schemes	Pan-European eID solution
Description	Federated identity management system in a specific country (underpinned by the national unique ID)	National federated identity system open for customers of another country, or several cross-connected national federated systems	Common pan-European architecture
Implementing entity	Individual banks, in collaboration with national authorities	Individual banks, in collaboration with national authorities	EU member states, public administrations in collaboration with the private sector
Timeframe and feasibility	Established in some EU member states, in early stages in others	Pilot projects	Solution in the long run
Examples	See Table 2 on page 19	STORK 2.0 eBanking Pilot (banks in Austria, Iceland, Slovenia) – see box on page 9	Does not exist yet

Presently, firms must comply with a substantial body of regulatory requirements in each member state. A more long-term solution is the harmonisation of the contract law in the European Union.[29] In the absence of common European contract law, the Rome I Regulation governs the choice of law in the EU.[30] It sets out which law is used to interpret contracts with an international element – contracts agreed by parties in different countries. The parties may choose the contract law of the financial services provider's home country to apply to cross-border transactions. This choice, however, is without prejudice to the protection afforded to the consumer by the law of the country in which he or she is habitually resident. Legal scholars have proposed a number of legal solutions to bring more clarity in this complex matter, including a double-layered approach (combining non-harmonised national and harmonized European law), or an optional European set of rules (the "blue button" idea).[31]

'The eIDAS regulation is built on the principle of a federated identity scheme which respects domestic arrangements.'

29 In 2010, the European Commission published a green paper and held a public consultation on the prospects of European contract law. This work was renewed in 2015 in the context of online sales within the digital single market strategy. European Commission, *Green Paper from the Commission on Policy Options for Progress towards a European Contract Law for Consumers and Businesses*, Brussels, 01 July 2010, COM(2010)348 http://ec.europa.eu/justice/news/consulting_public/0052/consultation_questionaire_en.pdf

30 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008R0593

31 See James Devenney and Mel Kenny (editors), *European Consumer Protection: Theory and Practice* (Cambridge: Cambridge University Press, 2012).

We believe simple and effective cross-border contract rules for consumers and businesses are a priority in cross-border retail financial services. On 09 December 2015, the European Commission adopted two policy proposals: on the supply of digital content and on the online sale of goods. Both proposals are meant to tackle the main obstacles to cross-border e-commerce in the EU: legal fragmentation in the area of consumer contract law and associated high compliance costs for businesses and low consumer trust when buying online from another country. We believe the same logic should be employed in the design of regulation on cross-border retail financial services.

A voluntary single contract for cross-border retail financial services would eliminate legal complexity and, at the same time, would enhance consumer rights on cross-border transactions.

'The eIDAS regulation could easily form the nucleus of a larger, more broadly needed reform to give Europe better standards for online interoperability throughout the economy.'

Consumer rights are at the core of contract law. The Directive on Consumer Rights regulates distance contracting as of 13 June 2014, but does not apply to contracts for financial services, including insurance and investment.[32] This area – the distance contracting of financial services – is regulated by the directive on distance marketing of consumer financial services (DMFSD), adopted in 2002.[33] After an extensive review, in November 2009, the European Commission concluded that "in most member states, the market for distance selling of financial services has not changed significantly since the directive was introduced. At this stage, there is no evidence that consumers face problems arising from incorrect implementation of the directive." Nevertheless, the European executive stated its intention to monitor the developments in the distance financial services sector, and to take appropriate action if needed.[34]

The directive was born in the floppy-disks and CD-ROMs realities of the late 1990s, with contracts negotiated at a distance being the exception rather than the rule. Considering the sweeping developments in the financial sector in the digital age, there is a need to examine the fitness of DMFSD for cross-border retail banking operations in Europe; and the European Commission itself has stated its intention to assess the potential of DMFSD.[35] If such assessment is to take place, it should be guided by the overarching logic of "digital by default" and the removal of administrative limits on distance contracting.

32 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1

33 Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0065

34 Communication from the Commission to the Council and the European Parliament, *Review of the Distance Marketing of Consumer Financial Services Directive (2002/65/EC)*, Brussels, 20.11.2009, COM(2009) 626 final. http://ec.europa.eu/consumers/archive/rights/docs/com_review_distance_mark_cfsd_en.pdf

35 European Commission. *Green Paper on Retail Financial Services: Better Products, More Choice, and Greater Opportunities for Consumers and Businesses*, COM/2015/0630 final http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:630:FIN

Cross-border redress in financial services: FIN-NET

FIN-NET is a financial dispute resolution network of national out-of-court complaint schemes in the European Economic Area countries (the EU member states, Iceland, Liechtenstein and Norway) that are responsible for handling disputes between consumers and financial services providers. Launched by the European Commission in 2001, FIN-NET provides consumers with easy access to out-of-court complaint procedures in cross-border cases. Out-of-court procedures aim to offer an alternative way to solve disputes quickly, cheaply and easily, which may reduce the need to go to court. The bodies handling the complaints have a good knowledge of the particular financial services sector, and even though their decisions are not binding on the businesses in all schemes, companies tend to follow them. The FIN-NET framework is designed to allow a consumer to contact the out-of-court complaint body in their home country even when they have a complaint against a foreign financial firm.

Consumers in 22 EU member states, Iceland, Liechtenstein and Norway benefit from full-sector coverage, provided by 58 members of the network. FIN-NET is still not represented at all in Bulgaria, Latvia, Romania, Slovakia and Slovenia. The Financial Ombudsman of Cyprus acts as an observer to the FIN-NET group and the Swiss Banking Ombudsman also joined FIN-NET in 2014 as an observer. These members and observers of FIN-NET are linked through a memorandum of understanding. This scheme, however, became subject to new quality standards in January 2016, as the Alternative Dispute Resolution (ADR) Directive 2013/11/EU and the Online Dispute Resolution (ODR) Regulation 524/2013 came in force. ADR/ODR should further contribute to the availability of low-cost, simple and fast mediation procedures in EU member states, including in the financial services area. For more, visit http://ec.europa.eu/finance/fin-net/docs/guide/consumer-guide_en.pdf and http://ec.europa.eu/finance/fin-net/index_en.htm.

As for consumer redress, the work of FIN-NET – a financial dispute resolution network of national out-of-court complaint schemes in the European Economic Area countries – should be continued and deepened (see the box on page 23). Importantly, it should expand to cover all 28 EU member states.[36] In order to boost consumer confidence in cross-border retail financial services, consumers themselves should be made aware of this pan-European EU-led scheme available to them.

One thing is clear – the European financial sector needs the single rulebook, a single set of harmonised prudential rules for financial institutions throughout the EU, providing high protection to depositors, investors and consumers. Specifically, the European co-legislators should make a greater use of regulations rather than directives; or, at least, limit the leeway for member states in the transposition of directives. Quite often, diverging implementation and excessive regulatory norms and guidelines emerging from varying

> ‘New approaches could cut rising costs of identity assurance by 90% and reduce levels of identity theft and fraud.’

36 Bulgaria, Latvia, Romania, Slovakia and Slovenia do not participate in FIN-NET, and Cyprus serves as observer. See the box on page 23 for more.

transposition of EU directives into national legislation (known as "gold-plating") defeat the expected policy objectives of the European regulatory landscape harmonisation.

Digital technology, uniting financial markets and consumers on the continent and beyond, can hardly be regulated by diverging and fragmented legislation. We support the on-going collaboration among the European Commission's directorate-general for communications networks, content and technology (DG-CNECT), directorate-general for financial stability, financial services and capital markets union (DG-FISMA) and directorate-general for justice and consumers (DG-JUST) in pursuing the policies of digital identification in the financial sector. In particular, a cross-DG eIDAS interest group is set to become an important platform for such collaboration. Likewise, financial services should receive a prominent role in the eIDAS Observatory, launched on 30 June 2016 and meant to serve as a main platform to support a continuous dialogue and co-operation between stakeholders on digitisation challenges and opportunities.

'In the digital age, risk is caused by the denial of advanced, future-oriented solutions.'

Every new thing, every new undertaking looks risky and uncertain. There are always temptations to stick to decades-long tried-and-tested solutions, which are perceived as less risky. In the digital age, however, risk is caused exactly by the denial of advanced, future-oriented solutions. Outdated personal identification schemes cannot be a stumbling block in accessing modern, state-of-the-art financial services. Electronic identification and authentication should open up a wealth of financial products and services for all European consumers, allowing smooth cross-border access to a variety of financial services across the EU. Opening a deposit bank account in Spain and taking a mortgage in Germany – with the click of a mouse – should be possible in the single European market. Only by providing certainty on the legal validity of all digital services will businesses and citizens use digital means as their natural way of interaction.

References and further reading

Davies, Sally. "Banks Want to Keep your Digital ID in their Vaults," *Financial Times*, 02 September 2014 http://www.ft.com/intl/cms/s/0/9c1e4b06-328b-11e4-93c6-00144feabdc0.html

Dunkley, Emma. "Banks Accept Thumbprints and Selfies as They Chase Millennials," *Financial Times*, 08 April 2016 http://www.ft.com/intl/cms/s/0/95f3d770-fd71-11e5-b5f5-070dca6d0a0d.html

Euro Banking Association. *Opinion Paper on Digital Identity: From Check-out to Check-in, EBA Working Group on Electronic Alternative Payments* (Paris: Euro Banking Association, 2014) https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_Opinion_Paper_on_Digital_Identity_From_check-out_to_check-in.pdf

European Banking Authority. *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, Discussion Paper EBA/DP/2015/03, 08 December 2015 https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf

European Banking Federation. *EBA Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised PSD2*, 08 February 2016, Brussels http://www.ebf-fbe.eu/wp-content/uploads/2016/02/EBF_019489-EBF-Response-to-EBA-Discussion-Paper-on-SCA-and-secure-communications-under-PSD2-Final.pdf

----------. *e-Identification / e-Signature* http://www.ebfdigitalbanking.eu/EBFDB_56.html

European Commission. *Green Paper on Retail Financial Services: Better Products, More Choice, and Greater Opportunities for Consumers and Businesses*, COM/2015/0630 final http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:630:FIN

---------. *Questions and Answers on Trust Services under eIDAS* https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

European Financial Services Round Table. *The European Financial Services Landscape in 2015* (Brussels: EFR – European Financial Services Round Table, 2015) http://www.efr.be/newsstory.aspx?pvs=OACE76J%2frn7cFvK2rdSCMQ%3d%3d

Filippov, Sergey. *Financial Services in the Digital Age: Leveraging Technology and Regulation to Achieve a Stronger Capital Markets Union* (Brussels and London: the Lisbon Council and Nesta, 2015) http://www.lisboncouncil.net//index.php?option=com_downloads&id=1159

---------. *Government of the Future. How Digital Technology Will Change the Way We Live, Work and Govern* (Brussels and London: the Lisbon Council and Nesta, 2015) http://www.lisboncouncil.net//index.php?option=com_downloads&id=1215

PBLQ, the Dutch Institute for Public Administration. *International Comparison eID Means. Report Commissioned by the Dutch Ministry of the Interior and Kingdom Relations* (The Hague: Government of the Netherlands, 2015) https://www.government.nl/binaries/government/documents/reports/2015/05/13/international-comparison-eid-means/international-comparison-eid-means.pdf

Servida, Andrea. *Blogs. Digital Single Market* (Brussels: European Commission) https://ec.europa.eu/digital-single-market/en/blog/eidas-regulation-and-european-digital-single-market-4

Interviews

The author would particularly like to thank senior European Commission officials, financial professionals and industry experts who shared their wisdom, ideas and knowledge in a series of expert interviews:

- **Elena Alampi-das Neves Moreira**, assistant policy officer, task force legislation team (eIDAS), directorate-general for communications networks, content and technology, European Commission
- **Pascale-Marie Brien**, senior policy adviser, European Banking Federation
- **Sébastien de Brouwer**, executive director for retail, legal, economic and social policy, European Banking Federation
- **Ashley Davies**, senior developer, Number26 GmbH
- **Israel Hernanz**, innovation and development manager, financial systems and regulation, Banco Bilbao Vizcaya Argentaria (BBVA)
- **Katharina Lüth**, head of Europe, SavingGlobal Raisin
- **Robin Marshall**, chief information officer, Ulster Bank, on behalf of Banking and Payments Federation of Ireland
- **Olivier Salles**, head of unit, retail financial services and payments, directorate-general for financial stability, financial services and capital markets union, European Commission
- **Andrea Servida**, head, task force legislation team (eIDAS), directorate-general for communications networks, content and technology, European Commission
- **Bertil Vagnhammar**, policy officer, anti-money laundering policy, task force financial crime, directorate-general for justice and consumers, European Commission
- **James Waterworth**, vice-president, Europe, Computer and Communications Industry Association (CCIA)

As well as all participants and organisers of the eIDAS stakeholder event on 17 May 2016 "eID: Emerging Business Cases – Boosting Uptake," in particular:

- **Gino Giambelluca**, market and payment system oversight directorate, Banca d'Italia
- **Peter Kustor**, head, department for eGovernment, federal chancellery, Austria
- **David Rennie**, head, industry engagement for the identity assurance programme, GOV.UK Verify
- **Ott Vatter**, head, products and partnerships, e-Residency, government of Estonia

Additional acknowledgements

The author would like to thank the following individuals for their expert contribution and active support of this research project:

- **Francisco Javier Arias Marin**, head representative to the European Union, Banco Bilbao Vizcaya Argentaria (BBVA)
- **Christopher Haley**, head of startups and new technology research, Nesta
- **Brit Hecht**, senior policy adviser, European public affairs, Banco Bilbao Vizcaya Argentaria (BBVA)
- **Paul Hofheinz**, president, the Lisbon Council
- **Bernard Le Masson**, global managing director for public service, Accenture
- **Stian Westlake**, executive director of policy and research, Nesta

Digital Insight 06/2016 | ISSN: 0775-2180 (print); ISSN: 0775-2547 (digital)
Published under the editorial responsibility of the Lisbon Council and Nesta
Responsible editor: Paul Hofheinz, president, the Lisbon Council asbl

About the European Digital Forum

The **European Digital Forum** is a think tank dedicated to empowering tech entrepreneurs and growing Europe's digital economy. The initiative is led by the Lisbon Council, a European think tank based in Brussels, and Nesta, the United Kingdom's innovation foundation, in collaboration with the European Commission's Startup Europe initiative. The European Digital Forum was launched at the World Economic Forum in January 2014 as a vehicle to intellectually accompany the 22-point action plan put forth in the **Startup Manifesto** (www.startupmanifesto.eu) written by the Leaders Club, an independent group of founders of world-leading technology companies based in Europe, including Atomico, HackFwd, Rovio, Seedcamp, Spotify, Tech City Investment Organisation (TCIO), Tuenti and The Next Web. In the manifesto, which was drafted to spur discussion on improving Europe's startup ecosystem and digital-era performance, the European tech leaders proposed establishing a permanent independent think tank to explore and elaborate a more decisive approach to startups, an invitation which was seized and carried forward by the Lisbon Council and Nesta in 2014. Among the founding partners of the initiative are the European Investment Fund (EIF) and Banco Bilbao Vizcaya Argentaria (BBVA). Accenture is a partner. Follow the European Digital Forum on twitter at www.twitter.com/edf_eu.

www.europeandigitalforum.eu

The Lisbon Council asbl
IPC-Résidence Palace
155 rue de la Loi
1040 Brussels
Belgium

Nesta
1 Plough Place
London EC4A 1DE
United Kingdom

Design by karakas