EUROPE'S DIGITAL IDENTIFICATION OPPORTUNITY

William Echikson

CENTRE FOR EUROPEAN POLICY STUDIES

The Centre for European Policy Studies acknowledges support for this study from Deloitte, Mastercard, Stripe and Workday. Research was conducted in complete independence and the author takes full responsibility for its findings

Contents

Executive Summary

Europe has constructed a world-class digital identity and verification infrastructure for its public services. If it encourages and pushes the private sector to leverage and build on this accomplishment, the continent is poised to reap significant social, political and economic benefits.

The Covid-19 pandemic makes progress in digital identity and verification more pressing than ever. Digital verification helps people prove their identity without having to travel in person to a store or a government office. During the crisis, it has enabled consumers to buy goods and services and prove their age online and allowed furloughed students to take exams. Digital identity and verification is the ultimate social distancing tool. Even after the pandemic subsides, implementation of effective contactless identification will be required to unlock social and economic benefits.

Identity verification is critical to the economy. It isn't a 'nice to have.' It already is a regulatory requirement in many sectors, beginning with the financial industry. And yet while the internet makes it easy to grow businesses online, identity verification remains an area that continues to require physical interaction. The lack of robust, easy-to-use digital identity and verification has onerous, complex and costly consequences for all businesses, particularly start-ups and small enterprises.

Consider a few scenarios to understand why this is the case:

- Log into a bank in any European member country and request a mortgage. There is no need to upload reams of financial data, no requirement to mail or even scan and email a copy of your passport or other identity document. Via a mobile app, the bank receives secure verification of one's financial history, allowing it to approve or deny the loan request within seconds.
- Walk into an airport. There is no need to carry a boarding pass. Because airline documentation is linked to government-issued identity and verification documents, you proceed straight to security. Data protection concerns are allayed because the information is transferred via secure blockchain. The security check itself will be swift and almost painless, since security staff will be informed of previous clearances.
- The Belgian drinking age is 18. On their 18th birthday, a young Belgian wants to celebrate with a bottle of nice wine. They don't want the seller to know anything else about them other than their age – not their gender, name or nationality. Under Europe's new cross-border identity scheme, it is possible to provide the right amount of information – and no more.

As these examples demonstrate, digital verification goes far beyond an electronic identity card or an electronic signature that proves one's identity and consent. This is digital identification. By digital verification, we mean the collection of data verifying both identity and credentials – academic, financial and educational– which can be transmitted remotely in non-paper form.

While pursuing this seamless digital verification future, Europe must avoid creating a surveillance state. No one wants governments or public authorities to accumulate large amounts of sensitive information stored in digital form, which can be hacked, stolen or misused. Nor does one want to create a centralised 'digital identity' that could lock out legitimate users by mistakenly identifying them as 'bad actors', preventing them from buying, selling, or transferring money or information. As governments and industry work together to solve the technical challenges, both must remain aware of these crucial data protection concerns.

But the truth is that digital identification and verification offer opportunities to improve security and data protection, when compared to the high-risk collection and storage of paper documentation. Paper documents are easy to falsify. They may be stolen or lost and misused.

Secure encrypted blockchain or other types of privacy-protected digital verification avoid these risks. Constructed with care, they must comply with the European Union's General Data Protection Regulation (GDPR) and fit well into the European Commission's data strategy of February 2020, which supports the establishment of "common European data spaces," promoting the creation of "secure and universally usable digital identities."[1]

This report argues that Europe enjoys a huge opportunity to achieve its goal of secure, data protection-respecting digital verification. Today, governments control most forms of verification with passports and other government-issued credentials. Under the new regulation, it should be possible to allow individual European citizens to generate and control their own identity and credentials and to reveal the minimal information required by the application. An effective digital verification system will represent a major step forward to allow Europe to construct an effective digital single market.

The report will focus on Europe's government-led authentication programmes and how the private sector can build on it. It will not discuss in depth private sector initiatives led by Big Tech companies such as Apple, Google and Facebook. These initiatives do not offer legal certainty and they raise regulatory issues outside the scope of this study. Apple knows the apps that you purchase, Google follows your search history; Facebook hosts your social history and all three have developed secure double authentication. Europe could encourage – or force - internet giants such as Facebook and Google to build privacy-protected digital verification. The Commission's June 2020 consultation for its main regulatory digital initiative, the Digital Services Act, includes questions about digital identity and the measure of control exerted by Big Tech over it.

[1] European Commission, (2020b), "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, 2020.

Present-day verification often represents a time-consuming, arduous process, often requiring paper documentation. A passport, proof of address, driver's licence must be produced, along with a myriad of certifications guaranteeing credentials. Often, a physical face to face meeting is needed. Even if a physical meeting is not required, it can take days, even weeks to verify the validity of documents – such as nursing certifications, credit scores or corporate registrations.

Europe has made a strong start. Many of the continent's national digital verification programmes are world-class, including the government-led Belgian programme and a bank-led Nordic regional effort.

The European Union has constructed a unique cross-border electronic identification infrastructure with digitally linked verification (eID) and interoperable electronic authentication (eIDAS). To date, 12 European Union members plus the United Kingdom have given notice of their eID plans, with Denmark almost ready to notify and Latvia launching its process. A full list can be found on the European Commission's website.[2] A new Single Digital Gateway is being built that will allow citizens and companies moving to another EU member state to register their car or claim pension benefits without any physical paperwork.[3]

The European Union is the first and only region in the world where digital ID and verification are provided securely and are enforceable legally. The European Commission's vision is clear: to allow "people, companies (in particular SMEs) and public administrations to safely access services and do transactions online and across borders in one click."[4] European Union citizens should enjoy security and convenience "for any online activity such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another member state, authenticating for internet payments, bidding to on line call for tender."[5] If this goal is reached, studies from the World Bank, McKinsey and others show that the European economy could receive a boost of up to 3% of GDP.[6]

Bold steps are required to realise this windfall, however. The new European Commission (in office since December 2019) recently finished a public consultation on the eIDAS evaluation roadmap[7] and will soon be considering policy changes, including possible changes to existing legislation to increase the private sector use of this digital verification infrastructure.[8]

The issue has taken on greater urgency since the Covid-19 crisis. At their meeting in March 2020, European leaders discussed an initiative titled European Digital Identity, "with the aim of developing an EU-wide digital identity that allows for a simple, trusted and secure public system

[2] European Commission, (2019d), "Overview of Pre-Notified and Notified eID Schemes Under eIDAS."

[3] European Commission, (2018d), "The single digital gateway."

[4] European Commission, (2018a), "Trust Services and Electronic identification (eID)."

[5] Ibid.

[6] J. Manyika, S. Lund, M. Singer, O. White, O, C. Berry, (2016), *Digital Finance for All: Powering Inclusive Growth in Emerging Economies,* McKinsey Global Institute.

[7] European Commission, (2019f), "Secure electronic transactions – application of EU rules (report)

[8] Ibid.

for citizens to identify themselves in the digital space by 2027," according to the European Council's draft conclusions. [9] Though never formally adopted, the draft has encouraged the European Commission to come up with proposals by the end of 2020 and to revise the eIDAS Regulation.

This paper aims to add to this public debate and push forward regulatory moves to increase the deployment and uptake of digital verification, both within and across the borders of the European Union.

Europe's digital verification ambitions avoid most of the emerging political tensions about how to regulate Big Tech. While governments and internet companies will be contesting questions ranging from liability to content moderation and copyright, regulators and businesses agree on the necessity of building an effective digital verification system. This consensus allows both sides to work together in a constructive manner.

Despite this consensus, some sensitive challenging choices remain. Data protection and security concerns must be addressed. National objections to accepting other EU members decisions on authorising digital credentials must be overcome. The potential payoff is too large to ignore. Europe has a giant opportunity to become the leader in cross-border digital verification and take important steps to improving its single market and competitiveness.

[9] L. Kayli, (2020), "EU Leaders Want a 'European Digital Identity' by 2027," *Politico, Morning Tech Europe,* March 10.

1. The Global Identification Challenge

Throughout the world, a lack of accurate, trustworthy identification and verification represents a major economic and social drag.

The problem is most pressing in the developing world. Approximately one billion people lack a legally identified form of identification.[10] They have no birth certificate, no identity card, no passport or no driver's licence. Without identification they "may be denied access to critical government and economic services," McKinsey Research reports.[11]

Digital ID is only part of this story. The utility of a government-issued paper or digital identification depends on what information it contains and what type of services it can unlock. Does it just show where and when one is born? That is enough to prove that a teenager ordering an alcoholic drink is legal. It will not prove eligibility to obtain a mortgage or prove the credentials to work as a nurse or doctor. These tasks require one's financial information and education credentials. Throughout this paper, we will use the term digital verification to represent a broad definition of credentials-based authentication.

Most digital verification systems, even in the developed world, remain primitive. About 3.4 billion people own some form of officially recognised identity but with limited ability to use it in the digital world. The remaining 3.2 billion, mainly in Europe and other developed countries, benefit from digital ID – and what McKinsey describes as a "digital trail," the ability to leverage identity online in an effective and efficient way. Even lucky Europeans with a digital identity are often unable to accomplish complicated tasks requiring significant amounts of verified credentials-based information.[12]

Weak or non-existent digital verification represents a considerable cost and administrative hurdle. On average, today, businesses in Europe spend six to seven weeks verifying the identity of potential business partners or clients before starting to conduct business.[13] A few real-world, contemporary European examples illustrate the challenge.

- A Belgian citizen needs to open a bank account for a Dutch foundation. No Belgian bank will provide this service. The Belgian must travel across the border in person, prove his or her identity, show the notarised paper registration of the foundation, the original paper Chamber of Commerce credentials and sign the

[10] World Bank, (2018), ID4D Data: Global Identification Challenge by the Numbers.

[11] White, A. Madgavkar, J. Manyika, D. Mahajan, J. Bughin, M. McCarthy, & O. Sperling, (2019), *Digital identification: A key to inclusive growth. Executive summary*. McKinsey Global Institute.

[12] Ibid.

[13] Global Legal Entity Identifier Foundation, (2017), *The Legal Entity Identifier: The Value of the Unique Counterparty ID*.

bank account papers before a watching bank officer. In fact, they cannot do this alone. The bank requires two officers of the foundation to be present in person.[14]

- An Irish fin-tech company wants to onboard a Greek merchant for its payment service. A dozen different paper forms, full of official stamps, are required. Each European Union country has different rules on registration and on what percentage of shareholding requires authentication. The paper chase slows the company's pan-European rollout.[15]
- When a Swedish resident marries a Slovak citizen in Slovakia, it takes months of visits to different government offices to register the marriage and name change. The obstacles make it difficult for the wife to receive working papers or open a bank account and can create friction in the young marriage.[16]

If trustworthy digital identification and verification became the norm, these painful bottlenecks could be lifted, unlocking what has been estimated as time savings of 110 billion hours through streamlined access to public and private sector services.[17] Improved customer registration could reduce onboarding costs by up to 90%, and reduce payroll fraud, saving up to $1.6 trillion globally.[18]

For emerging economies, effective digital identification and verification could boost GDP by an average of 6% by 2030.[19] Some major developing countries could benefit even more: digital ID could unlock an additional 13% of GDP in Brazil by 2030.[20] Some 39 million Brazilians now without bank accounts could be able to open one. Other big potential beneficiaries include Nigeria (7%), and India (6%). Of the 1.7 billion people without a bank account in 2017, one in five blamed the lack of necessary identification documents.[21]

Women in the developing world will benefit most since they disproportionately lack identification.[22] Some 45% of women over the age of 15 live without identity papers in low income countries, compared to only 30% of men.[23] According to the World Bank "Increasing the identification of women can improve their inclusion and autonomy." When Pakistan used its national digital ID database, the government was able to make cash transfers to women for

[14] Author experience.

[15] Stripe company interview.

[16] Personal interview with author.

[17] Manyika et al., op. cit.

[18] Ibid.

[19] Ibid.

[20] White et al., op.cit.

[21] Ibid.

[22] Clark, J., Dahan, M., Desai, V., Ienco, M., de Labriolle, S., Pellestor, J.-P., … Varuhaki, Y. (2016), "Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation", World Bank Group-GSMA.

[23] World Bank. (2018). *ID4D Data: Global Identification Challenge by the Numbers*.

the first time – and a greater portion of household income was spent on nutrition and education than when the money went directly to men.

Although the potential upshot for developed European economies is not quite as revolutionary, it remains impressive. McKinsey estimates digital identification and verification could unlock an average of 3% of mature economies such as those of the US and Europe.[24]

Job searches will be eased. Digital identification and verification could, if used well, verify credentials and references, thereby eliminating background checks and allowing faster onboarding for both permanent and part-time gig positions.

Governments will see a potential boost in their tax revenues and a streamlining of their services. Estonians vote online, which authorities estimate saves 11,000 working days per election.[25] This is for a country counting a mere 1.3 million citizens.

Digital identity and verification would also improve tax collection. The International Monetary Fund believes that digitisation could broaden tax bases while streamlining tax filing.[26]

Perhaps the biggest boost will come to finance. New customers would not have to visit a bank branch to open an account or obtain a mortgage. Financial institutions must, by law, verify the identity of their merchants to comply with Know Your Customer and Anti-Money Laundering regulations.[27] In the UK, almost a third of financial applications are abandoned due to difficulties in registration. With digital verification, businesses will onboard clients in as little time as it takes for them to click 'login' on a mobile device. McKinsey estimates that the cost of providing digital accounts are 80% to 90% lower than using physical branches.[28]

The technology required to carry out a digital identification and verification programme is available – and its price is coming down fast. Biometric authentication, fingerprint sensors and bar codes may be leveraged to create secure signature or facial recognition. Blockchain is emerging as a viable way to allow the storage of data.

Keeping personal data secure is key – as is respecting human rights. In 2018, two German media companies analysed 2,000 credit reports, and found that many individuals received a negative rating despite never having defaulted on loans.[29] In February 2020, Dutch judges ruled illegal the government's algorithmic risk scoring system that used profiled citizens to predict the likelihood that social security claimants would commit benefits or tax fraud. Human rights campaigners have dubbed it a "welfare surveillance state."[30]

---

[24] White et al., op.cit..

[25] E-Estonia, (n.d), *E-identity: ID Card*.

[26] S. Gupta, M. Keen, A. Shah, & G. Verdier, (Eds.), (2017), *Digital Revolutions in Public Finance*. International Monetary Fund.

[27] White et al., op.cit.

[28] Ibid.

[29] Algorithm Watch, (2018), "SCHUFA a black box: OpenSCHUFA results published."

[30] N. Lomas, (2020), "Blackbox welfare fraud detection system breaches human rights, Dutch court rules," *Tech Crunch*, February 6.

A more mundane obstacle is unifying different European Know Your Customer regulatory frames, according to Francesco Cardi, Chief Strategy Officer of the digital verification leader Onfido. Ireland and the Netherlands take a 'risk-based' approach to digital verification, leaving to regulated entities the freedom to apply a wide set of measures, depending on the risk level associated with the use case. In these countries, banks are allowed to verify low-risk use cases with a simple third party database hit (typically, credit rating agencies), and handle high-risk cases by asking the user for legal documents and recorded videos or photos. Other EU members adopt a stricter approach, requiring a check of the user's legal documents and biometrics for all cases. For instance, in Germany and Spain banks must conduct live video call when onboarding each customer."[31]

As Europe moves to gain the full benefit of digital identification and verification, it must be careful to overcome these obstacles and dangers.

[31] Interview, Francesco Cardi, 17 March 2020.

2. Europe and Digital Verification

Europe's impressive journey to digital identification and verification has been long and arduous. Interoperability is easy to envision but expensive and difficult to achieve. The continent must overcome its different national legal frameworks and a multitude of different technical standards," notes a European Commission report.[32]

Europe's digital identity schemes remain fragmented, due to different historical and cultural attitudes among the 27 European Union member states. Under EU rules, national governments remain responsible for issuing identity. While countries such as Italy, Germany, Spain and Belgium long have had national identity cards, the UK and Denmark have no accepted national identity system and civil liberty motivated resistance to government-controlled proof of identity remains strong.

Because of their different histories and cultures, EU member states today rely on different types of digital identity cards, driver licences, or, among the Nordic countries, bank IDs. Within the EU27, 86 different versions of ID cards and 181 type of residence documents exist, says Pierre-Jean Verrando, Director General of the Eurosmart, a trade association for digital security companies.[33]

Instead of seeing this fragmentation as a disadvantage and insisting on a one-size-fits all formula, the European Commission has accepted the diversity and attempted to take advantage of it. EU policy focuses on securing desired common verification outcomes while relying on each nation's identity infrastructure. National verification schemes bring benefits. They build on existing national infrastructure and allow for digital verification to be tailored local markets and conditions; there is no need for a single accepted national identity card or a single accepted set of verified credentials. It should not matter, in theory, if a smart card, bank card, or SIM/mobile phone device is used for holding and transmitting identity credentials.

What is needed is to ease mutual recognition – the process by which European countries recognise and accept each other's national verification schemes. European policy aims to allow this interoperability. The European Commission has legislated and built an ambitious digital ID and verification system. Three basic building blocks buttress the European effort:

1. ID Cards: In 2006, the European Union agreed on a common design and minimum-security standards for national identity cards. Cards must be made of laminated paper and contain name, birth date, nationality, photo signature, card number and end date of validity. Some cards contain more information, such as height and eye colour.

[32] European Commission, (n.d.-a), *Electronic Identities – a brief introduction*.
[33] P. J. Verrando, (2019), "New EU eID cards regulation - a big move to keep a step ahead". Presentation: *The Identity Conference*, Eurosmart.

Importantly, countries are not required to issue such electronic identity cards, and some do not, for a variety of reasons ranging from the cost, in Greece, to fears of impinging upon civil liberties, in Denmark.[34]

2. eIDAS: The 2014 European Union regulation on electronic identification, authentication and trust services encourages member states to build and recognise private and public cross-border electronic identity verification systems.[35] Trust services do not depend on a physical ID card. They work with other types of verified national electronic identification schemes and credentials. eIDAS provides the legal framework for a market of trust services. Mutual recognition between EU members and cross-border legal certainty is crucial.

   This is where the acronyms become confusing. In EU jargon, eID does NOT refer only to electronic identity cards, it refers to the wider spectrum of digital identity credentials. eIDAS, by contrast, refers to the narrow authentication process, ensuring that electronic seals, time stamps and other electronic delivery services "work across borders and have the same legal status as traditional paper-based processes."[36] Under eIDAS, trust services rely on notified and legally recognised eIDs.

   eIDAS makes it mandatory for European Union public administrations to accept the electronic seals and signatures from other countries, whenever they require them at national level. A Cooperation Network allows EU members to achieve interoperability and security for their eID schemes. As we will see later, the narrow authentication process works well, but the cross-border acceptance of broader digital verification remains awkward and inefficient and needs additional refinement and improvement.
3. Single Digital Gateway: In 2018, the European Union mandated that member states must digitise 21 administrative procedures, including a birth certificate, car registration, starting a business or submitting a corporate tax declaration by the end of 2023.[37] This data will be available online through a single EU-wide online portal called Your Europe." Alongside this project, a separate new regulation tightens the security of ID cards.[38]

   Under the Single Digital Gateway, a French university will finally be able to verify the credentials of a German student submitting his or her academic diplomas directly from the German university without having to send in notarised paper forms or appear in person. The European Commission believes the Single Digital Gateway could save EU citizens up to 855 000 hours of their time annually and companies more than EUR 11 billion per year.[39]

---

[34] Council of the European Union, (2006), "Draft Resolution of the Representatives of the Governments of the Member States meeting within the Council on common minimum security standards for Member States' national identity cards."

[35] European Commission, (2018a), *Digital Single Market Policy: Trust Services and Electronic Identification [eID]*.

[36] Ibid.

[37] European Commission, (n.d.-d), op., cit.

[38] Verrando, op., cit.

[39] European Parliament, (2018), "Single digital gateway: a time saver for citizens and companies," *Press Release,* December 18.

The journey towards an interoperable digital European verification system began back in 1999 with the passage of the Electronic Signatures Directive. It provided a legal framework for the recognition of electronic signatures[40] across the European Union. Since then, the Commission has developed and financed a series of important steps:

- In 2006, the Commission published an eGovernment action plan[41] urging member states to "establish secure systems for mutual recognition of national electronic identity for public administration websites and services.[42] The Commission could not force member states to comply - it could only attempt to encourage and mobilise them.
- In 2008, the Commission introduced a "modular technological infrastructure" called STORK, built on top of national eID infrastructure. STORK proved that eIDs could safely and securely be used across borders.
- In 2012, the Commission created the Connecting Europe Facility (CEF) which provided €870 million for the creation of cross-border digital services in Europe.[43]
- In 2013, the Commission launched the Electronic Simple European Networked Services (e-SENS). Pilot projects were launched in 22 countries, building up a series of generic IT solutions for speeding cross-border identification.[44]

These projects shared a goal of improving access to eGovernment public services. Private sector applications were neglected. In its 2006 working paper, the Commission listed its priorities as "Social Security, Pensions, Health, company registration, certificates and licenses (Drivers and vehicles) and Taxation (VAT)."[45]

Difficulties soon emerged. The initial Electronic Signatures Directive limited its scope to EU public services. As a directive and not a regulation, the directive on eSignatures "left discretion over implementation into local law in the hands of member states, leading to a fractured, non-interoperable set of standards," the EU Blockchain Observatory and Forum in a 2018 study.[46]

Each European country continued to enforce a different legal framework for electronic identity and the definition of authentication levels. Member countries promoted their own local E-Signature standards, which were not recognised elsewhere. The Commission itself complained

[40] Commission of the European Communities, (2006), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions:"i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All."

[41] Ibid.

[42] D. Tinholt, N. van der Linden, S. Enzerink, R. Geilleit, A. Groeneveld, & G. Cattaneo, (2019), *eGovernment Benchmark 2019: Empowering Europeans through trusted digital public services*, European Commission.

[43] European Commission. (n.d.-e), "STORK | Take your e-identity with you, everywhere in the EU,"

[44] eSENS, (2017), "e-SENS – paving the way to the 'live' phase of cross-border digital public services."

[45] European Commission, (n.d.-a), *Electronic Identities – a brief introduction*.

[46] J. Grandsenne, (2018), "EU BLOCKCHAIN OBSERVATORY AND FORUM: Workshop Report e-Identity", Brussels, November 7, 2018.

that the Electronic Signatures Directive made it "de facto impossible to conduct cross-border electronic transactions."[47]

E-Signature proved unfit for the new internet age. As Richard Oliphant, EMEA General Counsel of the electronic signature company Docusign notes, the regulation "was drafted with hardware-based smartcard and handheld USB token technologies in mind and failed to account for new technologies that have emerged since 1999, including mobile technologies and the Cloud".[48]

Radical change was required and it came in the 2014 eIDAS regulation. eIDAS allowed European citizens, provided certain criteria are met, to access public services in other EU member states. Unlike the previous voluntary electronic signature directive, eIDAS committed member states to "cooperate in order to reach interoperability and security of electronic identification schemes".[49] Although eIDAS did not harmonise how member states issue eID credentials, it set the criteria by which eID are legally recognised across the Union and mandated the Commission to publish detailed criteria that allow member states to map their eID against a security benchmark (low, substantial and high).[50] Member states must give notice of their electronic identification schemes to Brussels.

eIDAS represented a major element of the ambitious 2015 European Digital Single Market strategy. Through 16 initiatives – including an end to unjustified blocking of content at national borders, a revamp of copyright, and an overhaul of telecom rules – the Commission attempted to unite Europe's fragmented digital economies into a unified market encompassing more than 500 million consumers.[51]

eIDAS created a European internal market for electronic trust services by ensuring that they will work across borders and have the same legal status as traditional paper-based processes. The Regulation defines an 'electronic document' as any content stored in electronic form, in particular text or sound, visual or audio-visual recording, covering 'blocks' in a blockchain.[52]

eIDAS recognised specific electronic signature types across the entire European Union, including:

- Electronic Signature: any signature in electronic form used to sign an electronic contract.[53]

[47] Ibid.

[48] R.Oliphant, (2016), "Learning from History: The Origins of eIDAS."

[49] European Commission, (2018c), "Electronic Identification and Trust Services (eIDAS): clear Benefits for SMEs."

[50] Ibid.

[51] W. Echikson (2017), "Europe's Digital Single Market Gets an F" *Huffpost.*

[52] European Commission, (2020), "Discover eIDAS."

[53]European Commission, (2019), "CEF eSignature facilitates the first electronic signature on an EU regulation!"

- Advanced Electronic Signature: one type of electronic signature with more stringent requirements for verifying the signer's identity and binding it to the document.[54]
- Qualified Electronic Signature: another type of electronic signature that meets all the requirements of an Advanced Electronic Signature but must be backed by a certificate from an organisation certified as a "Qualified Trust Service Provider" and produced using "Qualified Signature Creation Device."[55]

Under eIDAS, a qualified electronic signature issued by a trusted service provider established in one EU member is valid throughout the Union. This allows electronic verification of diplomas and other educational achievements, in theory solving the challenge for a nurse educated in one EU member state who seeks work in another member state hospital. He or she no longer needs to send a notarised paper certificate; eSignature and eSeal could verify the nursing certificate.[56]

After five years, a total of 172 qualified trust service providers have been established across the European Union. Individual member states have launched ambitious eID schemes and begun to experience the benefits of streamlined access to government services such as online tax filing and eHealth. Only 65% of the EU population is covered by qualified trusted service providers.[57]

Crucially, once an eID is legally recognised, the private sector can rely on it for identification and authentication. eID and eIDAS are embedded in sector-specific legislation, from new anti-money laundering to payment services, where it represents a key opportunity to fulfil the Know Your Customer requirement.

Yet failings are visible. Although the signature part of eIDAS has worked well, the broader eID part of the scheme to trust each other's credentials needs improvement. Only 14 out of the 27 European Union members have 'notified' eIDs under eIDAS. Many governments have felt little incentive to expend resources, given tight budgets and varying priorities.[58] The coordination network has proved to be slow and inefficient. Almost all progress concerns government services; the gigantic opportunity of private sector pickup has been missed.

A wide performance gap is also visible. In its latest benchmark, the European Commission noted a large gap between Nordic frontrunners and other countries in the number and scope of public services available to be verified and accessed online. While almost 98% of public services are available in countries such as Finland and Estonia, less than 40% are available online in Romania, Bulgaria and Greece.[59] The average European level is close to 65%, with some southern Europeans, namely Portugal and Malta, performing above average.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] European Commission, (2019b), op. cit.

[59] Tinholt et al. op. cit.

Public and Private Uses of eIDAS

Source: "Trust in a Digital Society" (2018) presentation by Anders Gjøen DG CONNECT, European Commission Unit, eGovernment & Trust.

The use of of digital identification and verification varies country by country. Estonia and Belgian cards allow access to more than 100 applications, from e-Health to public transport. Portugal allows e-Tax declarations.[60] And yet, many countries offer fewer than a dozen applications – and these are only public (not private) applications.[61]

Why has the pickup been so different across the continent?

Once again, part of the challenge is Europe's diversity. Although member states must comply with the security requirements of travel documents and are able to notify their eiD under eIDAS trust services, countries approach the challenge in different ways. Belgium operates a government-driven centralised system. The Nordics (i.e. the Finns, Swedes, Danes, Norwegians and Icelanders) prefer a decentralised, private-sector bank-led system. Some countries accept national identity schemes; others reject them out of civil liberty concerns.

eIDAS mandates the mutual recognition of different national digital verification systems, but the continent's system of peer review to allow cross-border functionality is complicated. Here's how it works – or rather fails to work. A member state notifies others that it has a new eID scheme via the Cooperation Network.[62] A formal review is scheduled. The Cooperation Network appoints a coordinator, a rapporteur, three to five experts, and an observer. The rapporteur leads the work, while an observer reviews draft documentation. After the review is completed, the committee holds a vote to approve. The coordinator provides "strategic oversight" and attempts to mediate disputes.[63] A majority is required.

This is time-consuming. Participants describe peer review sessions for approval as day or multiple day-long entailing mind-numbing word-by-word, line-by-line reviews. Some sessions involve as many as 70 questions. One regular participant described the process as having someone "pick your nose" for hours on end.[64] Measures are required to simplify and speed up the adoption of digital identity and verification.

An additional important challenge is security, particularly for physical documents. Some European ID and residence documents do not meet international document security standards. Even e-leader Estonia's ID card revealed a security weakness, reports Eurosmart.[65]

The dangers of weak digital verification security are serious: in the US, private companies such as credit monitor Equifax hold an abundance of data to verify identity and financial history. This privately-run system bringing continent-wide data together allows a quick one-stop-shop to verify the identity and credentials of more than 300 million American consumers. It also increases vulnerabilities. In September 2017, Equifax announced that it had experienced a data breach, which impacted the personal information of approximately 147 million people.[66]

---

[60] Autoridade Tributária e Aduaneira, (2020), "Portal das Finanças: Pagamentos."

[61] Verrando, op. cit.

[62] European Commission, (2019), "Single Market Scoreboard."

[63] Ibid.

[64] E. Van de Wynckel, (2019) *Identificatie, Authenticatie en Authorisatie*, DG Digitale Transformatie.

[65] Verrando, op. cit.

[66] JND Legal Representatives. (2019), *Equifax Data Breach Settlement*.

Equifax-style scandals underline the priority to protect privacy. In May 2018, Europe rolled out the pathbreaking GDPR data protection rules. GDPR includes broad definitions of what constitutes personal data, including emails and IP addresses. Under GDPR Europeans enjoy strong controls over their digital and identity data, including the right to demand that their data be erased and to restrict its use. Europe's privacy regulators have yet to give guidance on good GDPR practices with respect to eID and eIDAS applications.

GDPR should not present an insurmountable obstacle to digital verification. Under GDPR, consent is recognised as one of the alternatives for lawful processing of personal data. Most eID and eIDAS applications already obtain consent from users.[67] Right to review and erase has been implemented in some national eID cards. In Belgium, the country's ID card allows citizens to check which government officials have accessed their data – and to demand an explanation as to why their files were accessed. Estonians enjoy similar rights.

For the private sector, too, data protection rules could improve their own digital identity systems. Facebook and Google run what the World Bank calls a "self-asserted digital identity ecosystem" where "users choose their own digital identity attributes, and no verification against official identity documents is required, resulting in a lower level of security."[68] Logging in with Google or Facebook, the Commission fears, will require consumers to "unnecessarily" share personal data with "unrelated platforms" to access products or services online. If the companies could use effective eIDAS-powered GDPR- compliant identity checks, this verification could be improved. We would be sure that a person's Facebook and Google pages were genuine – while ensuring that Facebook and Google only receive the minimum-required information from their users.

For this vision to become a reality, security must be upgraded. Under a European Commission proposal, now adopted, ID cards should contain a facial image and two fingerprints and contain "sufficient capacity to guarantee the integrity, authenticity, and confidentiality of data." Governments are required to exchange the necessary information both "to authenticate the storage medium and to "access and verify biometric data." In addition, e-services must be physically or logically separated from the biometric data.[69] The European Parliament and European Council adopted these proposals this year and they become binding in August 2021.[70]

European authorities recognise the challenges to achieve world-class digital verification. The European Commission recently closed a public consultation and is considering putting forward policy changes, including new legislation by the end of the year.[71]

[67] Ibid.

[68] J. Clark, M. Dahan, V. Desai, M. Ienco, S. de Labriolle, J. Pellestor, … Y. Varuhaki, (2016), "Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation", World Bank Group-GSMA.

[69] Ibid

[70] Ibid.

[71] Gobierno de España. (2019), "The European Commission launches the public consultation of eIDAS."

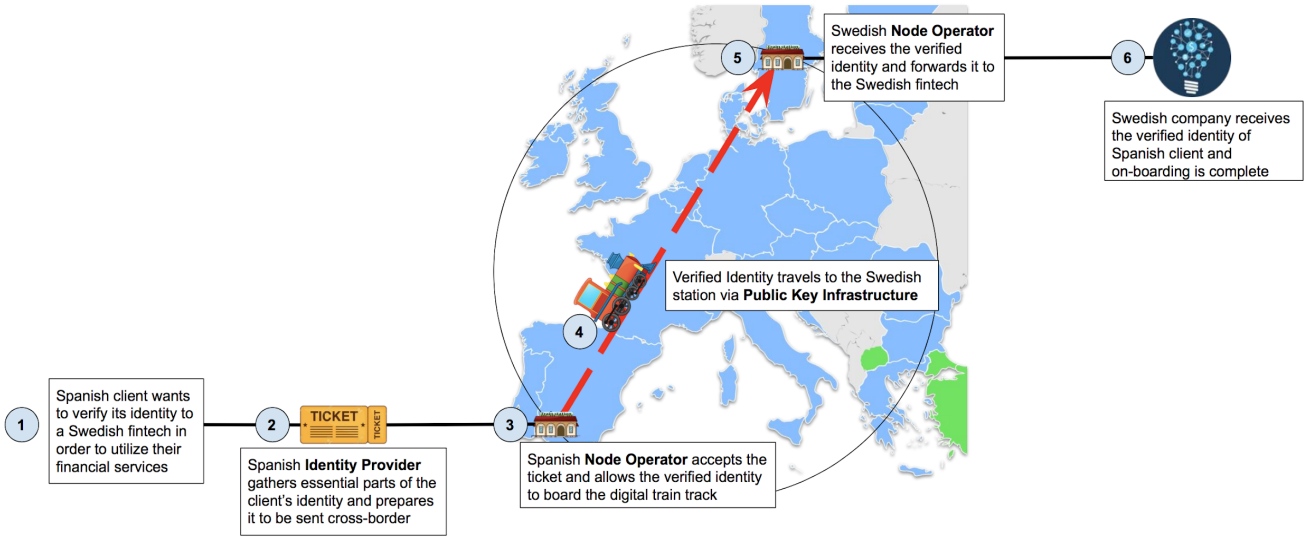
3. Policy Recommendations

Building a 21st Century Digital Train Network

Just as Europe is building high-speed trains to crisscross the continent, it should aim to build a high-speed digital identification and verification network.

The figure below explains digital identity train travel. A Spaniard wants to 'travel' digitally to Sweden to benefit from a Swedish fin-tech service. He or she buys a digital train ticket in Spain that represents his or her verified digital identity and boards the train in Spain. The train speeds to Sweden and stops at a Swedish node station, where the identity is verified and sent on for use at the fin-tech company.

Europe's Digital Identity Train



Source: Geoff Skelly, CEPS.

The vision that corresponds to this conception is a decentralised identity and verification system. Instead of a government or other central authority holding personal information, the goal "is to put the user at the centre of the framework and so remove the need for third parties to issue and administer identity," according to the EU Blockchain Observatory.[72] "This goal can be achieved by putting as much of the identity infrastructure as possible in the users' hands and otherwise relying on trustworthy decentralised methods" such as blockchain "without the

[72] T. Lyons, L. Courcelas & K. Timsit, K. (2019), *Blockchain and Digital Identity*, The European Union Blockchain Observatory and Forum. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

need for a third-party authority." Users create their own digital identities and attach information to their identity from trusted authorities.

Although European Commission officials are correct in proclaiming their digital verification framework as a global leader, it has failed to gain widespread daily pickup. Europe should be bold, expand the scope of effort and simplify its implementation. It should create an inclusive system, one that works for all European Union citizens, not just those that own the latest smartphones – and it should reassure privacy-sensitive Europeans that they continue to own and control access to their own data.

Our recommendations to achieve these ambitious goals include:

First, and perhaps most important, promote private pickup. The European digital verification system was designed to ease citizen-government interactions, but citizens conduct one or two interactions each year on average with their authorities. Private sector use will be key to reaching its potential, allowing private businesses to speed up the rollout of their services across the broad EU single market.

At present, only European governments may 'notify' eID schemes. Private companies should be able to propose solutions. New rules are required to verify the technology and process of private schemes and consider them as qualified trust services. Common identity verification standards should be instated in key pieces of legislation, as has been the case in the financial sector's anti-money laundering code. This is crucial because digital verification should allow banks and other financial institutions to meet Know Your Customer requirements – and to increase the effectiveness of their efforts to combat financial fraud.

Europe's Single Digital Gateway will allow the automated cross-border exchange of evidence for public services. It, too, is restricted to public services and government-approved private services. The Gateway should be extended to allow private actors, under strict conditions, to verify some information.

In February, 2020, a Commission Expert Group came up with other important new proposals designed to allow finance institutions to identify customers digitally at distance. The first report laments the present fragmentation of the European identification landscape and analyses current shortcomings and challenges.[73] A second report recommends measures to allow a Know your Customer "based on attributes, both for customer identification and customer due diligence matters" that "can either be document-based (i.e. when attributes are remotely extracted from existing ID or CDD documents) or natively digital, where attributes are communicated through established IT protocols without supporting documents."[74]

[73]European Commission (2019), Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions - December 2019 https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

[74] European Commission.(2019).,Assessing portable KYC/CDD solutions in the banking sector: The case for an attribute-based & LoA-rated KYC framework for the digital age - December 2019 https://ec.europa.eu/

Public private schemes should be encouraged. A good example is the Netherlands' impressive eHerkenning. It replaces the multiple sets of digital keys previously used by the Dutch government with a single token that enables organisations to make their services accessible online and securely to companies, civil servants and consumers. Users log in and eHerkenning checks whether the person using a service is actually who they say they are, and whether they are authorised.

The ultimate goal should be an attribute-based verification mechanism under which citizens and businesses own their own data. A trusted authority, public or private, would provide verification. Users could share the requisite attributes – a birth date, instead of sharing the full copy of an ID card, or even a yes/no reply (Q: Are you above 18? A: Yes). Microsoft, Deloitte and other organisations are working on such solutions.

Second, boost innovation including the adoption of blockchain while being technology neutral.

Blockchain offers the technical advantages of a decentralised identity model, with no storage on central database. It leaves individuals in control of their data. In principle, eID and eIDAS permit and encourage blockchain. The European Commission has sponsored the European Blockchain Partnership to promote a "digital identity" that protects privacy. Some decentralised blockchain ledgers seem to offer both data protection and security for data flows.

Nevertheless, some uncertainty remains. For blockchain signatures to be authorised, every signatory may need to undergo the costly and time-consuming process required for obtaining a certificate.[75] A European Parliament report recommends that "legal certainty for those wanting to use blockchain technologies is regulatory guidance regarding how specific concepts ought to be applied where these mechanisms are used."[76]

Blockchain should not be favoured over other technology solutions that promote simplicity, because data protection and user-centricity should be encouraged. Several organisations are currently working on this approach (see for instance the work of Mastercard on a decentralised interoperable digital identity model). Another good example is Fido. This public-private consortium has developed a cryptographic, on-device authentication that it claims is "safer and easier to use than passwords and one-time passcodes."[77]

Third, clarify GDPR data protection rules. Europe's data protection authorities need to provide workable rules to guide both governments and the private sector in their pursuit of digital identity and verification. How should GDPR principles such as data minimisation be applied?

---

info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

[75] Deloitte, (2019), "Blockchain: Legal implications, questions, opportunities and risks."

[76] Michele Finck, (2019), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf p. IV

[77] FIDO, (2017), "FIDO Alliance Launches European Working Group to Expand Use of Authentication Standards"https://fidoalliance.org/fido-alliance-launches-european-working-group-expand-use-authentication-standards/

Should there be limitations on what data can be stored and for how long? How should data subject rights, including the Right to be Forgotten, be implemented and enforced?

Such reassurance could take the form of various regulatory initiatives. The European Data Protection Board needs to update some opinions including one on anonymisation techniques. A good sign is that the European Data Protection Board has announced that it will publish additional blockchain guidance in 2020.[78]

Fourth, increase regulatory and financial incentives to accelerate digital verification. An example would be enabling eID/eIDAS to ease and simplify compliance with GDPR. Legally recognised and enforceable eID, solutions could exchange and transact with trustworthy identity credentials and attributes, while enforcing data minimisation and 'need2know' principles. Although the European Union should not oblige Google and Facebook and other tech giants to use eIDAS to verify the identity of their users, the EU should allow them to, and give them incentives to do so. **It could promote an open European ID login standard in its upcoming Digital Services Act.**

Fifth, offer clarity on potential regulatory conflicts. Today, verified credentials are being reused outside of their initial use case. The EU Blockchain Observatory "asks for legal clarification on the reuse" of credentials subject to anti-money laundering and PSDII payment regulations.[79]

Sixth, look at simplification. Instead of the present peer review system, a single European committee could review eID schemes. This unbiased eye could speed up the eID scheme review process and allow for private sector trusted service providers to enter the market. Although the committee's decision should be final and binding, national government fears could be assuaged by allowing them to vet and appeal recognition of trusted service providers before allowing their application.

Seventh, avoid allowing the push for digital verification to turn into digital protectionism. A buzz-term these days in Brussels is 'tech sovereignty'. Debate on digital identity and verification should focus on the needs of European consumers and businesses rather than on the geopolitical considerations shaping other aspects of European tech policy. It should not be about escaping the grip of large US and Chinese tech companies, nor should it be mixed up with dreams of creating a European data cloud or other industrial initiatives. It should be kept apart from a new Digital Services Act and other upcoming regulations designed to compel digital giants to take on more responsibility for what they host on their platforms.

Once Covid-19 subsides, Europe will need to reignite its economy. Digital identity and verification should play a key role.

---

[78] European Data Protection Board (2019), "EDPB Work Program 2019/2020." https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

[79] T. Lyons, L. Courcelas, & K. Timsit, (2019), *Blockchain and Digital Identity*, The European Union Blockchain Observatory and Forum.

Case Study:
Belgium - Leveraging Digital Verification

In Brussels, a patient hands over a prescription to a pharmacist. The face value of the medication is €50. Before paying, the patient hands the pharmacist his/her Belgian identity card. The government's subsidy is deducted, and the patient only pays €15, for example.

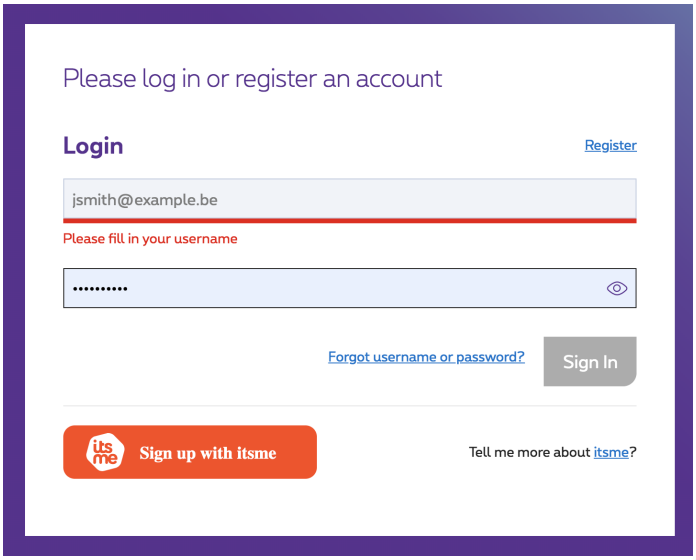
This time and money-saving exchange is made possible thanks to the innovative Belgian digital electronic identity card. More than perhaps any other European Union country, Belgium has leveraged digital identity for both public and private use. Its success shows what already is possible – and what remains to be done.

Belgium enjoys a longstanding system for identifying its citizens, dating back to Napoleonic times. During the 19th century, the newly independent country developed a civil registry, where all citizens and new-born children were required to be registered in a centralised database. Unlike in other countries such as the United States and United Kingdom, both of which have no single national identity cards, citizens trust the government to keep a record of their identity.

Today, each Belgian new-born is assigned a unique number that is carried throughout his or her life. This is mandatory, not voluntary. The national registry number contains, or links to personal information such as his or her mother and father, marital status, home address, and financial information, including tax payments. It allows an almost unlimited amount of personal information and credentials to be stored in a secure government database – and potentially shared for verification - through a citizen's identification number.

The rollout has been steady. In 2003, Belgium began issuing chip-based ID cards, replacing its previous paper-based cards. By 2008, every Belgian citizen over the age of 12 held an ID card that streamlines access to digitised government services. Belgian citizens under 12 years-old

carry a Kids card, which only allows for qualified electronic signatures and authentication. The total number of cards issued numbers 115% of Belgian citizens, because it includes foreigners holding residency permits.



The card's utility has expanded over time. The first government service to go online was taxes – and almost all Belgians now file electronically via Tax-on-Web. More services such as health are being added at a regular pace. Until November 2018, only the government was authorised to process stored data. A new law permits the private sector to take advantage, provided the government accepts the use case and the private companies receive GDPR-compliant consent from their clients. It is too early to judge.

Originally, a card reader was required to use the eID card. Today, a web app called Itsme® allows mobile phone access.[80] It replaces card-readers, passwords and tokens with a single five-digit personal code. All you have to do is log in using your personal Itsme® code or fingerprint. About 17.5% of all logins for government transactions now come via Itsme®, and 21% of Belgian citizens reported that they will use Itsme® for filing taxes in the next tax reporting period.[81]

Other ground-breaking experiments are taking place. The city of Antwerp has launched a decentralised blockchain pilot that allows individuals to decide with whom data is shared. The Port of Antwerp is also leveraging blockchain to create a 'smart' port, speeding up logistics of unloading at one of the world's busiest harbours – while increasing the security of the cargo information.[82]

[80] Itsme (2019), "Tax-on-web with itsme® making strong progress in Belgium: easy to use, secure and recognised by the government."

[81] Ibid.

[82] Port of Antwerp, (2017), "Smart port with blockchain."

Case Study: A Nordic Success Story

by Geoff Skelly

In Europe's north, it is almost as easy to buy a house online as it is to buy a book. Finns, Swedes, Danes, Norwegians and Icelanders can apply for and sign loan documents without even leaving their couch. The entire process of approving or denying a mortgage application takes two to three minutes.

Just as the Nordics are renowned for building a comprehensive welfare state on top of free-trade-minded market economies, they are solving digital verification through a combined pragmatic public and private-sector effort. Financial institutions have created identity systems called BankID, which the government recognise as legally binding for documents, transactions and other operations, both public and private. In Sweden alone, the digital BankID has 7.5 million users – almost the entire adult population. The BankIDs work well across the Nordic borders. According to a Ramboll Consultancy Study the value of the Nordic eID system reaches €17 billion annually.[83]

Unlike Belgium, where the government built upon its own central population registry, the Nordics distrust government-controlled citizen identification. This opened the door to private-sector solutions. The most popular and successful method leveraged the infrastructure of private banks. During the 1980s, Nordic banks needed a way to verify the identity of the person cashing a cheque, so they began issuing physical ID cards. The banks soon digitised the ID card, allowing it to be updated and verify a client's financial information. Banks soon realised their identification technology could be leveraged to ease non-banking tasks, and Nordic citizens began using their bank ID card (not a card, but a mobile phone solution) to perform a wide variety of tasks.

Governments picked up on the opportunity. In 2017, the Nordic Council and the Council of Ministers created the Council of Ministers in Digitisation to lead Nordic efforts on issues relating to eID and cross-border operability. The Nordic Council of Ministers in Digitisation agreed to utilise the existing bank infrastructure to install eID, permitting the bank ID system to access government programmes. In Norway and Sweden, the eID scheme is called BankID, while in Finland it is called MobileID, and in Denmark the NemID. Despite the different names, all these public ID systems verify identity through information accessed by a bank card.

[83] L. van Marion, & J.H. Hovland, (2015), *The Nordic Digital Ecosystem: Actors, Strategies, Opportunities",* Nordic Innovation, Oslo.

In Norway and Denmark, uptake is well over 90%, with citizens using their bank identity solutions, on average, once every two days. That adds up to 150 million times a year. Nordic governments have bolstered the system's utility by increasing online public services from 200 to 3,000. Today, the BankID allows Nordic access a broad range of public services, from online tax-filing to transferring academic records when applying to international schools.

Private sector use is booming. Because all banks in Norway use the same eID, a Norwegian citizen can access or even open a bank account at any Norwegian bank from anywhere in the world. All Norwegian banks accept the same BankID, allowing almost all financial transactions to be done digitally.

The Nordic identification system is considered a semi-centralised, federated system. This means there are multiple, government-endorsed digital identity providers that compete in an open market for customer service. Citizens are able to choose from a multitude of trusted identity providers, varying from banks to mobile operators. In Norway, 90% of identification is done through BankID while the remaining 10% is done by private companies that specialise in verification, like Buypass or Signicat.

These companies play an important role because they provide additional options for B2B verification when BankID is not an option. Despite large investments in digital identification across the EU, 2019 revealed that 38% of all European financial service applications are abandoned due to verification challenges. These third-party verification providers are necessarily filling this gap by providing more options to citizens.

The next step is to expand the system beyond the northern region. The Nordic region is already partnering up with Baltic nations – Europe's first multi-regional digital network. As the clear front-runner, the rest of Europe should look to the north as a roadmap for a pan-European solution to the digital verification challenge.

Case Study: UK e-Verification Struggles

by Justin Jin

When the UK government launched GOV.UK Verify in 2011, supporters billed it as a revolutionary digital verification tool. It would not depend on an open-to-abuse central government citizen database. The private sector would drive a decentralised operation, with competition making it cheap and effective.

Instead, Verify.gov has struggled. Pickup is low, both in the private and public sectors. The system suffers from a complicated authentication process – and most of all, from its voluntary rather than mandatory mandate.

Part of the specific UK challenge is historical. Unlike many other European countries, the UK has never had a centralised government ID database or national identification system, for fear of government overreach. Attempts to produce one generated significant political pushback.

Without a single institution able to command the trust of a large majority of the British public, digital identity efforts allow only niche applications. A national insurance number is required to receive state pension and other benefit payments but is not legally permitted to be used as a form of ID for other operations. The National Health System Card and authentication for the Gateway tax platform allow access to their individual narrow silos. None of the systems is interoperable.

GOV.UK Verify was created to respond to the same challenges as the National Identity cards, except in a more politically palatable form. Rather than a centralised database, it relied on a federated system of databases, each providing access when absolutely needed to confirm a user's identity.[84] A user paying their taxes through GOV.UK Verify would register or log in on the website in a process not unlike registering or logging in to a bank account.

A Labour government attempted reform in 2006 with the passage of the Identity Cards Act. It proposed combining biometric and property information, connecting the resulting profile to an identity card which, as Tony McNulty, the then Home Office Minister stated, would "be a panacea for identity fraud, for benefit fraud, terrorism, entitlement and access to public services".[85] Ministers claimed that the consolidation of identification methods would save

[84] E.A. Whitley, (2018), "Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach." Center for Global Development. *CGD Policy Paper 131.* November.

[85] BBC News, (2005), "Labour admits ID card 'oversell'", 4 August.

anywhere from £650 million to 1.1 billion per year, as well as disrupting organised crime and terrorism.[86]

Identity Card fell short of those expectations. Beyond the inevitable data protection and human rights issues raised by a centralised government database linking biometric, residential, and potentially criminal records with huge swathes of other personal information from a host of government databases, and widespread fears of discrimination against minorities, the technology was buggy and unreliable.[87] Some 31% of people were unable to verify their identities with facial recognition and around 20% of all people were unable to verify their identities using their fingerprints.[88] The database itself was not secure; some 25 million records were lost in 2007. After the 2010 elections, which brought the Conservatives to power, the project was ended.

Government projections were far too optimistic. A 90%+ identification success rate was predicted, with 25 million users and 19 government agencies signing up for GOV UK.Verify by 2020. Instead, the latest available figures show only 3.6 million users, 11 agencies signed up and a success rate of only 48%.[89]

Many agencies, including the Gateway tax portal and the National Health System card, declined to join and established their own, separate standards and platforms. Even for an unsuccessful government infrastructure project, Verify was "unusually bad," says Pauline Ngan and Sian Jones of the National Audit Office in an interview, and one of two to receive a red flag from the Infrastructure Projects Authority in 2018.[90]

After billions of pounds spent, the UK identification space remains fragmented across Great Britain and Northern Ireland. The Scottish government has announced a project aiming to create an independent system.

[86] Home Office Identity & Passport Service, (2007), *What are the benefits of the National Identity Scheme?*
[87] S. Arnott, (2006), "Cost of ID card technology pencilled in at £800m", *Vnunet News*, 12 October.
[88] D. Moss, (2009), "Collar the lot of us! The biometric delusion: Optimism beats evidence in the drive to fingerprint the world", *The Register*, 14 August.
[89] C. Burt, (2016), **"**Gov.UK digital ID service has fraction of intended users and verifies less than half successfully." *Biometric Update*, 6 March.
[90] D. Kundaliya, (2019), "'Verify' and 'TCEP' programmes deemed unachievable by UK government projects watchdog." *Computing.*

Case Study: Digital Identity Around the Globe

by Justin Jin

No magic bullet single formula exists for building a secure, privacy-protective digital identity scheme. Around the world, three different types of digital verification systems have emerged, from a centralised government-driven system such as the one in Belgium to the private operations run by American and Chinese tech giants Google, Facebook, Tencent and Alibaba.

Different types of transactions require different levels of authentication; the greater the risk of the transaction, the greater the assurance level required. In the Google and Facebook model, users choose their own digital identity and no verification against official identity document. This seems appropriate for the low-risk application of checking the social media network. It is not considered secure enough for high-risk transactions such as collecting benefits, which require "possession of a secure device, such as a physical token, a mobile phone, or a smartcard" to provide stronger security and a World Bank report finds "no examples of countries that have considered this (Google-Facebook) approach to provide access to their digital services".[91]

Government-driven, centralised systems are the most common. In addition to Belgium, Nigeria and India operate such a system. India's is the world's largest, with more than a billion people and more than 90% of their population enrolled. Called Aadhar, it authenticates access to a wide variety of government services, from rural employment systems to food security systems to pensions.[92] The government is pushing to link a wide range of private services, from bank accounts to HIV treatment.[93]

Aadhaar demonstrates the value of making enrolment easy. It accepts a wide range of documents to prove identity and address – including options for those who lack prior identification documents. Enrolment is free and mobile centres accept rural residents.[94]

But Aadhar's ambitious scope raises deep privacy concerns. Indian Supreme Court has prohibited mandatory enrolment in Aadhar and discrimination in services to those without an Aadhar number.[95] Aadhar does not count as proof of citizenship or residence. Given the recent controversies over citizenship and identity in India, Aadhar may soon become another flashpoint.

By contrast, the American digital identity system is decentralised, with no national scheme. It is an open marketplace of verification providers, each of which is accepted for different levels of verification. On the public side, login.gov, formerly known as the Federal Cloud Credential

[91] Clark et al., op. cit.

[92] K. Deepalakshimi, (2017), "The long list of Aadhar-linked schemes", *The Hindu*, 24 March.

[93] M. Rao, (2017), "Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India" *Scroll.in* 17 November.

[94] World Economic Forum,(2018), *Identity in a Digital World A new chapter in the social contract*. Cologny/Geneva.

[95] HT Correspondents, (2013), "No person should suffer for not getting Aadhaar: SC." 24 Sep 2013, *Hindustan Times*

Exchange (FCCX), streamlines access to expedited airport security check-in, and allows candidates for jobs in the Customs and Border Patrol.

Private credit-rating companies such as Equifax, which collects financial data tied to a single identity, are equally important identity verification providers. They generally work with financial institutions looking to confirm the existence of prospective borrowers. A host of other, smaller identification providers for various services, all of which are governed by government issued standards known as Know your Customer (KYC) and anti-money laundering (AML).[96]

Mixed public-private, semi-centralised federated systems are the most prevalent, and include the various Nordic BankIDs and the UK's GOV.UK Verify. Under such programmes, the government recognises several digital identity providers, including private sector players such as banks or mobile operators. Citizens are free to choose between them. Another example is the system used in Australia. The country has two major portals, Digital ID and myGov.id, both of which can be used to access government services. Neither depends on a physical card. Government agencies including the Post Office and Department of Defence as well as private companies like DigiCert provide authentication.

China's digital identity system represents a controversial model. Tencent's WeChat and Alibaba's AliExpress serve as aggregators, allowing consumers to connect their bank accounts, personal social media, and government identity. Both use text message and biometric photo authentication. Once authenticated, the app allows a wide variety of transactions, from purchases to investment to paying government fines. In some regions, like Guangzhou, the government has agreed to allow a trial of WeChat as official government identification.[97]

Today, WeChat functions as financial artery of the Chinese economy. Cash and credit cards have been almost entirely displaced as methods of payment, and WeChat is accepted everywhere from high-end restaurants to humble street vendors. The Chinese government has begun linking state service provision to these apps, including identification for entering and exiting Hong Kong. Instant verification of consumer identity is possible due to connection of government-issued ID to account. Business accounts are allowed, functioning in much the same way as an individual account for purposes of verification, albeit with business documentation instead of personal documentation required.

The big cloud hanging over China is, of course, its authoritarian government. China's communist authorities use access to these private authentication systems to enforce their one-party rule. In Xinjiang, home to a Muslim Uighur province, police scan identification cards, taking photographs and fingerprints, and searching cell phones. In some cities, like Kashgar in western Xinjiang, police checkpoints and facial-recognition cameras are omnipresent.[98] The government also collects and stores citizens' biometric data through a required programme advertised as Physicals for All.[99]

---

[96] Trulioo. (2019), "KYC: 3 steps to effective Know Your Customer compliance."
[97] Rohaidi, N. (2018), "Guangzhou now uses WeChat for digital identity", *Gov Insider*, 10 January.
[98] Wee, S. (2019), "China Uses DNA to Track Its People, With the Help of American Expertise." *The New York Times.* 21 February. https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html
[99] Ibid.

Bibliography

References

Algorithm Watch (2018), "SCHUFA a black box: OpenSCHUFA results published" (https://algorithmwath.org/en/schufa-a-black-box-openschufa-results-published/).

Arnott, S. (2006), "Cost of ID card technology pencilled in at £800m", *Vnunet News*, 12 October. (https://web.archive.org/web/20070930200641/http://www.vnunet.com/computing/news/2166159/cost-id-card-technology).

Autoridade Tributária e Aduaneira (2020), "Portal das Finanças: Pagamentos" (https://www.portaldasfinancas.gov.pt/at/html/index.html).

Burt, C. (2016), "Gov.UK digital ID service has fraction of intended users and verifies less than half successfully" *Biometric Update*, 6 March (https://www.biometricupdate.com/201903/gov-uk-digital-id-service-has-fraction-of-intended-users-and-verifies-less-than-half-successfully).

BBC News (2005), "Labour admints ID card 'oversell'", 4 August (http://news.bbc.co.uk/2/hi/uk_news/politics/4744153.stm).

Commission of the European Communities (2006), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions:"i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All" (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0173&from=EN).

Council of the European Union (2006), "Draft Resolution of the Representatives of the Governments of the Member States meeting within the Council on common minimum security standards for Member States' national identity cards" (http://www.statewatch.org/news/2006/dec/eu-id-cards.pdf).

Clark, J., M. Dahan, V. Desai, M. Ienco, S. de Labriolle, J.-P. Pellestor … Y. Varuhaki, (2016), "Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation", World Bank Group-GSMA (https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf).

Deepalakshimi K. (2017), "The long list of Aadhar-linked schemes", *The Hindu*, 24 March (http://www.thehindu.com/news/national/the-long-list-of-aadhaar-linked-schemes/article17641068.ece).

Deloitte (n.d.), "About Smart ID" (https://www.deloitte.co.uk/smartid/).

Deloitte, (2019), "Blockchain: Legal implications, questions, opportunities and risks" (https://www2.deloitte.com/content/dam/Deloitte/za/Documents/legal/za_legal_implications_of_blockchain_14052019.pdf).

Echikson, W. (2017), "Europe's Digital Single Market Gets an F", *Huffpost* (https://www.huffpost.com/entry/europes-digital-single-market-gets-an-f_b_59231eace4b0e8f558bb28a8?guccounter=2).

E-Estonia (n.d), *E-identity: ID Card* (https://e-estonia.com/solutions/e-identity/id-card/).

EHerkenning (n.d.), "Login with eHerkenning" (https://www.eherkenning.nl/en/inloggen-met-eherkenning).

eSENS (2017), "e-SENS - paving the way to the 'live' phase of cross-border digital public services" (https://www.esens.eu/).

European Commission (n.d.-a), *Electronic Identities – a brief introduction*.

European Commission (n.d.-b), *eID Documentation: Peer Review* (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Background+of+eID).

European Commission (n.d.-c), *eID Documentation: Background of eID* (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Peer+review).

European Commission (n.d.-e), "STORK | Take your e-identity with you, everywhere in the EU" (https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu).

European Commission (2017), "Commission expert group on electronic identification and remote Know-Your-Customer processes (E03571)" (https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailPDF&groupID=3571).

European Commission (2018a), *Digital Single Market Policy: Trust Services and Electronic Identification [eID]* (https://ec.europa.eu/digital-single-market/en/trust-services-and-eid).

European Commission (2018b), *Digital Single Market Policy: EU Trusted Lists* (https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers).

European Commission (2018c), "Electronic Identification and Trust Services (eIDAS): clear Benefits for SMEs" (https://ec.europa.eu/digital-single-market/en/news/electronic-identification-and-trust-services-eidas-clear-benefits-smes).

European Commission (2018d), "The single digital gateway" (https://ec.europa.eu/growth/single-market/single-digital-gateway_en).

European Commission (2019a), Assessing portable KYC/CDD solutions in the banking sector: The case for an attribute-based & LoA-rated KYC framework for the digital age, December 2019 (https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf).

European Commission (2019b), "CEF eSignature facilitates the first electronic signature on an EU regulation!" (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/09/27/CEF+eSignature+facilita_tes+the+first+electronic+signature+on+an+EU+regulation).

European Commission (2019c), *Digital Single Market Policy: Connecting Europe Facility in Telecom* (https://ec.europa.eu/digital-single-market/en/connecting-europe-facility).

European Commission (2019d), "Overview of Pre-Notified and Notified eID Schemes Under eIDAS (https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS).

European Commission (2019e), *Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions,* December 2019 (https://ec.europa.eu/info/sites/info/files/

business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf).

European Commission (2019f), "Secure electronic transactions – application of EU rules (report) (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/11973-Report-on-the-Application-of-the-eIDAS-Regulation).

European Commission (2019g), "Single Market Scoreboard" (https://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm).

European Commission (2020a), A European Data Strategy (https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy).

European Commission, (2020b), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: A European strategy for data* (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN).

European Commission (2020c), "Discover eIDAS" (https://ec.europa.eu/digital-single-market/en/discover-eidas).

European Data Protection Board (2019), "EDPB Work Program 2019/2020" (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf).

European Parliament (2018), "Single digital gateway: a time saver for citizens and companies" *Press Release,* December 18 (https://www.europarl.europa.eu/news/en/press-room/20180711IPR07739/single-digital-gateway-a-time-saver-for-citizens-and-companies).

European Union Agency for Network and Information Security [ENISA] (2017), *eIDAS : Overview on the implementation and uptake of Trust Services One year after the switch over* (https://doi.org/10.2824/611041).

FIDO (2017), "FIDO Alliance Launches European Working Group to Expand Use of Authentication Standards" (https://fidoalliance.org/fido-alliance-launches-european-working-group-expand-use-authentication-standards/).

Finck, M. (2019), *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* European Parliamentary Research Service (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

Gobierno de España (2019), "The European Commission launches the public consultation of eIDAS" (https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Octubre/Noticia-2019-10-11-Comision-Europea-lanza-consulta-publica-eIDAS.html?idioma=en).

Grandsenne, J. (2018), "EU Blockchain Observatory and Forum: Workshop Report e-Identity, Brussels, November 7, 2018" (https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf).

Global Legal Entity Identifier Foundation, (2017), *The Legal Entity Identifier: The Value of the Unique Counterparty ID*.

Gupta, S., Keen, M., Shah, A., & Verdier, G. (eds.) (2017), *Digital Revolutions in Public Finance*. International Monetary Fund.

Hansteen, K., Ølnes, J., & Alvik, T. (2016), *Nordic digital identification (eID): Survey and recommendations for cross border cooperation*, Nordic Council of Ministers.

Home Office Identity & Passport Service (2007), *What are the benefits of the National Identity Scheme?* (https://web.archive.org/).

HT Correspondents (2013), "No person should suffer for not getting Aadhaar: SC", 24 Sep 2013, *Hindustan Times* (https://www.hindustantimes.com/delhi-news/no-person-should-suffer-for-not-getting-aadhaar-sc/story-i4lEYx2uIRpMObetGOazTO.html).

Id (n.d.), "About id" (www.idservice.com/aboutid).

Ilves, L. K., & Osimo, D. (2018), *A Roadmap for a Fair Data Economy: Policy Brief*, SITRA.

Itsme (2019), "Tax-on-web with itsme® making strong progress in Belgium: easy to use, secure and recognised by the government" (https://www.itsme.be/en/blog/my-minfin-with-itsme).

JND Legal Representatives (2019), Equifax Data Breach Settlement (https://www.equifaxbreachsettlement.com).

Kayali, L. (2020), "EU Leaders Want a 'European Digital Identity' by 2027," *Politico, Morning Tech Europe,* March 10.

Kundaliya, D. (2019), "'Verify' and 'TCEP' programmes deemed unachievable by UK government projects watchdog", *Computing* (https://www.computing.co.uk/ctg/news/3079245/verify-major-infrastructure-project-impossible).

Lomas, N. (2020), "Blackbox welfare fraud detection system breaches human rights, Dutch court rules" *Tech Crunch*, February 6 (https://techcrunch.com/2020/02/06/blackbox-welfare-fraud-detection-system-breaches-human-rights-dutch-court-rules/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAN2B-iuKdxJeceHS8TZn44lN6iLgIIYFiuTC6n1XIuuR-eVbwQTAQlHri5C-N37OUAyUCgWj5VLNxsOZT5HwoO2-bKqnv8ZOJKl4zhk_tUed1LPnmff_pDd5Av9-FO_xnFJIAma097lyTVOoSAfcn4ik92aGdzK_642zo1S-U95N).

Lyons, T., Courcelas, L., & Timsit, K. (2019), *Blockchain and Digital Identity*, The European Union Blockchain Observatory and Forum (https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf).

Manyika, J., Lund, S., Singer, M., White, O., Berry, C. (2016), *Digital Finance for All: Powering Inclusive Growth in Emerging Economies,* McKinsey Global Institute.

Mastercard (2019), *Restoring Trust in a Digital World*.

Morse, A. (2019), *Report by the Comptroller and Auditor General: Investigation into Verify*, National Audit Office.

Moss, D. (2009), "Collar the lot of us! The biometric delusion: Optimism beats evidence in the drive to fingerprint the world", *The Register*, 14 August (https://www.theregister.co.uk/2009/08/14/biometric_id_delusion?page=2).

Oliphant, R. (2016), "Learning from History: The Origins of eIDAS" (https://www.docusign.com/blog/learning-from-history-the-origins-of-eidas/).

Port of Antwerp (2017), "Smart port with blockchain" (https://www.portofantwerp.com/en/news/smart-port-blockchain).

Rao, M. (2017), "Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India", *Scroll.in* 17 November (https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar).

Rohaidi, N. (2018), "Guangzhou now uses WeChat for digital identity", *Gov Insider*, 10 January (https://govinsider.asia/security/guangzhou-wechat-digital-identity/).

Servida, A. (2016), *Demystifying the new eIDAS framework: Regulation and Implementing Acts,* Brussels.

Tinholt, D., van der Linden, N., Enzerink, S., Geilleit, R., Groeneveld, A., & Cattaneo, G. (2019), *eGovernment Benchmark 2019: Empowering Europeans through trusted digital public services*, European Commission (https://doi.org/10.2759/950318).

Trulioo (2019), "KYC: 3 steps to effective Know Your Customer compliance" (https://www.trulioo.com/blog/kyc/).

Van de Wynckel, E. (2019), *Identificatie, Authenticatie en Authorisatie*, DG Digitale Transformatie.

Van Marion, L & Hovland, J.H. (2015), *The Nordic Digital Ecosystem: Actors, Strategies, Opportunities."* Nordic Innovation, Oslo (https://norden.diva-portal.org/smash/get/diva2:1295202/FULLTEXT01.pdf).

Verrando, P. J. (2019), "New EU eID cards regulation - a big move to keep a step ahead", Presentation: *The Identity Conference*, Eurosmart (https://www.eurosmart.com/wp-content/uploads/2019/07/EUIDCard-1.pdf).

Wee, S. (2019), "China Uses DNA to Track Its People, With the Help of American Expertise" *The New York Times,* 21 February (https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html).

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., & Sperling, O. (2019), *Digital identification: A key to inclusive growth, Executive summary*, McKinsey Global Institute.

Whitley, E. A. (2018), "Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach" Centre for Global Development, *CGD Policy Paper 131,* November.

World Bank (2018), *ID4D Data: Global Identification Challenge by the Numbers* (https://id4d.worldbank.org/global-dataset).

World Economic Forum (2018), *Identity in a Digital World A new chapter in the social contract*. Cologny/Geneva.

Interviews

Erling Håberget, Odd. 2019. Interview by Geoff Skelly. CEPS, July 5.

Odd Erling Håberget is the International Business Development Manager at Vipps, a Norwegian mobile payment application. Odd shared with us his expertise in data security and card payment infrastructure and services.

Johnson, Dan. 2019. Interview by Geoff Skelly. CEPS, July 19.

Dan Johnson is the Vice President of the Digital Identity and C&IS groups at Mastercard. Dan helped us to understand how Mastercard is going about building their own digital identity infrastructure to fill the gaps left open by the eIDAS regulations.

Müller, Pål. 2019. Interview by Geoff Skelly. CEPS, June 27.

Pål Müller is the Sales Director at Buypass, a Norwegian certificate authorizer. Buypass issues personal certificates to individuals and enterprises to allow for easy and secure identification and online payments across national borders. Pål helped us to understand the steps taken by Norwegian private companies to create a streamlined digital network in the Nordic region.

Cardi, Francesco, Interview, William Echikson, March 17, 2020

Francesco Cardi is Senior Strategy Officer of the digital verification company Onfidio.

Tsormpatzoudi, Pagona. 2019. Interview by William Echikson and Geoff Skelly. CEPS, July 12.

Pagona Tsormpatzoudi, is a Senior Managing Counsel, Privacy and Data Protection at Mastercard in Waterloo.

Van De Wynckel, Erik. Rogiers, Mathijs. Peeters, Noel. Vanhaecht, Jan. Interview by William Echikson and Geoff Skelly. CEPS, July 3.

Servida, Andrea. 2019. Interview by Geoff Skelly. CEPS, July 3.

Andrea Servida is the head of the “eGovernment and Trust” unit at DG CONNECT. This group led the European eGovernment Action Plan 2016-2020 and rolled out the eIDAS regulations on electronic identification and trust services for electronic transactions. Andrea helped us to understand how CEPS and the European Commission could hopefully work together to create a unified standard of security for digital services across the European Union.

Alvik, Tor. 2019. Interview by Geoff Skelly. CEPS, July 1.

Tor Alvik works at the Agency for Public Management and e-Government (Difi) in Norway. Tor has been instrumental in the strategic development of eID in Norway and leads Difi’s team involved in connection Norwegian and European infrastructure.

Friis Møller, Morten. 2019. Interview by Geoff Skelly. CEPS, June 20.

Morten Friis Møller works in the Nordic-Baltic Co-operation on Digital Identities (NOBID), which strives to ensure access to public services in other countries based on the eID schemes of a number of Nordic and Baltic nations. Morten shared the Nordic and Baltic model of digital services and hopes that the NOBID can act as a guideline for how the European Union can create its own single digital market.

ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy, Resources and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)