

DIGITAL IDENTITIES IN EUROPE

ANALYSIS, IMPLICATIONS AND OUTLOOK
OF THE DEVELOPMENT OF NATIONAL
OBSTACLES TO INTERPRETATION AND
IMPLEMENTATION

This report is based on the analysis of publicly available information at the time of writing. The information therein was correct to the best of the authors' knowledge and illustrates Arkwright's interpretations and working hypothesis at the time of publication. The report is not intended to be used within investment or management decisions and Arkwright accepts no related liability or responsibility. The brands and business models mentioned in the report are property of their respective companies.

INDEX

1. EXECUTIVE SUMMARY	5
2. PREFACE	8
3. INTRODUCTION	10
– 3.1. ELECTRONIC IDENTIFICATION SOLUTIONS ON THE RISE	10
– 3.2. MILESTONES IN IDENTIFICATION METHODS & TECHNOLOGIES	14
4. REGULATORY FRAMEWORK	19
– 4.1. REGULATORY LANDSCAPE	19
– 4.2. REGULATORY CHALLENGES	24
– 4.3. REGULATORY OUTLOOK	25
5. MARKET OVERVIEW	28
– 5.1. SELECTED COUNTRY CLUSTERS	28
– 5.2. CURRENT DEVELOPMENTS AND TRENDS	33
6. THE ROAD AHEAD	41
7. CONCLUSION	45
ARKWRIGHT PROFILE	46

**Digital Identities in Europe
Analysis, implications and outlook
of the development of national obstacles
to interpretation and implementation**

Published By
Arkwright Consulting AG
Alstertwiete 3
20099 Hamburg
Germany

Written and edited by:
Frank Wunderlich
Jerrit de Vries
Nicholas Kirilof

To request an electronic copy and for more
information on the topics of this report
please contact:
nicholas.kirilof@arkwright.de
jerrit.devries@arkwright.de

If you would like to be subscribed or to be
removed from our mailing list, please write to:
subscriptions@arkwright.de

Copyright © 2022
Arkwright Consulting AG
All Rights Reserved

1. EXECUTIVE SUMMARY

EUROPEAN PERSPECTIVE ON EIDS

This white paper is the continuation of our 2019 briefing on eIDs in the Nordic countries. Then, we analysed the development of federated eIDs such as BankIDs, explained why the Nordic countries are leaders in this area, and discussed possible future scenarios. Now, we are going to turn our attention to the rest of Europe, analysing the extent to which other countries have caught up, how various approaches differ, or borrow, from those found in northern Europe, and what developments we might see in the future.

EID SOLUTIONS ON THE RISE ACROSS EUROPE

eID comes in many forms, and adoption of electronic ID solutions (eIDs) is on the rise in many European countries, as detailed in Chapter 5. We identify four drivers for this trend: i) ongoing digitalisation, ii) the Covid-19 pandemic, iii) business considerations, iv) evolving regulations.

AN EVOLVING REGULATORY LANDSCAPE

One of the main drivers for EU and national markets are constantly evolving regulations. We identify two types of laws: facilitating laws such as eIDAS, which encourage the use of digital identities, and imposing laws (such as anti-money laundering laws), which mandate eIDs.

The main challenge for any Europe-wide eID system is to resolve the tension between legislation on an EU level, and the same rules once they are transposed into national legislation. The EU's main goal is not to establish its own solution, but to establish interoperability between solutions on a national level. One of the biggest obstacles alongside a fragmented legal framework will be reaching mass adoption within markets with different dominant identification methods. We see great promise in the eID wallet, announced by commission president Ursula von der Leyen in 2020, combined with Qualified Electronic Signatures, which will allow national flexibility while ensuring reciprocal recognition and portability for citizens.

OVERVIEW OF EUROPEAN MARKET

Our analysis of the European eID market in Chapter 5 divides Member States into groups according to the maturity of their identification methods and acceptance across the population: pioneers (where most Nordic countries are located), followers and laggards. In all three clusters, we observe several dynamics: ongoing consolidation, expansion of national players and new innovations entering the market.

FUTURE SCENARIOS

Finally, we look to the road ahead. For eIDs to be successful, they need to be convenient and enjoy high adoption. This is not the case for government-issued eIDs, and private entities have filled this gap in many countries.

This makes it difficult to predict what lies ahead. The success of private eIDs in many countries is a barrier to any universal, government-mandated initiative. However, the idea of entirely private-sector solutions raises questions about whether the state is willing to cede control in what is traditionally at the core of its duties: verifying citizens' identities and issuing the documents with which they can prove it. Further, a private-only approach raises the prospect of a mosaic of private equity-funded solutions and an outcome dependent on which provider acquires which.

2. PREFACE

DIGITAL IDENTITIES

When required to prove our identities, traditionally we have done so with physical media such as ID cards, passports or a driver's licence. This is satisfactory as long as business is conducted in person, but since services and the way in which we are doing business are increasingly being digitalised, new identification processes have emerged. These identification methods are the digital counterparts to the aforementioned physical identification methods. They provide the credentials necessary to trust that a person is who they claim to be online, and enable them not only to use services digitally, but also to carry out onboarding processes entirely remotely.

DIGITAL IDENTITY REFERS TO THE ACCEPTABLE AND TRUSTED DIGITAL FORMAT OF A PERSON OR COMPANY'S IDENTITY. DIGITAL IDENTITY VERIFICATION IS BECOMING INCREASINGLY CRUCIAL FOR THE ONBOARDING OF CUSTOMERS AT BANKS, TELCOS, RETAILERS/ E-TAILERS, AND INSURANCE COMPANIES AS THE WORLD RAPIDLY DIGITISES RIGHT NOW.

DIRECT TRANSACT

Northern Europe has been a first mover in the field of digital identities for years. Countries in this region have generally found ways to provide their citizens with online identities which are recognised by casual, private users and governmental authorities alike. Opting for a federated approach, banks have joined forces and taken on a crucial role in this endeavour. Collectively, they have already authenticated the majority of their countries' citizens and transferred them to an online solution – online banking. After the use of e-IDs for online banking became well established, other online services were created, exploiting the same ID methodology and digital environment to promote market penetration while engendering acceptance among the general public in northern Europe. In a previous paper titled "Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets", published in 2019, we already related the history, recent developments and implications of e-IDs in northern Europe.

EUROPEAN DIMENSION

In recent years, the rest of Europe has been rapidly catching up, offering a wide range of solutions that are disrupting markets by challenging incumbents' business models, reacting to changing customer needs and responding to the latest regulatory changes.

National solutions are expanding across borders and EU initiatives aim to consolidate different approaches. The lessons learned from the Nordic markets can be extracted and used to analyse the spread of digital identities across Europe.

Thus, this paper is a logical extension of the "federated e-IDs" paper and broadens the view to a European level, looking at possible scenarios for future developments of digital identities in Europe.

For this purpose, we take a closer look at the regulatory environment and its relevant innovations as well as the developments resulting from changed market dynamics in European countries, before discussing the road ahead.

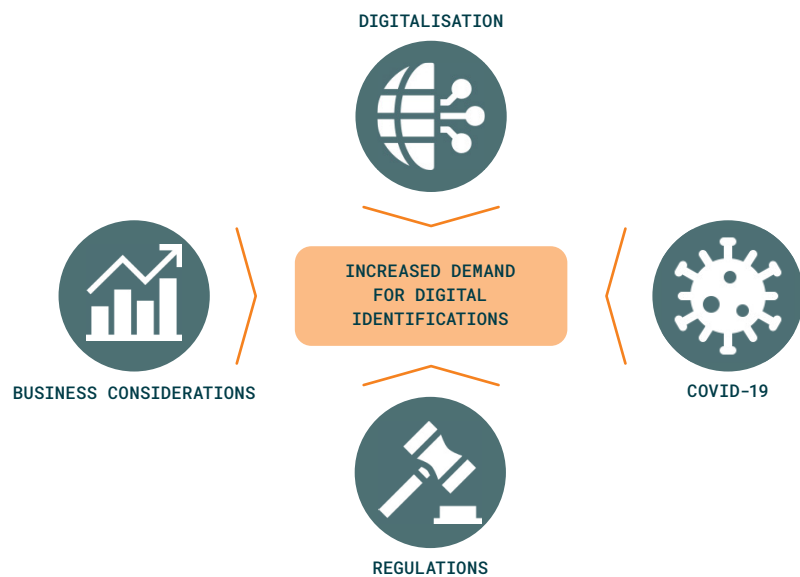
3. INTRODUCTION

3.1. ELECTRONIC IDENTIFICATION SOLUTIONS ON THE RISE

Market dynamics throughout Europe are shaped by four main factors (see chart below) that have contributed to increasing demand for digital identification. We will take a look at these in detail in this paper:

- Ongoing digitalisation,
- Long- and short-term Covid-19 implications,
- Changing regulations and business considerations.

Fig. 1 – Factors driving the demand for digital identification.



DIGITALISATION

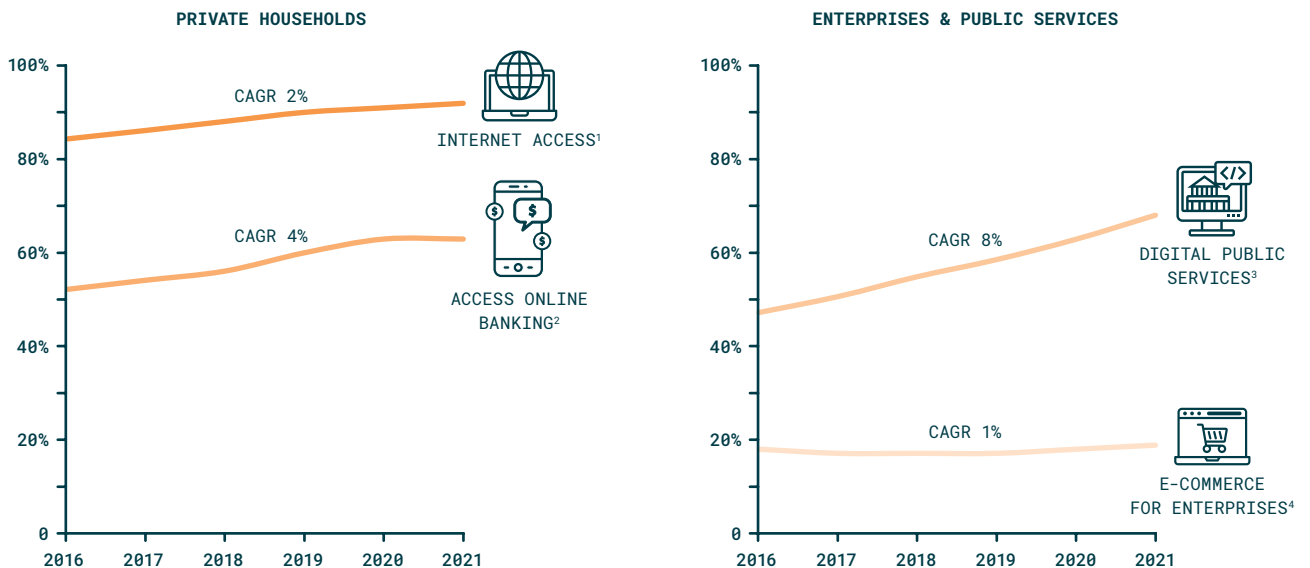
When it comes to digital identities, digitalisation affects three different areas in particular: governmental structures, business offerings and the personal digital environment.

Governmental structures refer to the acceptance of e-IDs for public services such as car registration and other public-sector services.

Business offerings have changed dramatically over recent years. Besides the fact that e-commerce has become the dominant channel for shopping in many verticals, digital services and solutions are also becoming the new standard forms of interpersonal communication and transacting with financial institutions. Offering digital services and solutions entails fast and convenient onboarding and identification processes.

The **personal digital environment** is dependent on access to broadband internet, digital tools such as smartphones and the ability to participate in a digital world. Through 24/7 online availability, it has become possible to move analogue processes online, such as payments between peers, bank account transactions, changing insurance plans or trading stocks; all services which require a certain level of security and validated identifications. While the level of digitalisation – in terms of speed and availability of internet connections – varies across Europe, the trend over recent years shows an increasing share of the population gaining access to fast internet in every country. Access to online banking plays a crucial role. Compared to northern Europe, it can be seen as one vital part of the e-ID ecosystem and a point of contact that benefits from existing means of identification.

Fig. 2 – Trends indicating increasing digitalization in the EU27.



¹ Eurostat (2021): % of households with internet access.
 ² Eurostat (2021): % of individuals living in cities using internet banking.
 ³ Eurostat (2021): % of enterprises with e-commerce sales of at least 1% turnover (excl. financial services).
 ⁴ Eurostat (2021): Weighted score of the DESI (Digital Economy and Society Index) dimension (0 to 100).

COVID-19

The two most obvious implications of digital processes compared to analogue processes are increased speed because on-site appointments are no longer necessary and more convenient due to remote processes and better user experience, ultimately making an enjoyable process of a formerly inconvenient procedure. Digitalisation as a trend in its own right is again catalysed by the current Covid-19 situation.

Covid-19 has had massive implications for our daily life and requires us to substantially reduce physical contacts, making it unviable to offer certain services in their traditional (analogue) form. Businesses and governments are therefore required to offer new (non-physical, i.e. digital) solutions and enable remote onboarding and identification processes, since the requirements for these services stay the same even when on-site counters are closed. Video identification is an example of a form of digital identification that gained significant relevance in Germany during the pandemic.

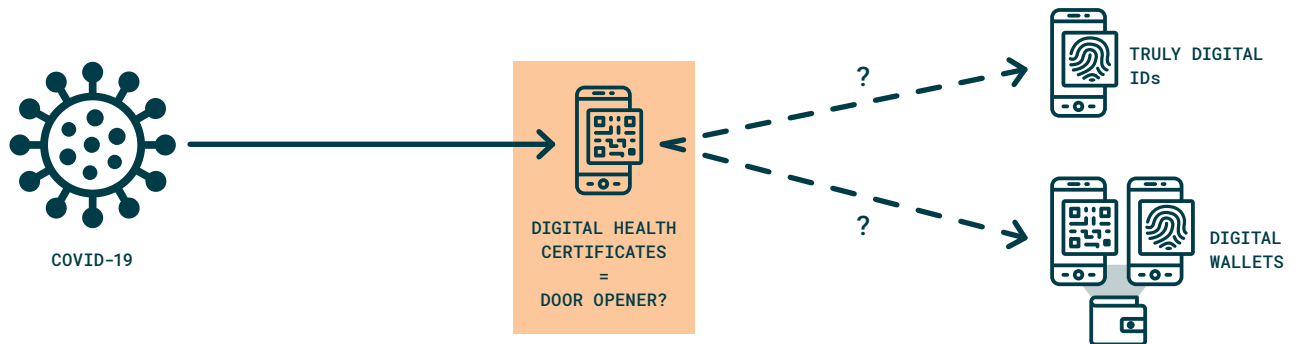
THE COVID-19 PANDEMIC, MORE THAN ANY OTHER EVENT IN RECENT HISTORY, HAS HIGHLIGHTED THE NEED FOR DIGITAL SERVICES AND LAID BARE THE SHORTCOMINGS IN DIGITALISATION PREVALENT ACROSS OUR CONTINENT.

JOINT DECLARATION ON COOPERATION AND EXCHANGE
OF BEST PRACTICES IN THE FIELD OF SELF-SOVEREIGN
IDENTITY BETWEEN THE FEDERAL REPUBLIC OF GERMANY
AND THE KINGDOM OF SPAIN

Since humans are creatures of habit, it can be assumed that these developments will continue beyond Covid-19.

The parallels to cashless payments are obvious: once someone is familiar with a new payment method, the barriers to returning to the initial form (e.g. cash, which is increasingly substituted by non-cash payments) are high. Digital Covid-19 health certificates, stored mainly in smartphone apps, are another example of digital mass adoption and growing acceptance. Since these certificates are already a form of digital identification, this might encourage the adoption of truly digital IDs.

Fig. 3 – Digital health certificates as a door opener for digital identities?



REGULATIONS

Additionally, evolving regulations are continuously driving up the number of digital identifications since European and national regulations have opened up to non-face-to-face forms of identification over the past 20 years. The main objectives of these changes are usually to prevent fraud on the one hand and enable fast and convenient solutions for end customers on the other. These two divergent interests lead to different national laws and European initiatives trying to reconcile different regulatory landscapes. Details on specific regulations and their implications can be found in [Chapter 4](#).

In general, one can observe that the regulatory environment has tended to become stricter in recent years. For example, because anti-money laundering (AML) regulations have subsumed new industries or imposed stricter rules on those already regulated, we can observe a rising demand for digital identification in the affected European countries. An example can be found in the online gambling industry in Germany, where the new State Treaty on Gambling, which came into effect in July 2021, requires providers to fulfil mandatory age verification requirements.

BUSINESS CONSIDERATIONS

From a business perspective, there are many factors which favour increased demand for digital identification. Digitalisation can provide an end-to-end digital process, thereby improving the customer experience through faster turnaround times and a seamless process uninterrupted by offline steps. Additionally, digital idents enable cost savings (up to €5 per ident) for customers of these services. Apart from these business considerations, the environment is changing. Since more and more existing products or services are becoming digital, a higher number of idents will be needed. Fintechs are only one example of an industry which is solely acting in the digital payment ecosystem and depends on such new forms of identifications.

[...] YOU NEED TO BE CERTAIN YOUR DIGITAL TRANSACTIONS ARE FULLY LEGAL, ACCEPTED ACROSS BORDERS, AND COMPLETELY SECURE. BUT IN REALITY WHAT YOU ARE SIGNING, WHEN MAKING A DEAL, IS JUST ONES AND ZEROS ON A COMPUTER.

SIGNICAT

In some cases, certain products in the area of financial services or fintechs can only be offered because we have new forms of digital IDs and these are both economically beneficial (no need for personnel, lower costs) and meet customer requirements (faster and more convenient). These prerequisites, in turn, also foster an increasing number of identifications.

3.2. MILESTONES IN IDENTIFICATION METHODS & TECHNOLOGIES

In addition to these general driving forces of digital identification, the range of methods and providers of these solutions is evolving as well. Even though the markets in Europe vary in the solutions they use and provide, technical and regulatory advances are supporting the general trend towards more sophisticated solutions with higher ease of use for the end user and lower costs per identification for financial institutions.

Traditionally, the identity of an end customer has been verified in face-to-face situations, where the end customer can present themselves physically to the financial institution or to a service provider such as a post office or a bank. Through the emergence of online channels, more and more solutions have been developed, and providers of these solutions have emerged that allow financial institutions to identify prospective customers that are not physically present. It should be noted, however, that in most cases it is not the actual proof of identity, i.e. comparing a government-issued identity document with the person to whom it belongs, that has changed, but rather the process by which this takes place and the technology used in this process.

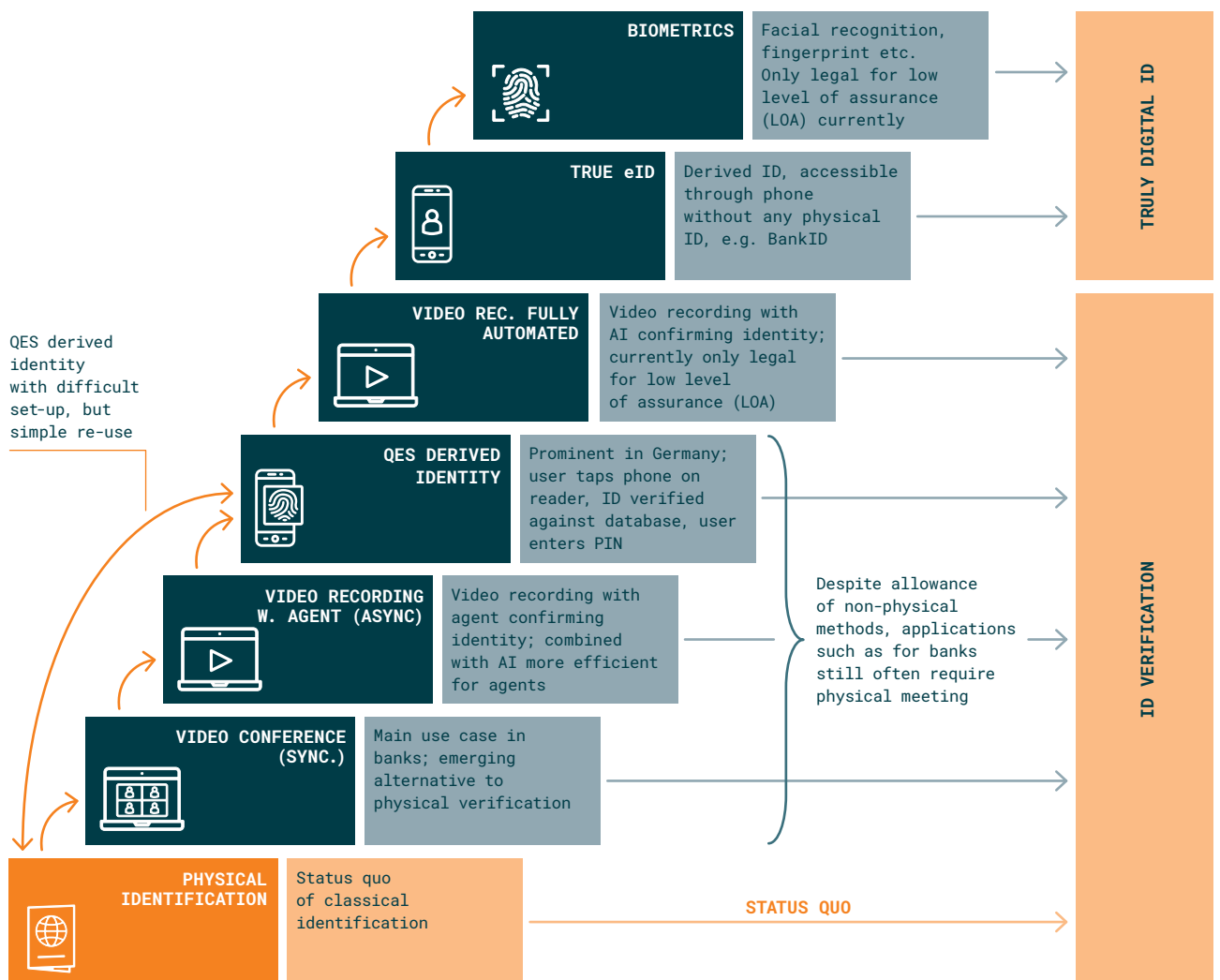
TECHNOLOGICAL DEVELOPMENTS

Video identification, for example, is a method through which a video connection between the user and an ident provider is established and an agent engages with the user in real time to capture evidence of the ID document and the user's face.

In Germany, it was introduced in 2014 when the German Federal Financial Supervisory Authority BaFin officially approved this method as compliant with the Anti-Money Laundering Act (GWG). Other EU countries like Spain followed, where video identification was introduced in 2016. Since then, video identification has been steadily improved, for example by separating out the user process and the review process by the agent.

Fig. 4 – Evolution stages of different identification options.

In asynchronous video identification, a user records a video that is later reviewed and validated by the agent. This can avoid bad user experience (e.g. waiting in long queues) and reduce validation time for agents and therefore costs for financial institutions. However, one can only fully benefit from these advantages if the error rate, and the risk associated with it, can be kept at a minimum. See also the chart in Fig. 4 for the main evolution stages of electronic identifications.



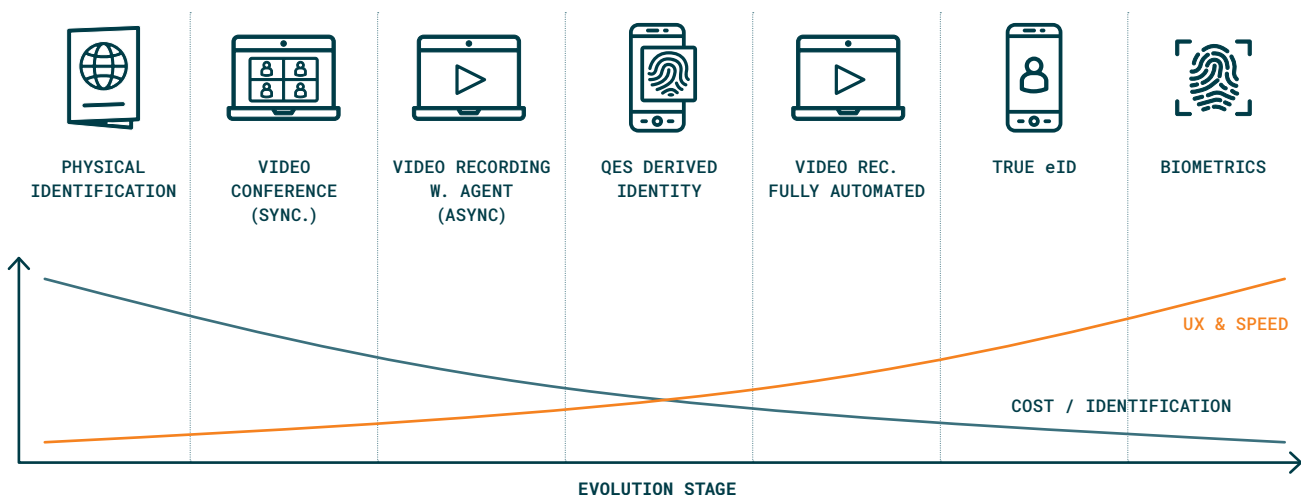
Other technological advances led to new solutions that are fully automated without any human being physically involved. In these AI/ Auto-ident solutions, artificial intelligence and machine learning technology are used to check ID documents for authenticity and conduct all relevant security checks. By comparing the user's biometrics from a self-recorded selfie or video with the photo on the ID document, it is ensured that the ID belongs to the user executing the identification process.

Incorporating functionalities in smartphones like Near Field Communication (NFC) has allowed providers to also create solutions that use the smartphone as a card reader and read out the information from electronic identity card chips (e.g. nPa in Germany).

DEVELOPMENT TRENDS IN THE EU

"Truly digital" IDs are even more convenient for users. Examples of truly digital IDs are eIDs in northern Europe, Estonia and Benelux. Here, an identification is often derived from a mobile phone without any physical ID. Compared to other methods, digital IDs allow the consumer to use them not only for the initial onboarding process but also for authentication on a regular basis (e.g. for online banking logins), which represents a significant increase in convenience from a consumer perspective.

Fig. 5 – Different identification options compared by UX, speed and costs.



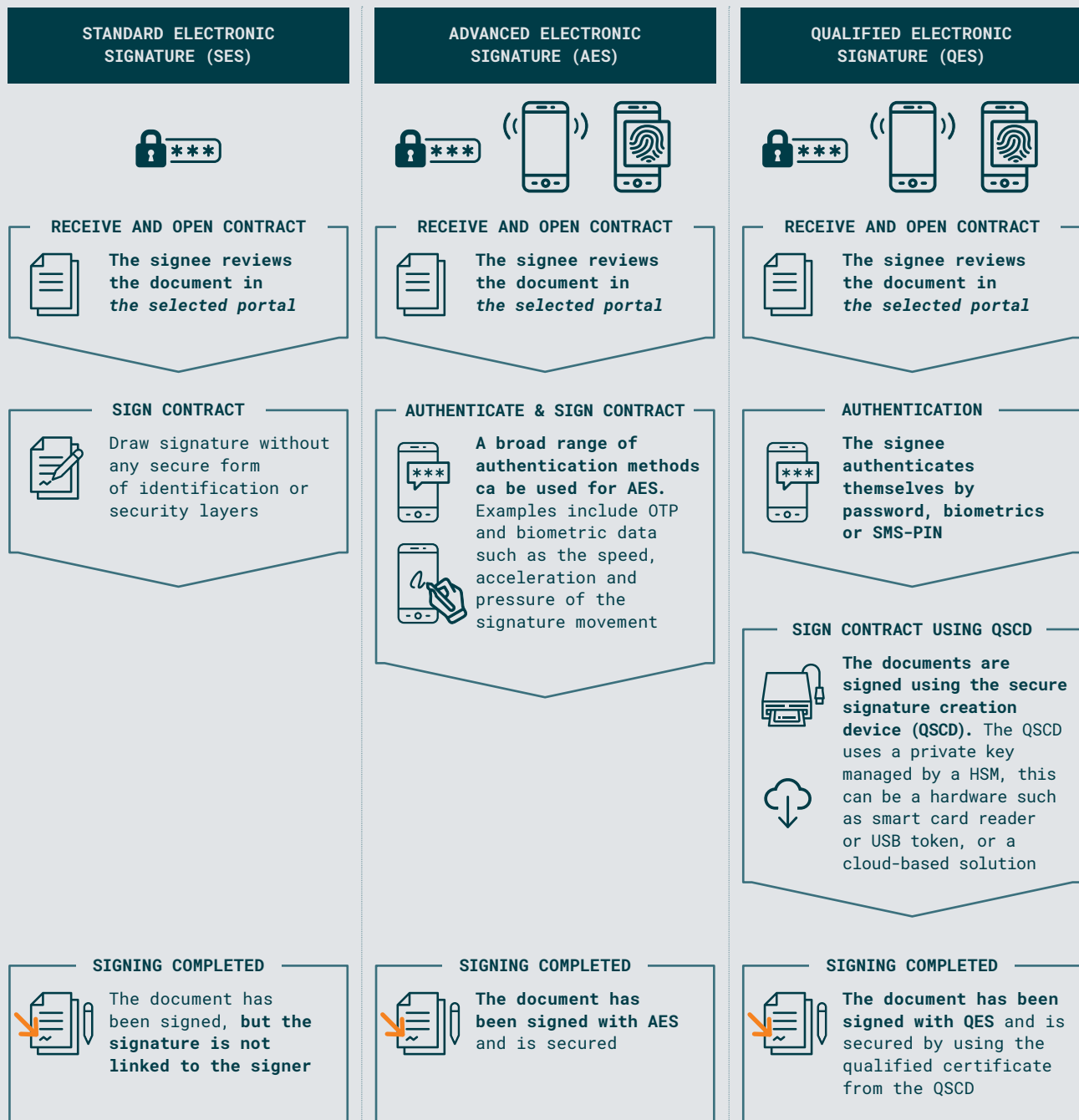
QUALIFIED ELECTRONIC SIGNATURE (QES)

Because of different regulations and market environments, not all of these methods are available in every country in the EU. Nevertheless, in more and more countries, one can see a trend towards truly digital IDs, even though they are still at different stages in this process (see also [Chapter 5](#)).

Digital signatures play a special role for (online) identifications. Qualified electronic signature (QES) is perceived as the most complete and secure method to verify identity (which is also accepted in Europe under eIDAS and national AML laws). Key advantages include time and cost efficiency, and the highest level of security even compared to classical handwritten signatures. Under eIDAS regulations, a QES has the same legal effect as a handwritten signature. QES requires a qualified certificate, which must be issued by a qualified trust service provider, listed under eIDAS approved services. This certificate links the identity of the signee to the signature. To create the signature itself, a hardware device (qualified signature creation device) is mandatory – this may be a mobile phone or an online software solution (e.g. eSign from IDnow).

See [Fig. 6](#) on the following page for different types of electronic signatures.

Fig. 6 – Types of electronic signature.



4. REGULATORY FRAMEWORK

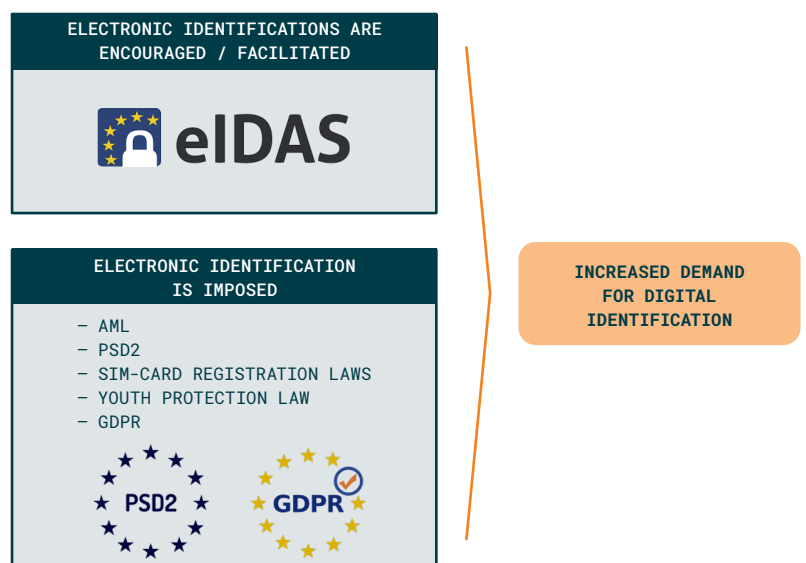
4.1. REGULATORY LANDSCAPE

To understand the European market for electronic identification and developments in individual countries, it is useful to begin with a look at the overarching regulatory landscape in Europe.

For the purposes of this white paper, we will distinguish between imposing laws and facilitating laws:

- **Imposing legislation** are rules and regulations that make identification mandatory for specific use cases – such as the Anti-Money Laundering Directive, Payment Service Directive 2, Youth Protection Act and Telecommunications Act – or impose requirements on it like the General Data Protection Regulation.
- **Facilitating legislation** facilitates electronic identification within Europe, for example by making it applicable across countries. Here, eIDAS is the most noteworthy example. In the following section, we will take a look at both types of regulation.

Fig. 7 – Two types of legislation: imposing and facilitating.

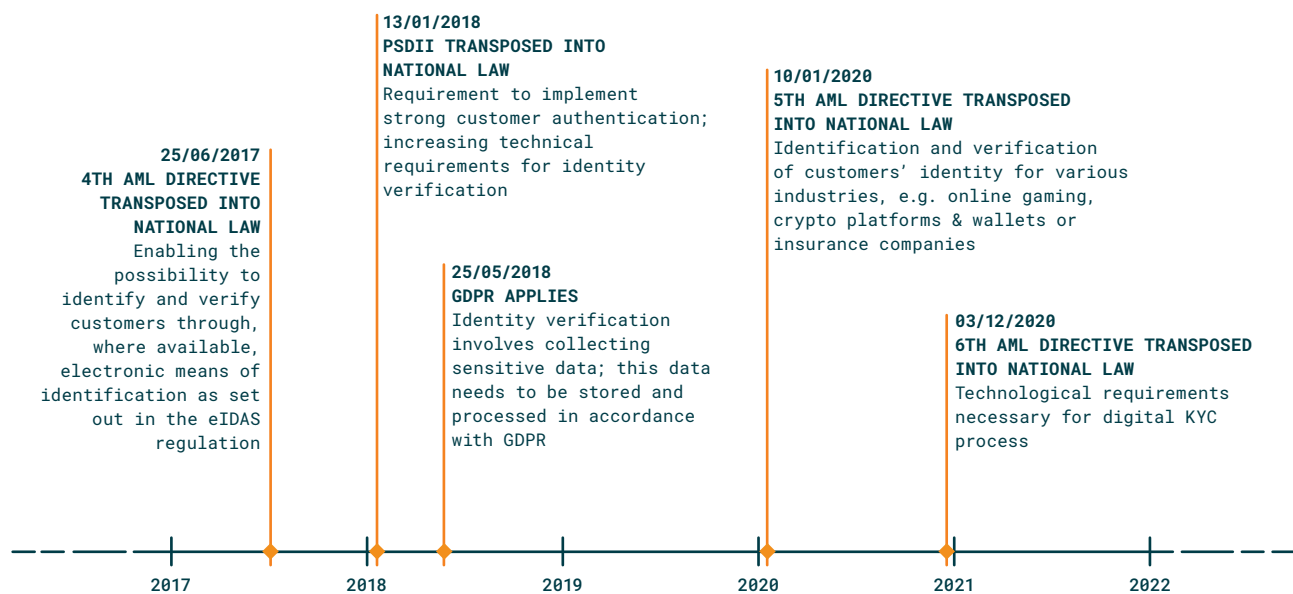


ANTI-MONEY LAUNDERING (AML)

Regulations that Impose Requirements

One regulation that has a strong influence over the electronic identification landscape in Europe is the Anti-Money Laundering (AML) directive. The objective of AML is to prevent money laundering and the financing of terrorism. Therefore, institutions that fall under AML (e.g. financial institutions) are obliged, among other things, to conduct special Know-Your-Customer (KYC) procedures, including verifying the customer’s identity, during onboarding.

Fig. 8 – Legislation imposing requirements for identification (extract).



Since June 2021, the sixth AML directive has been in force. The directives are issued by the EU to provide a general framework as a minimum standard for Member States, which their governments are responsible for transposing into national law. National authorities like the BaFin in Germany or Sepblac in Spain often support the national government and are responsible for interpreting the law and supervising its implementation. In case of the KYC process, this means that while the EU’s directives state that a KYC process has to take place, the exact requirements for this process and, by extension, the authorised identification procedures, are defined by each Member State.

PSD2

The Payment Services Directive 2 (PSD2) also plays an important role within digital identities. Key objectives of PSD2 are to protect consumers and to make payments more secure while increasing innovation and competition in the payments market, not only amongst banks. For example, banks and other payment providers must implement strong customer authentication, a mechanism designed to increase technical requirements for identity verification.

SIM-CARD
REGISTRATION
LAWS

Besides AML and PSD2, other regulations also make identification necessary for specific use cases. In 2020, the European Commission asked Member States to take a position on a common European approach to banning anonymous SIM cards. Although this has not been implemented, it can be observed that many European countries such as Spain, Italy, France and Germany have taken this as an opportunity to introduce national laws (e.g. the Telekommunikationsgesetz in Germany) requiring their citizens to identify themselves when activating SIM cards in order to combat terrorism.

YOUTH
PROTECTION
LAW

Local youth protection laws also play a role in European countries when it comes to identification. Although they often do not require users to identify themselves, they often recommend it or at least require some form of age verification. Typical examples of use cases for this can be found in the gambling industry, eSports or age-restricted products or services.

GDPR

A framework that does not require identification per se but does impose requirements on electronic identification providers and methods is the General Data Protection Regulation (GDPR). Identity verification always involves collecting sensitive personal data, including videos, scans, pictures and biometrics, which need to be stored and processed in accordance with GDPR.

AN INSTITUTION, WHETHER PRIVATE OR PUBLIC, THAT PROCESSES OR EXCHANGES PERSONAL DATA, OR DOES ANYTHING RELATING TO IT, MUST USE ALL POSSIBLE TECHNOLOGY MECHANISMS TO ENSURE THE DATA IS PROTECTED.

AET EUROPE

EIDAS

One of the main challenges here is that GDPR objectives often contradict other regulations: while supervisory authorities often demand the collection of more and more data, GDPR stipulates that only data that is necessary may be collected and stored.

Regulations that Facilitate Identification

The second type of regulation that this paper covers are directives and guidelines that facilitate electronic identification across the EU.

The most important framework is the electronic Identification, Authentication and Trust Services regulation, or eIDAS, which has been fully in force since 2018. The aim of eIDAS is to strengthen trust in electronic transactions between companies, citizens and authorities by creating a common legal framework for cross-border recognition of national electronic identification schemes and standard rules for trust services across the EU.

For this reason, according to eIDAS, each EU member state can register eID schemes, which other EU members have to accept at a given level of assurance. From the private sector, different Qualified Trust Service Providers (QTSP) are cooperating with national authorities to offer these solutions. Here, eIDAS distinguishes between three different levels of confidence that can be put on a person's claimed identity when identifying themselves electronically: low, substantial and high. Furthermore, eIDAS regulates the use of trust services, in particular electronic signatures. It introduces three different types of electronic signatures – simple, advanced and qualified – and enables their use across the EU, with Qualified Electronic Signatures (QES) having the same legal effect as handwritten signatures in every country.

eIDAS thus provides an interoperability framework to ensure that national methods are recognised for use in the public and private sectors (currently on a voluntary basis) across the EU.

Even though all the regulations presented have an impact on the use of electronic identification in Europe, when regulations are addressed below, it is usually in the context of eIDAS and AML, as these two frameworks have a more direct impact on the use of electronic identification across several countries in the EU.

EIDAS 2.0 AND DIGITAL WALLETS

In June 2021, the EU Commission presented a draft for eIDAS 2.0. The aim is to create a European standard for identity wallets, although it is explicitly not about a central technical European wallet solution. All official documents (e.g. driving licences, ID cards) should be able to be stored in this wallet. Within 12 months, all member states must provide their citizens with a wallet and accept eligible wallets as a valid identification method. For the technical implementation, cooperation with the Qualified Trust Service Providers would be an option, with whom the eID schemes are already being successfully implemented under eIDAS 1.0. Based on the eIDAS 2.0 draft, national authorities must maintain a list of personal attributes (including age, gender, financial data, educational and employment history), which can be shared with a wallet solution at the user's request. The further digitalisation of administrative procedures and the possibility of digitally managing any type of official document could enable a further step towards mass acceptance of digital identification. For the current status of these wallet solutions, see also [Fig. 11](#).

Fig. 9 – Application areas of eIDAS and incorporating wallets as part of eIDAS 2.0.

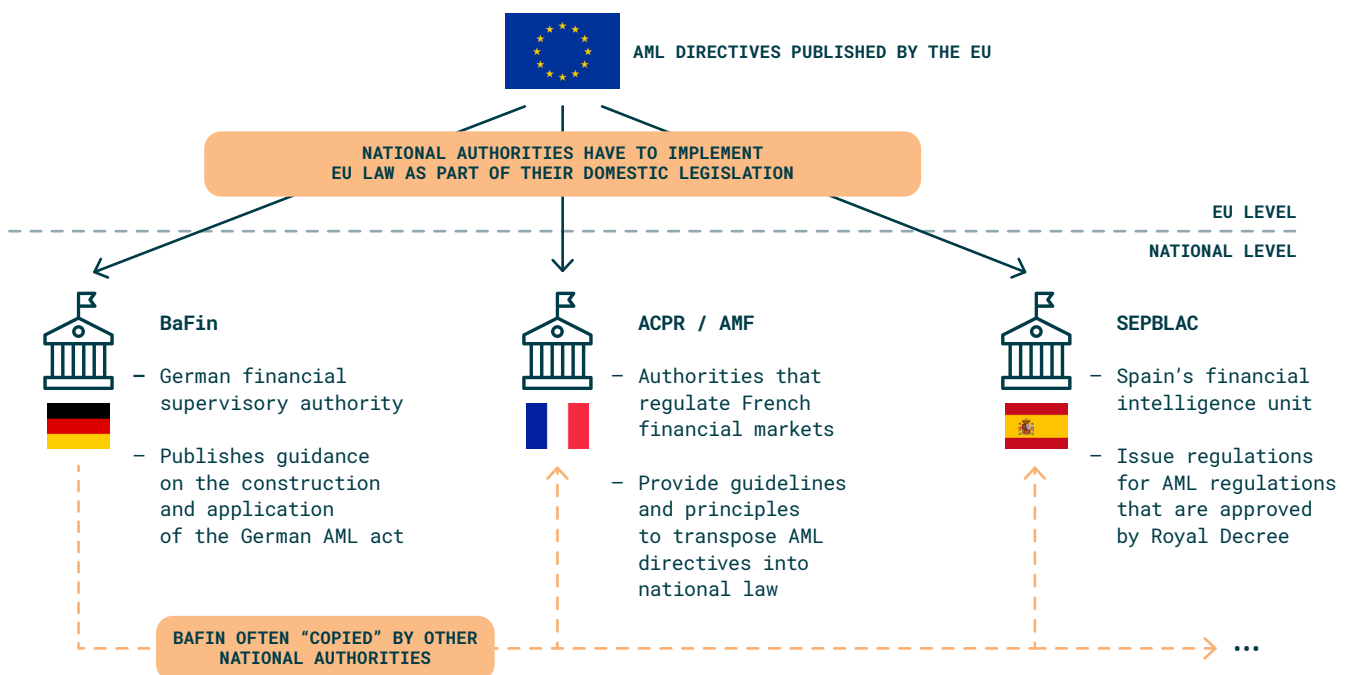


4.2. REGULATORY CHALLENGES

All in all, the regulatory environment in Europe is challenging. This is mainly due to the fact that the existing legal framework is open to interpretation, resulting in very different ways of implementing at the national level and a very fragmented ID solution landscape in Europe. This is also the reason why no real standard European solution that can be used across all EU member states has yet evolved.

In 2020, with AML directive 5 (AMLD5) coming into force, at least the contradiction between AML and eIDAS has been resolved, as AMLD4 deemed electronic identification riskier and required enhanced due diligence measures compared to physical identifications, while eIDAS encouraged electronic identification. Nevertheless, it is not yet possible to say that the regulatory landscape really promotes a standard electronic identification procedure across Europe. Different implementations on a national level, for example, mean that electronic identification procedures permitted in one country are not guaranteed to work in another. And even if the same procedures are allowed, there may be different requirements for the procedures themselves.

Fig. 10 – Regulatory challenge: EU law is interpreted differently on a national level.



A good example of this is video identification. While in Germany, for instance, there are precise technical requirements for conducting video identification, other countries are less strict (e.g. Spain, where no live interaction with an agent is needed) or do not explicitly regulate the requirements for the use of video identification at all (e.g. France).

Furthermore, although technical interoperability of national eID solutions is supported by the eIDAS framework, this only applies to eID schemes notified to the European Commission. There are no requirements for member states to develop national digital IDs or to make them interoperable with other states. This has led to large discrepancies between individual states in the EU. In addition, it seems that private-sector solutions, in particular, haven't really been able to take advantage of the framework so far. Although notifying private eID schemes is possible in principle, it seems that in practice the strict notification requirements tend to discourage this.

All in all, until now citizen adoption of the notified eID schemes is too low, their usage often too cumbersome and use cases rather limited.

4.3. REGULATORY OUTLOOK

One initiative to meet these challenges was announced by the President of the European Commission Ursula von der Leyen in her state of the Union address in September 2020, in which she proposed a European Digital Identity. In June 2021, further details of the plans were announced, including the introduction of a European digital identity wallet. Through this wallet, EU citizens should be able to use their national digital identities to access public, private and cross-border digital services in the EU. The solution is to be made available to all EU citizens and businesses on a voluntary basis. In this way, the EU Commission wants to become less dependent on private players and platforms, which are increasingly shaping the identity market. In this context, the commission particularly emphasises that it wants to enable EU citizens to access online services without unnecessarily sharing personal data with private providers. The initiative is built on the existing eIDAS regulation and is intended to address the limitations that were mentioned in the previous chapter of this whitepaper.

These limitations have led to discrepancies in the development of digital identities between countries, which have now become even more visible through the Covid-19 pandemic.

THE COMMISSION WILL SOON PROPOSE A SECURE EUROPEAN E-IDENTITY. ONE THAT WE TRUST AND THAT ANY CITIZEN CAN USE ANYWHERE IN EUROPE TO DO ANYTHING FROM PAYING YOUR TAXES TO RENTING A BICYCLE. A TECHNOLOGY WHERE WE CAN CONTROL OURSELVES WHAT DATA AND HOW DATA IS USED.

URSULA VON DER LEYEN,
PRESIDENT OF THE EUROPEAN COMMISSION
(SEPTEMBER 2020)

In February 2022, the EU started a tendering process with the goal of implementing the wallet solution presented above. The tendering process will run until August 2022, followed by the development of prototypes which should be the backbone of a European-wide eID ecosystem. See the chart in [Fig. 11](#) for an overview of the main objectives.

Fig. 11 – Components of recently published EU tender offer.

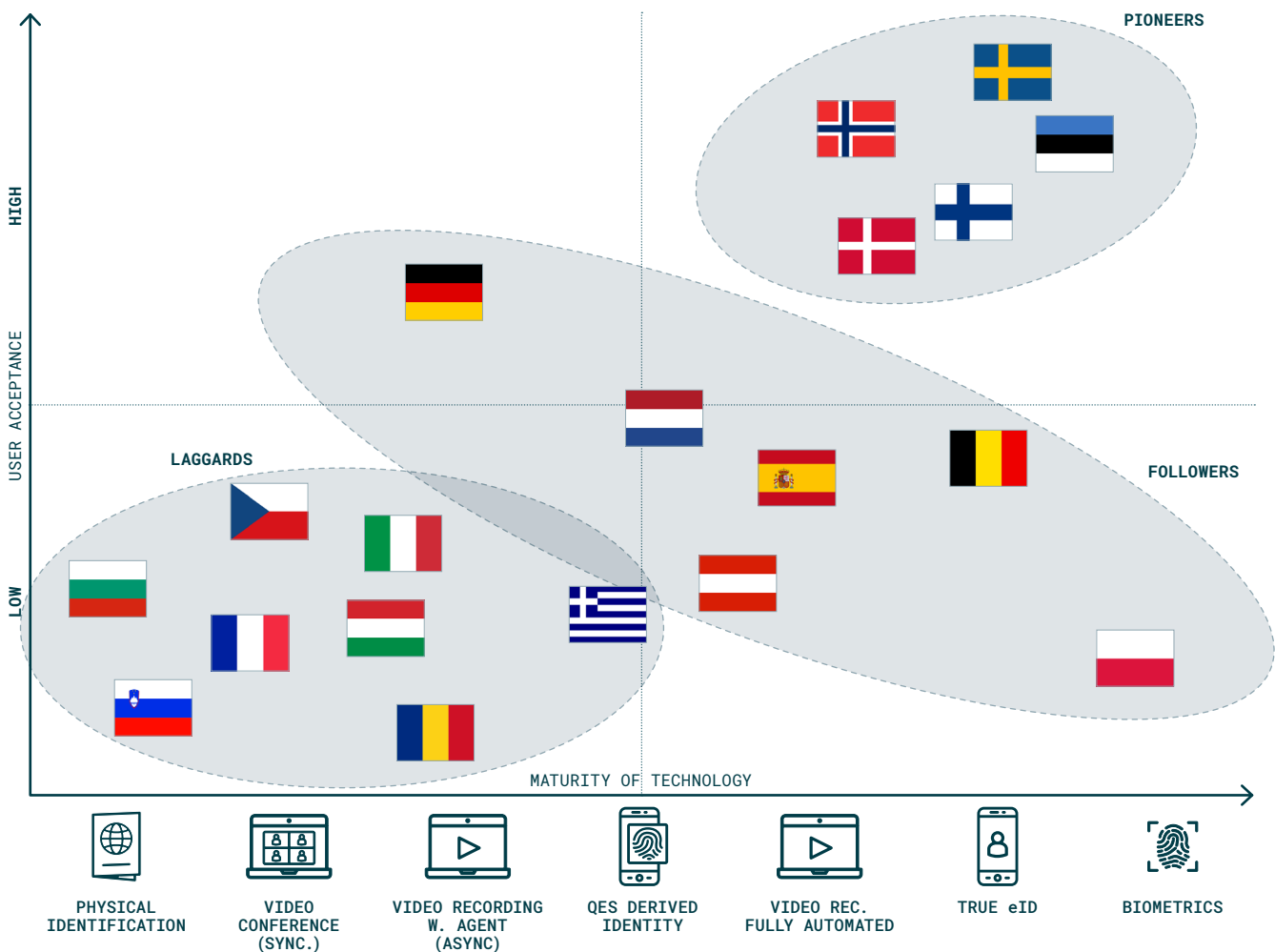


5. MARKET OVERVIEW

5.1. SELECTED COUNTRY CLUSTERS

Changes are happening not only in the regulatory sphere, but the market environment in Europe is also very dynamic and rapidly evolving. To get a comprehensive understanding of the European landscape, we will take a look at different markets in this chapter. For this purpose, we have analysed selected European countries by maturity of the predominant identification method and market adoption and derived three clusters: “pioneers”, “followers” and “laggards”.

Fig. 12 – Market segments based on level of user acceptance and maturity of technology.



PIONEERS

The first cluster, which we refer to as “pioneers”, includes countries like Norway, Finland, Sweden, Denmark and Estonia. Characteristic for these countries is the widespread use of eIDs, for example MitID in Denmark and bankID in Norway. The acceptance and adoption of eIDs in the population in all countries of this first cluster is very high, as they are regularly used for all types of services that require identification, especially in the financial and public service area.

So far, Denmark, Estonia and Sweden have eIDs with a “notified” status, while Norway’s solution has been “peer-reviewed”. Solutions by the private sector, mostly banks, are predominant in these countries, while government-provided solutions are virtually non-existent.

All in all, it seems that since most countries in this group already have their own sufficient solution, their need for a unified solution, based on eIDAS, might be of minor relevance.

FOLLOWERS

The countries in the second cluster, which we call “followers”, include Germany, the Netherlands, Spain and Austria. This group is characterised by the fact that neither user acceptance nor adoption of eIDs amongst the population is as high as the pioneers countries, nor are the methods used for identification as sophisticated. Typical methods include synchronous and asynchronous video identification, and methods that involve biometrics or bank identification processes.

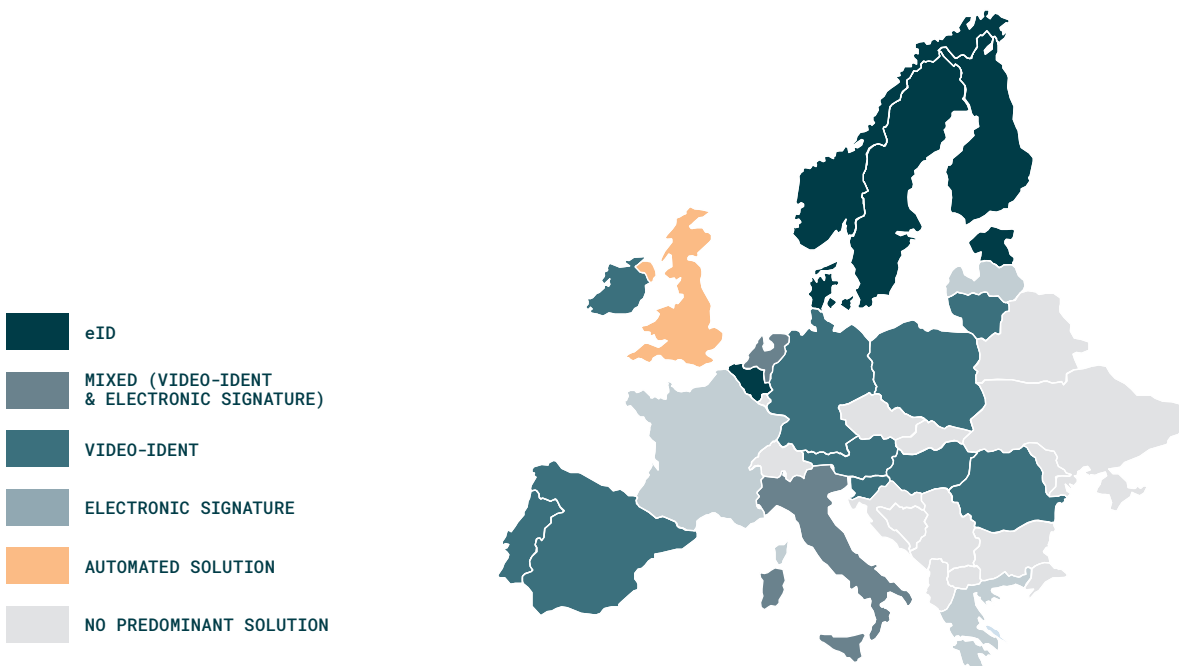
National eID schemes have mostly been notified to eIDAS. Most of these countries have a public-sector electronic identification solution (e.g. digital identity cards), which have primarily been used for public services until now. In contrast to the pioneers, in these countries the private providers often lack the critical mass to become the dominant solution, for example Verimi or Yes in Germany, or QuickSign in Spain. Accordingly, the potential customer reach is smaller than in the pioneer countries, and the development towards predominance of a state-owned or private solution is uncertain. At the end of this chapter, the German online digital ID will be described in detail as a good example for the status of “follower” countries.

LAGGARDS

Members of the “laggards” cluster include countries such as Bulgaria, Slovenia, the Czech Republic and France. The characteristics of this group are missing digital identification methods – physical on-site identifications or less user-friendly identification methods such as printouts of contracts in combination with a bank transfer are predominant – alongside generally low user acceptance and adoption. In addition, there is a lack of legal clarity surrounding national AML law – for example in France, where national AML does not explicitly regulate identification methods, which can lead to no method becoming predominant. Legally unclear settings tend to suggest restrained markets where it cannot yet fully be assessed whether a state or private solution will prevail in these countries. The proportion of these countries that have already notified eIDAS of an eID scheme is also low due to several factors such as limited political ambitions, lower market pull factors than in other countries, and simply no transposition of EU law into national AML law.

Fig. 13 – Dominant digital identification method per country.

The graphic in Fig. 13 also summarises the geographical distribution of the predominant identification method for each country, highlighting especially the pioneering role of northern Europe.



EXAMPLE: GERMAN ONLINE DIGITAL ID

The German electronic ID card is emblematic of the “follower” cluster. New legislation for electronic identifications on mobile devices came into force on 21 September 2021 (Smart eID Act), enabling the new digital ID. Even before that solution, semi-digital solutions for on-line public services were on the market but with little adoption among citizens. From a technological perspective, this solution offers an identification without a third party but is not as convenient or technologically advanced as a true eID.

Fig. 14 – Setup and requirements of the online digital ID solution.

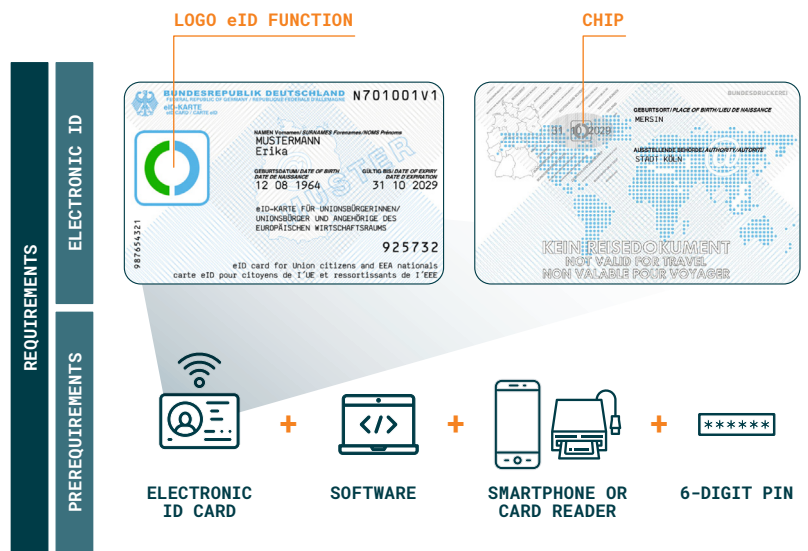


Fig. 15 – Process of identification for online (public) services.

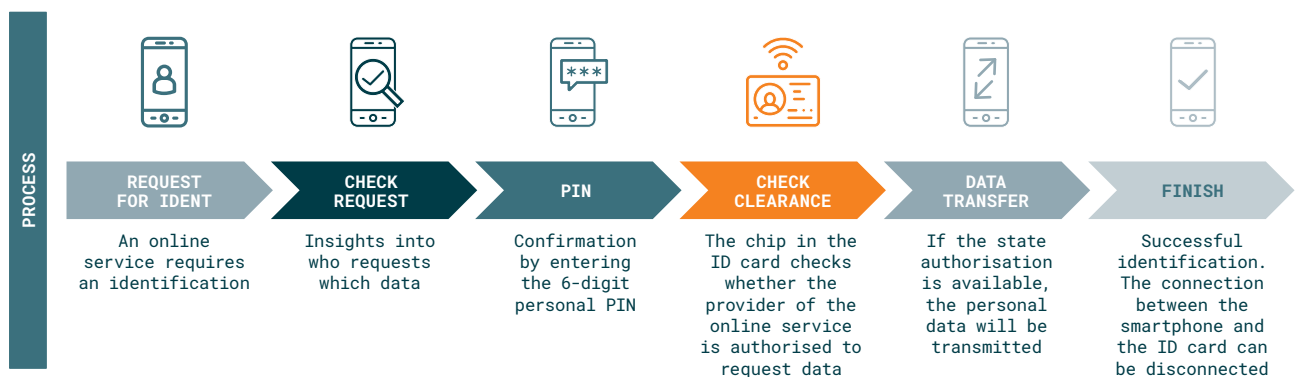
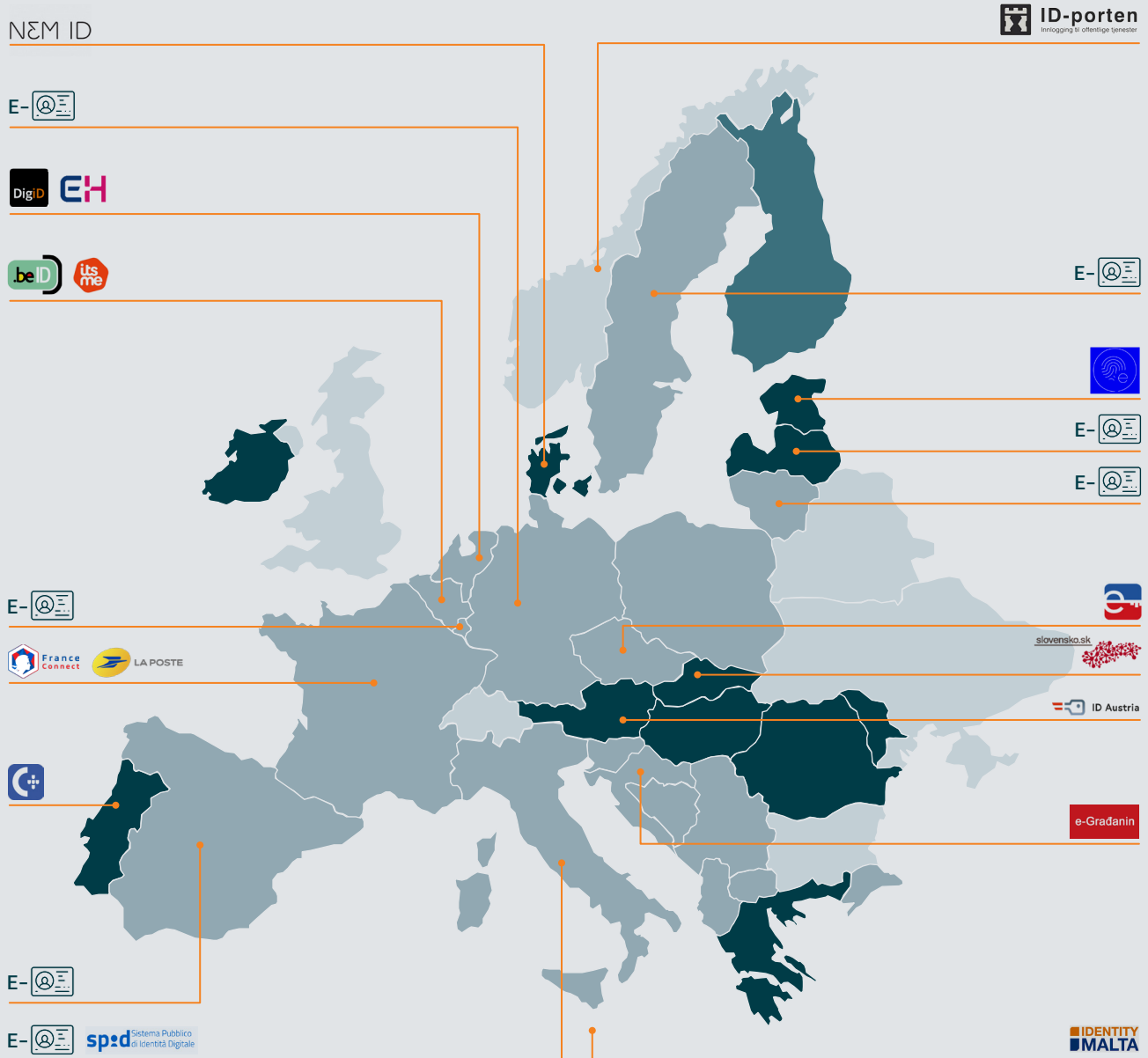
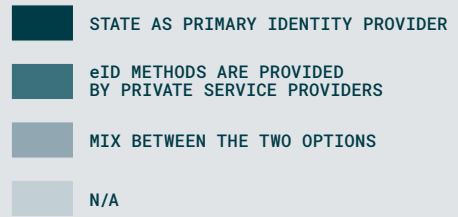


Fig. 16 – Overview of notified eID schemes under eIDAS⁵ and role of the state.



SELECTED NON-NOTIFIED SOLUTIONS

PRIVATE SOLUTIONS:



PUBLIC SOLUTIONS:



MIXED SOLUTIONS:



⁵ Including pre-notified and peer reviewed schemes.

NOTIFIED SCHEMES UNDER EIDAS

To complete the market picture, it is necessary to look at the role of the state in connection with eIDAS-notified schemes. So far, the technological component and acceptance have been considered, but the individual EU states enjoy different degrees of support from their respective governments. There are countries where the state is the primary identity provider (e.g. in Eastern Europe), whereas in Northern Europe the state plays more of a moderating role between the private sector and public-sector solutions. Nevertheless, almost all states have at least one solution that falls under the eIDAS regulation.

5.2. CURRENT DEVELOPMENTS AND TRENDS

Despite varying degrees of maturity across the clusters, some trends and developments can be observed in the European market. Several of these will be looked at in more detail in the following section, including:

- Consolidation across borders and within countries
- Expansion of national solutions to other member state markets
- Innovation in identification methods and rising governmental solutions as a counterpart to the private sector.

CONSOLIDATION

Consolidation between market players is occasionally of enough general interest to gain the attention of mainstream news outlets. For an overview of selected acquisitions in the European electronic identification space since 2019, see the table on the next page ([Fig. 17](#)).

In June 2021, for example, the German identity verification provider IDnow's acquisition of the French player ARIADNEXT was announced. Just a few months before, in March, IDnow announced its takeover of another Germany player, identity Trust Management (identityTM). Through these acquisitions, IDNow wants to offer a comprehensive portfolio of identity verification services for several European markets like Germany, the UK and France, and offer solutions that can be used across several countries and different use cases. To provide additional capacity to meet the rapidly growing demand for identification verification services, IDnow bought the call centre subsidiary Wirecard Communication Services ID in September 2020.

Fig. 17 – Overview of selected acquisitions in the European digital space since 2019.

YEAR	TARGET	COUNTRY	BIDDER	COUNTRY
2022	UBBLE.AI		CHECKOUT.COM	
2022	SPHONIC		SIGNICAT AS	
2022	SECUREKEY TECHNOLOGIES		AVAST	
2022	<i>Looking for targets</i>	–	WEBID	
2021	4STOP		JUMIO	
2021	ELECTRONIC IDENTIFICATION SL		SIGNICAT AS	
2021	DOKOBIT		SIGNICAT AS	
2021	EYN		ONFIDO LTD.	
2021	ARIADNEXT		IDNOW GMBH up for sale due to possible PE exit options	
2021	ENCAP AS		SIGNICAT AS	
2021	IDENTITY TRUST MANAGEMENT AG		IDNOW GMBH	
2021	HELLO SODA LTD.		ACUANT INC.	
2021	IVNOSYS SOLUCIONES, S.L.		SIGNATURIT SOLUTIONS, S.L.	
2021	PIXELPIN LIMITED		T STAMP INC.	
2020	I-HUB S.A.		BGL BNP PARIBAS	
2020	WIRECARD COMMUNICATION SERVICES		IDNOW GMBH	
2020	SCRIVE AB		VITRUVIAN PARTNERS LLP	
2020	ONFIDO LIMITED		TPG CAPITAL LP	
2020	INTERNATIONAL SMART CARD FACTORY COMPANY (PCARD)		IDEMIA	
2020	CONNECTED INFORMATION SYSTEMS B.V. (CONNECTIS)		SIDN SIGNICAT AS 2050 FOUNDATION	
2020	AIMBRAIN SOLUTIONS LTD.		BIOCATCH LTD.	
2019	ONEGINI		INNOVATIONQUARTER WALVIS PARTICIPATIES B.V. THE HATCH FIRM	
2019	EVOLIUM TECHNOLOGIES, S.L.U.		KEYFACTOR, INC.	
2019	IDFY NORGE AS		SIGNICAT AS	
2019	SIGNICAT AS		NORDIC CAPITAL	

EXPANSION

Similar developments can be observed in other markets. Another good example of this is the Nordic company Signicat, which is constantly acquiring other companies to establish itself in more and more markets and to further build its digital identity platform. In 2021 Signicat acquired the Spanish digital identity player Electronic Identification. The year before, in 2020, the Dutch company Connectis was acquired, as well as the two Norwegian companies Idfy (2019) and Encap Security (2021). WebID is another good example of a player that is currently looking for targets. **Fig. 17** shows an extract of acquisitions within the past three years.

It is not only through acquisitions that providers try to gain a foothold in other European markets, but also by expanding into these markets with solutions adapted to local requirements or that even become a standard throughout Europe.

International players are expanding into more and more European countries. Examples include:

- US player Jumio, which announced its launch of a French solution portfolio in July 2020 and appointed its first sales leader in the region and has European offices in Austria and London
- UK player Onfido, known for its strong go-to-market model using a partner ecosystem, has offices in the UK, France, Portugal and Germany

Other players, instead of adapting to national requirements, try to conquer Europe with a standard solution. For example, both ZealID from Sweden and the Spanish provider Electronic Identification (acquired by Signicat in 2021) offer procedures based on Qualified Electronic Signature (QES), which can supposedly be used in every country across the EU for AML use cases like opening a bank account.

In doing so, they take advantage of the eIDAS requirement that a QES must be accepted in all EU countries. To issue the signature, a video identification solution is used that does not require an agent to be present during the session.

The user simply needs to record a video of themselves and their ID, which is sent to the back office for asynchronous validation by a certified agent.

Using QES as a standard identification solution across the EU could have two notable advantages: firstly, international customers can use the solution and cover different markets in Europe with only one provider. Secondly, the procedure could be offered and used as an improved method in countries where so far only more complicated or more expensive procedures are allowed. An example of this is a country like Germany, where video identification currently requires live interaction with an agent. However, for QES-based identification, this requirement does not necessarily apply.

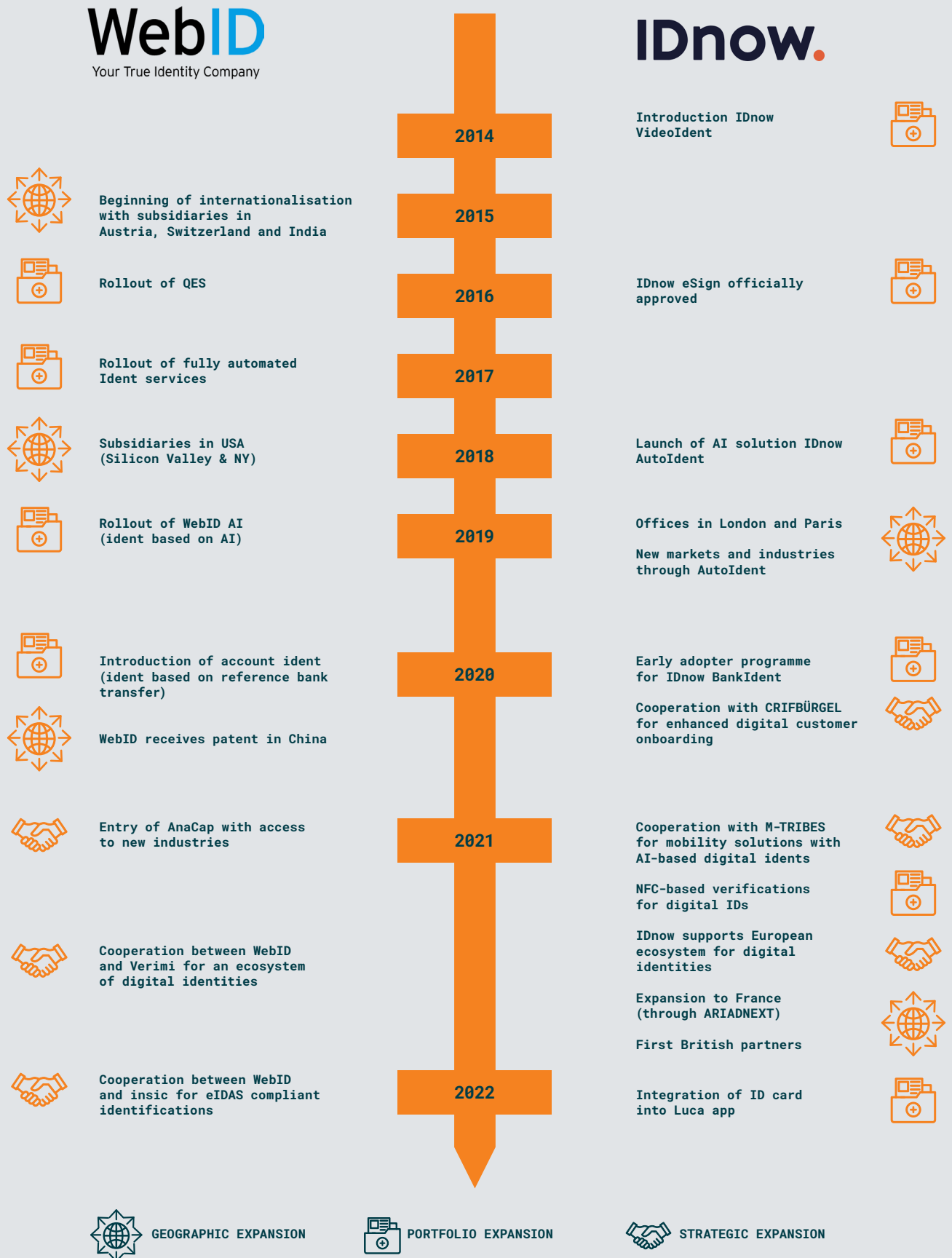
The chart in **Fig. 18** shows the dynamic of how different players (here: IDnow and WebID) are expanding their business and their product portfolios abroad.

INNOVATION

The identification market in Europe is also characterised by constantly new innovations. Identification procedures continue to develop, with new players entering the market either with more customer-friendly processes or new technological approaches. Also, existing players use innovative solutions to further strengthen their position. For example, the Spanish player Veridas (founded in 2017 as a joint venture between BBVA and das-Nano) employs AI algorithms to use face and voice biometrics for identification. The expected advantages are increased security and fraud prevention. The biometrics approach is also followed by many other players, including technology giants such as Google, Microsoft and IBM. A preliminary stage to biometric IDs was already launched by HSBC as “VoiceID” in 2016, for example, to reduce fraud in telephone banking.

Blockchain technology is also being used more and more frequently in innovative solutions. A consortium of banks in Spain, including Santander, LiberBank and others, are working on a self-managed digital identity that will enable customers to save their personal data in a single digital identity on their mobile device and to decide with whom they want to share them for relevant processes (e.g. renting a car quickly and easily or signing up for an insurance policy).




Fig. 18 – Overview of expansion activities using the examples of IDnow and WebID.



The solution is based on the blockchain structure of Ethereum and Quorum and was rolled out as a pilot in May 2021.

In addition, innovation is explicitly promoted on a European level, for example by the European Innovation Council, in the form of funding, networks and support. European cross-border solutions are to be given precedence over national-only approaches.

Fig. 19 – Examples of European innovations: IDnext Innovation Awards 2022.

ASIGNIO 	PureID 	EHerkenning 
<ul style="list-style-type: none"> - MULTI-FACTOR AUTHENTICATION – SYNCHRONOUS DUAL BIOMETRICS - PATENTED SIGNATURE RECOGNITION TECHNOLOGY - MORE SECURE WITH TWO BIOMETRICS AT ONCE, SIGN-IN & LIVE SELFIE OR VOICE & LIVE SELFIE 	<ul style="list-style-type: none"> - AWARD WINNING SOFTWARE PRODUCT FOR NFC-BASED IDENTITY VERIFICATION - CONVENIENT, SECURE, SCALABLE SOLUTION 	<ul style="list-style-type: none"> - ERECOGNITIONIS A DUTCH E-IDENTITY TRUST FRAMEWORK - ENABLES COMPANIES TO RE-USE DIGITAL IDENTITIES TO AUTHENTICATE THEMSELVES WITH GOVERNMENT ORGANISATIONS

GOVERNMENT SOLUTIONS

Governments, too, are increasingly developing solutions to avoid relying on private providers. A few examples are listed in the following section, which takes a deeper look at Greece, Germany, Estonia, the Netherlands, France and Denmark. Whether a common European solution is likely to emerge from national solutions will be outlined in the next chapter.

USE CASE: GREECE

In May 2021, for example, the Greek Ministry of Digital Governance launched a new KYC platform. Through the platform, Greek citizens who have a tax ID number or Taxisnet credentials can avoid the need to collect all their documents and submit them physically at a local bank branch. Once they give their consent on the platform, financial institutions can access the necessary data to verify the customer's identity and obtain contact details, information on professional activity and annual income.

USE CASE: GERMANY

In Germany, too, there are projects to promote digital identities. For example, the Federal Ministry of Economics and Technology aims to move identity cards, driving licences and other documents that authorities require to citizens' smartphones. This, in turn, is intended to ensure that, without an interest in commercial use of the data, a possibility is offered to identify oneself via a smartphone with an eID. Another project of the German government is the so-called Bürger ID (Citizen ID). The tax identification number, which is assigned to every citizen at birth, will no longer be used only by the tax office but will also be used by citizens when interacting with authorities and administrations digitally.

USE CASE: ESTONIA

Estonia is an example of a country that introduced a government solution for digital identification early on. Estonia has been offering the possibility to use private and public services with a digital ID only for more than 20 years. The Estonian digital ID is issued at birth and valid for life. Estonia has even gone so far as to issue e-residency, whereby non-Estonians can apply for e-residency and get access to the Estonian digital business environment via a digital ID. They can even be used for starting and running a business in Estonia entirely online.

USE CASE: THE NETHERLANDS

In the second half of 2021, the Dutch government announced the introduction of digital identity infrastructure. The aim is for Dutch citizens to only need one digital identity and to allow them to choose market solutions of their choice. This concept was presented by Raymond Knips, the State Secretary for the Interior and Kingdom Relations. Interoperability with eIDAS should be guaranteed, alongside easier access to Europe-wide KYC and AML checks. Although this is not a government solution in the narrower sense, it shows that national initiatives are also being set up to strengthen the use of eIDs. However, there is still no binding timetable for concrete implementation.

USE CASE: FRANCE

France is also working on a national digital ID solution (CNIE) for its citizens (Programme interministériel France Identité Numérique) in order to combine the physical ID with a digital one and enable easier use of online services. The government is working with Idemia, and digital identity is smartphone-based. To confirm their identity for

USE CASE: LIECHTENSTEIN

online services, the digital (physical) ID card is held to the back of a phone to establish an NFC connection. The associated app then authenticates the data stored on the chip. Valérie Peneau, director of the Programme interministériel France Identité Numérique highlights the benefit of this solution: “Our mission is to create and offer easy-to-use electronic identification tools that enable secure online transfer of citizens’ personal data so that transactions cannot be centralised or traced”.

In 2020, Liechtenstein introduced the digital identity eID.li. About one-third of Lichtensteiners currently use the eID for digital public services, which was developed by a subsidiary of the Austrian State Printing Office, among others. The core component is the MIA Platform, which covers various areas of application of the digital ID via an app: digital ID cards, digital health certificates or integration into the green passport (Covid-19 certificate), which will be implemented this year. What is new about this platform is that it is the world's first system for integrated identity management and is protected by blockchain key technology.

The next chapter examines whether national solutions will be dominant in the future or whether a European solution could prevail.

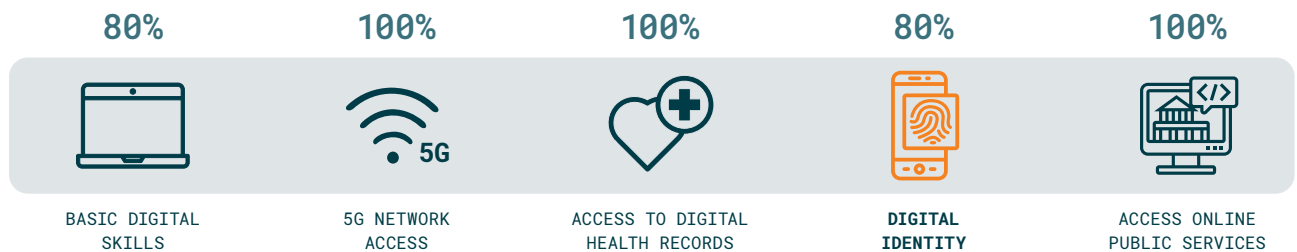
6. THE ROAD AHEAD

The legal framework and market dynamics presented raise the question of the direction in which the European market for digital identification will develop. At the end of this paper, we would like to outline a possible EU-wide solution, contrast this with a national-only solution and round off the chapter with questions that arise from our discussion.

EU GOALS

If one follows the plans of the EU and the digitalisation plans (Digital Compass 2030) in particular, digital identity constitutes an important pillar of the digitalisation agenda. The core points of the agenda are at least 80% penetration of basic digital skills, 5G network availability everywhere, 100% of EU citizens having digital access to their health records and being able to use all essential public services online. Furthermore, 80% should use a digital identity.

Fig. 20 – EU goals stated in the digital compass 2030 for EU citizens.



EU SOLUTION?

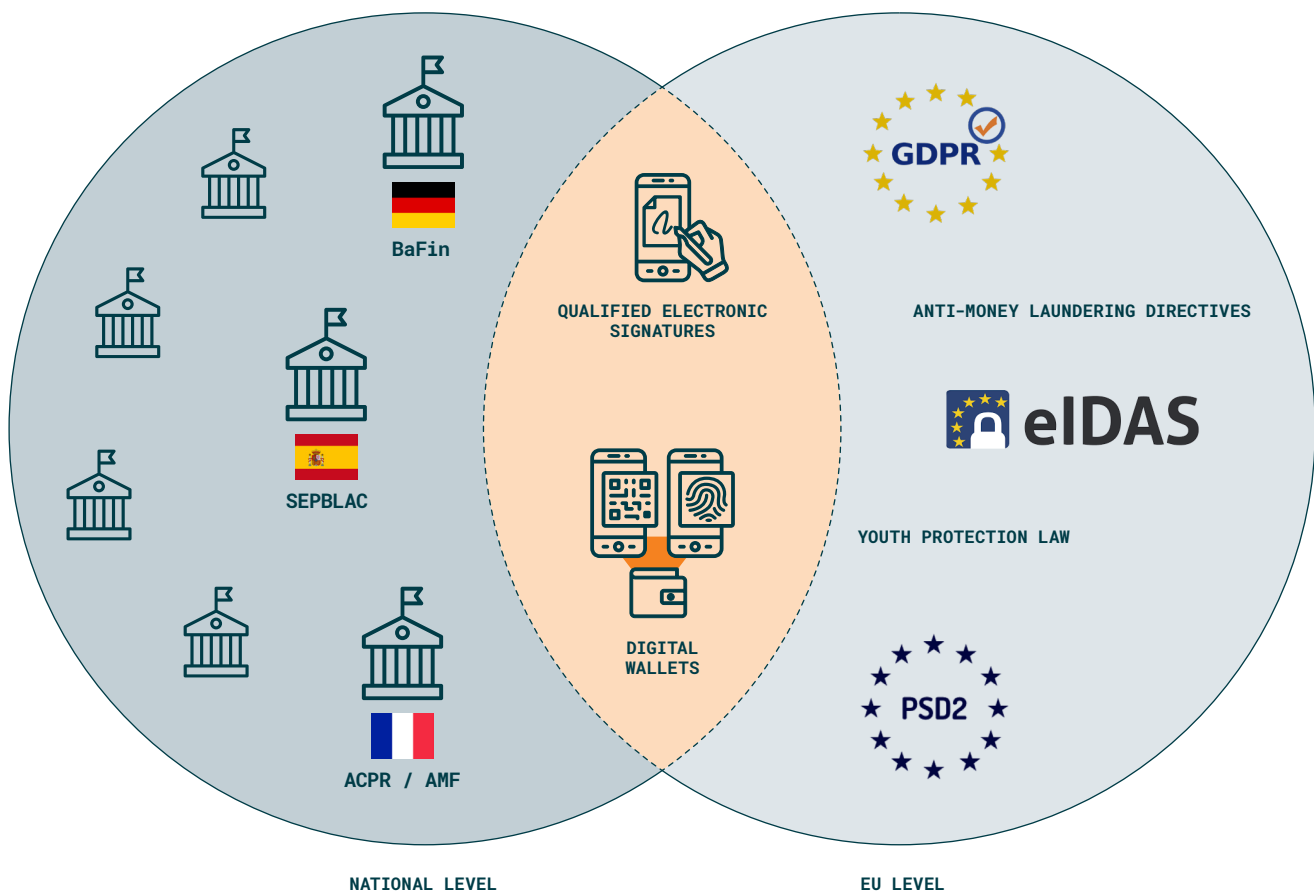
With regard to digital identity, the EU is more concerned with a bureaucracy-free acceptance of the various forms of electronic identification that have been issued on a sovereignly issued ID than with the mandatory placement of its “own” solution.

That the EU wants to create the underlying conditions, not insist on its own solution, is clearly demonstrated by the wallet presented in Chapter 4, which represents an integration approach. Since the previous chapters have shown that the EU countries are at different technological levels and that adoption ranges from “mass adoption” to “not actively used”, the Qualified Electronic Signature could play a decisive role. The prerequisites have been put in place to make a very simple, but still legally valid, form available to Member States under eIDAS.

PRIVATE SOLUTION?
SOLUTION?

Examples from Northern Europe, such as BankID, clearly show that private-sector solutions work in large ecosystems and can also be used in several regions. The market developments presented in Chapter 5 have also shown that there are different dominant processes or players depending on the region. In particular, the consideration of national needs by the respective players speaks for the implementation of existing private-sector solutions (e.g. basic affinity for cashless payments and processes in Denmark vs. cash relevance in Germany). By creating a European level of integration (the wallet), it would be possible to connect national solutions. This would not contradict a uniform EU solution.

Fig. 21 – Possible scenario unifying private and EU solutions.



TENSION BETWEEN EU-WIDE VS. NATIONAL SOLUTIONS

A core challenge remains in the national-only context: how can the users in the respective states know which identification methods are now available if there is no European comparative framework? In summary, it can be stated that this gap can presumably only be resolved by European structures, but that private-sector solutions can be integrated with their respective national characteristics.

Despite the EU's promising approach, there are hurdles ahead.

Currently, the EU's framework for eIDs is only applicable to eIDs used for identifying oneself to public services such as municipal offices, tax authorities and healthcare providers. To be successful, any regulations will need to be applicable to private-sector eIDs and provide reciprocal recognition between private providers.

Currently, however, fragmentation causes unsatisfactory user experience and is a barrier to adoption. Take, for example, the Netherlands, home to both DigiD and iDIN in contrast to the Swedish BankID, which enjoys much more universal coverage within Sweden. Consolidating the mosaic of different eIDs will be a priority, and key to ensuring adoption.

Government-mandated eIDs alone cannot be the solution. Private solutions with high adoption rates already exist – such as Sweden's BankID – and their operators would resist being replaced vehemently. Ensuring high adoption rates for any public-sector solution would also be challenging, as past experience shows.

Fostering private-sector solutions, however, is no panacea either: verifying individuals' identities by means of documents such as birth certificates, passports and identity cards is one of the state's fundamental prerogatives. It remains to be seen how far states will be willing to relinquish control in this area, similar to the challenge cryptocurrencies present to their authority in the sphere of issuing currency.

CONSOLIDATION

Whichever approach, or combination of approaches, prevails, consolidation of eID solutions is sorely needed as a prerequisite for convenient user experience, which is in turn required to ensure the adoption levels necessary for eIDs to take root.

On account of the surge in private equity investments in the area of eIDs, it will be interesting to see which players prevail, and who will be acquired by whom.

Will developments take a similar turn to the payments sector, where a phase of diversification is being followed by consolidation through mergers and acquisitions? In this case, for the time being, we would not expect to see any single EU-wide eID solution emerge at all. That being the case, it will be all the more fascinating to observe what balance the EU strikes, and whether it is successful in promoting uptake of electronic identification without relinquishing control entirely.

7. CONCLUSION

OPEN QUESTIONS

After evaluating the different aspects of the eID, various questions arise that cannot be finally clarified and will probably be addressed by further regulations and developments.

The influence of EU regulation, the commitment of the member states to promote cross-border acceptance and the population's general willingness to adopt will be decisive. For example, how will the eID position itself compared to an ID issued by a sovereign entity? You can travel with a government-issued ID such as a passport, but not yet with the eID. And in this context, what body is chiefly responsible for making that decision?

In addition to the previous forms of identification or activation of the eID, the question also arises as to how the digital equivalent can be created from a haptic ID. Could reading an NFC chip be an option? Will this be put on the mobile phone in the future? Once these questions about the eID product have been clarified, the question arises of a shift from national solutions to EU-wide acceptance and which procedure will prevail.

FINAL REMARKS

Following on from the previous whitepaper on federated eIDs in the Nordic countries, this paper has broadened the perspective from Northern Europe to the entire EU and highlighted current developments and challenges.

ARKWRIGHT PROFILE

WE BELIEVE
IN PRAGMATISM,
METICULOUSNESS
AND IN DEEP
KNOWLEDGE OF
THE INDUSTRIES
IN WHICH WE
OPERATE

Arkwright is a management consulting firm offering strategy advisory services to private corporations, NGOs, investors and start-up companies. Amongst a number of different industry-dedicated teams, our Digital, Payments and Digital Banking practice is one of the most experienced globally, positioning Arkwright as a high-end digital financial services and payments specialist strategy boutique.

With clients that include major financial institutions, central banks, technology providers and institutional investors as well as internet market places and media organisations, Arkwright has hands-on experience in leading and supporting the development of digital strategies and digital transformation.

Our knowledge of global cases and best practices, proprietary ideation methodologies and the hands-on experience of our management consultants and industry experts is able to support throughout the strategy and implementation phases.

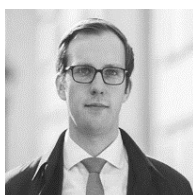
We believe in pragmatism, meticulousness and deep knowledge of the industries in which we operate. At the heart of our mission is the development and implementation of enduring performance improvements and growth strategies, in partnership with our clients.

When we founded Arkwright in 1987, we did so with a strong belief that clients' sustained success requires deeper collaboration and a different working model than what we experienced at the time. Since then, our focus on deep-rooted, long-term partnerships with selective clients has formed the basis of our approach and helped us grow to what we are today: an international consultancy with Nordic roots, operating truly globally from our offices in Hamburg, Oslo, London and Stockholm and with additional operational presence in the Middle East and the US.

AUTHORS



Frank Wunderlich
Partner



Jerrit de Vries
Partner



Nicholas Kirilof
Associate

