bankenverband

Position paper

Digital identities – steps on the path to an ID ecosystem

18 March 2021

Tobias Tenner
Associate Director
Head of Digitalisation
Telephone: +49 30 1663-2323
tobias.tenner@bdb.de

Stephan Mietke
Director
Telephone: +49 30 1663-2325
stephan.mietke@bdb.de

Association of German Banks
Burgstraße 28
10178 Berlin | Germany
Telephone: +49 30 1663-0
Fax: +49 30 1663-1399
www.bankenverband.de
USt.-IdNr. DE201591882

Contents

1 Executive summary

Digital identities have now become an integral of part of our everyday lives. Nine out of ten Germans use the internet, around 80 per cent make online purchases[1] and two thirds of them use online banking.[2] This trend has resulted in the need for digital identity data, including personal log-ins, which now form part of every digital customer journey. However, these are usually stand-alone solutions, which means a digital identity needs to be set up for each provider. In Germany, there is still a lack of available and widely accepted solutions with which people can digitally identify themselves to business partners everywhere (i.e. across various sectors). This is not only due to the lack of interoperability among existing solutions, but also because the identity data collected by businesses may not be used externally. The resulting lack of widely available digital identity data is holding back the urgent digitisation of Germany, and also of Europe.

It is, therefore, all the more important to create an ecosystem for the use and management of digital identities that can be employed across sectors and providers. The aim must be to enable people and, by extension, companies and things (Internet of Things) to be seamlessly integrated into digital value creation processes based on digital identities. At the core of an ecosystem of this kind is the provision of identity data that have already been confirmed by one party (e.g. a bank) and which other business partners can rely on. The identity data should be controlled by the respective identity subject, in keeping with the principle of digital sovereignty and in line with data protection legislation.

Businesses must work together with government to achieve this goal of a flourishing ID ecosystem. It would require new and close cooperation between the public and private sector, whose objective might even extend to formulating standardised procedural and organisational rules (a governance structure) as well as minimum technical standards. The ecosystem would not compete with existing providers of identity solutions, on the contrary, it would allow them to (further) develop their offers and innovations in a joint environment.

However, to achieve this, the legal and regulatory requirements for verifying identities, which are currently inconsistent, need to be harmonised across the different economic sectors. The only way to ensure that the new standards are widely accepted and that the market can adapt to them quickly is for the ecosystem to allow identity data to be used and exchanged across all sectors and for all parties. To achieve this, there needs to be equivalent requirements for the identification processes and mutual recognition by the respective supervisory authorities for all the regulated areas. The most effective way to attain full harmonisation would be by creating a standardised, cross-sector legal framework.

[1] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, pages 10 and 32.

[2] Association of German Banks (2020).

The ID ecosystem should be launched as a national initiative which could then also be developed into a standardised European framework and interoperable identity solution. European payment transactions provide a good example of how the rules and technological standards might be standardised. The private banks expressly welcome the German government's initiative launched late last year to create an open European ecosystem of digital identities.

In order for an ecosystem of digital identities to become a reality, the current legal framework needs to be adapted by incorporating the following measures.

1. There must be a general equivalence of requirements for identification processes in sector-specific rules (including in anti-money laundering and terrorist financing, in the telecommunications sector, the public sector and for trust services). Where these rules are based on European legislation, full harmonisation in the form of a European regulation will be required.

2. The most effective way to achieve full harmonisation would be using a single cross-sectoral European legal framework, which could then act as a reference for sector-specific regulations. This would also ensure that the scope of the data collected by those obliged to check identities is identical in order to make them re-useable throughout the EU.

3. Furthermore, the legislator must continue to create the framework conditions required to ensure legal certainty in the relationship between identity verifier and issuer. This should also include taking account of questions of legal responsibility, such as liability limits, in order to ensure a fair balance of interests and to provide the necessary incentive.

The upcoming revision of the eIDAS Regulation[3] should be used to define horizontally standardised requirements in the sense of full harmonisation at European level, thereby making the whole cross-border verification process much easier.

[3] REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

2 Initial situation

The digital transformation is progressing at pace, new technologies and services are welcomed enthusiastically where they promise to add value for users and are simple and convenient to use. The latest Initiative D21 study, the D21 Digital Index 19/20, reveals that the majority of citizens expect, and indeed, welcomes digitisation becoming an even more ubiquitous part of their daily lives.[4]

On average, every EU citizen currently has around 90 digital identities, including login data for social media accounts, online shops, mobility platforms or online banking.[5] And this figure will continue to rise due to the many digitisation initiatives being pushed in a variety of sectors. In the area of customer onboarding, there is still considerable room for improvement in the level of digitisation. One major weakness is that customers often have to enter lots of personal data manually as part of the application process, even though this information has already been verified and is available in other parts of the system, and simply needs transferring over to the application process. US tech companies have been aware of this problem for a while now. Users with Apple, Google, Facebook or Amazon profiles can use these to log in to other websites.

“What is a digital identity”?

The range of digital identities is broad: they can be limited to a simple combination of username/password with no reference to personal credentials or they can also be linked to personally identifiable information from official proof such as an ID document. They can also include more detailed information, such as payment data, health information or evidence of training and employment.

A “verified digital identity” is a data record that contains the identity and, where applicable, other identity credentials (e.g. holds the title of “Dr” issued by a university, owns a hunting licence issued by a local authority, etc.) about a natural person or legal entity which have been verified by one or more trusted sources (e.g. a bank).

Bringing together all these various data, which can paint a comprehensive picture of the respective person or entity, requires a high degree of integrity and trust within the entire system.

However, these single sign-on authentication schemes offered by tech companies do not guarantee that the data entered by the customer are actually correct. But in regulated sectors, such as banking or mobile telecommunications, companies are legally obliged to verify their customers’ data. Though they do so conscientiously, legally valid identification can often only be

[4] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, page 32.

[5] https://www.bundesdruckerei.de/de/Fokusthemen/Magazin/So-entwickeln-sie-sich-weiter.

carried out with a break in the media chain (e.g. video identification, the German Post-Ident service, etc.). In Germany, the electronic ID (eID) function of national ID cards has not been sufficiently accepted by consumers.

Several European countries have recognised this issue and come up with solutions, particularly in Scandinavia. In Denmark, 99 per cent of the population have been using a digital identity (NemID),[6] which is provided jointly by business and the government, for more than 15 years. With up to 100 million transactions per month, NemID is an integral part of Danes' digital lives. For example, 9 out of 10 customers use NemID to log on to their bank accounts or use administrative services. In 2003, a number of major banks in Sweden developed the BankID. Today, more than eight million out of 10 million Swedes[7] own a BankID which they use to log on to their accounts, verify their digital identities or legally sign contracts digitally.

In contrast, the basis for verifying the identities of natural persons in Germany is still physical documents such as personal ID cards, residence permits or passports. Although nearly all personal ID cards and residence permits issued in Germany are now equipped with electronic proof of identity (eID), and identification procedures like video identification are partly digital, the ID document must always be physically presented (in the form of a chip card) by the consumer for verification, which stands in the way of fully digital user experience.

Although, German ID cards and electronic residence permits have been issued with eID since 2010, the function is only activated in half of all documents.[8] In addition, only seven per cent of German citizens claim to have ever used their electronic ID card.[9] One reason for this is that the number of opportunities to use this function has only started growing quite recently. It could also be down to the inconvenience of needing to combine an ID card with a reading device or smartphone. The legal and technical requirements for transferring an electronic ID from a personal ID card or residence permit to a mobile device are currently being formulated. The objective is to allow identities to be verified solely with a smartphone and to increase user friendliness and acceptance.[10]

Another way of making digital identities available to a broad user base in the short term is to reuse existing identity data, as demonstrated by the Danish example mentioned above. Since banks and also companies from various other sectors are obliged to verify the identity of their customers, this verified information about a person could serve as the basis for creating a digital

[6] https://digst.dk/it-loesninger/nemid/tal-og-statistik-om-nemid/.
https://de.statista.com/statistik/daten/studie/19296/umfrage/gesamtbevoelkerung-von-daenemark/.
https://de.statista.com/statistik/daten/studie/260255/umfrage/altersstruktur-in-daenemark/ and calculations by the Association of German Banks.

[7] https://www.bankid.com/en/om-bankid/detta-ar-bankid.

[8] https://www.cio.de/a/der-online-ausweis-kommt,3654683.

[9] https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf, page 44.

[10] The Federal Government recently presented a draft bill for an amendment to the Act on Identity Cards and Electronic Identification, the Act on a Card with an Electronic Identification Function and the Residence Act (Smart eID Act).

identity. The data are based on government-issued identity documents and are checked at regular intervals, making them comparable in terms of quality and reliability.

The current situation shows that small and large businesses, as well as administrations and public authorities need to be able to implement future-proof and innovative identity verification procedures so that their digital services are used and accepted. Businesses are affected by this issue from both sides – because they need to prove their digital identities as well. They are therefore faced with the additional challenge of combining the digital identity of the legal person with the digital identity of the natural person(s) acting on behalf of the business.

3 The challenge

In Germany, there are currently more than 40 providers of digital identities[11] all competing for users. The exchange of data between these providers and requesting companies usually occurs via bilateral connections. These connections are complex. They require recurring integration costs, individual regulations for technical specifications and contractual agreements. Not only is there limited data portability between the various identity service providers, which often results in isolated applications and data silos, but the digital identities on offer do not always meet the high standards expected by the regulating authority. Ultimately, a company wanting to give its customers access to its services using a digital identity, is faced with the challenge of choosing, from a whole range of relevant suppliers, the best provider for them in terms of implementation costs, customer reach, conversion rate and potential economies of scale.

And what about the users? Despite demand being high, there is still a lack of practical applications in which the same digital identity can be used conveniently and for different purposes (regularly). Without practical applications, the individual will see no benefit from setting up a digital identity of this kind and demand will remain low. The classic chicken and egg problem.

How successful the use of digital identity solutions is will largely depend on how digital users behave in the future. Today, 74 per cent of citizens access the internet from mobile devices, and this figure jumps to 93 per cent in the 14 to 39 age range. In just a few years, more people will use a smartphone to access the internet than a desktop PC or laptop. The use of an app-based identity solution depends, not least, on the number of compatible smartphones in circulation.

Nevertheless, irrespective of the issue of user behaviour, if identity solutions really are to become a resounding success, there must be certainty that they are secure, convenient and, ideally, generally accepted and recognised. It is not only important that the standards enable fitting solutions, but that a fine balance can also be struck between usability and strong security. The maximum extent to which identity solutions can be standardised is therefore crucial.

[11] https://paymentandbanking.com/digital-identity-uebersicht-deutschland/.

At the European level, the 2014 eIDAS Regulation was a milestone, allowing mutual recognition of electronic identity systems in the EU. Its impact has been limited, however, since recognition is reserved for notified eID systems only. Its limitations were also compounded by a continued lack of operative and technical standards both in Germany and in the EU, particularly in the private sector. This resulted in ever increasing hurdles for the development of cross-sectoral and cross-border solutions.

Another challenge is the jungle of different legal requirements of identity verification, both across the various sectors as well as between the national and European levels. This leads to inconsistent framework conditions, hinders the mutual recognition of verified identity data when it comes to reusing them and, depending on their location, puts individual providers at a disadvantage in terms of European competition.

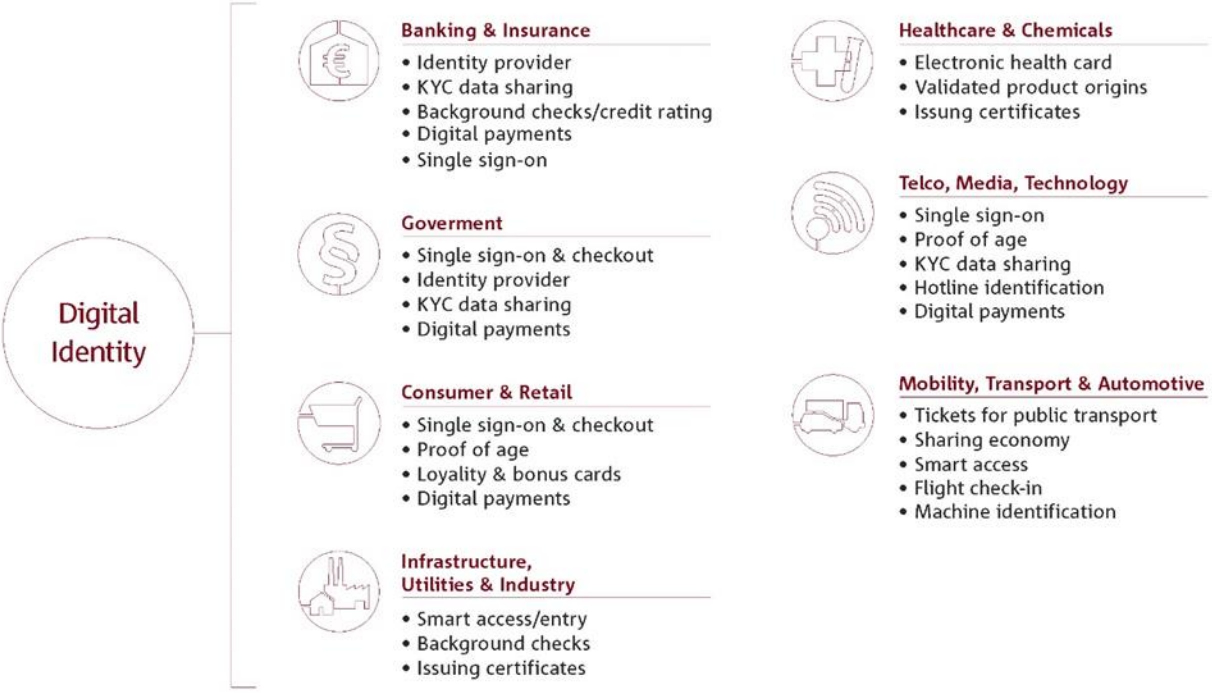
In order to simplify the standardisation and harmonisation process, Germany and Europe should take the approach of a public-private partnership. This would help promote the development of a set of rules, practices and standards that would achieve the interoperability required to provide and operate these identity solutions.

4 Objective: creation of an ID ecosystem

An answer to these challenges is an ecosystem in which digital identity data can be exchanged in a way that is secure, reliable, scalable and convenient. This will have a positive impact on the economic future of Germany and Europe while at the same time enhancing the private sphere of the individual. To be a success, an ecosystem of verified digital identities must

- be usable by different companies and across different sectors,
- enable interoperability with existing schemes,
- be based on consistent and, ideally, globally recognised standards,
- be usable by any individual in society, irrespective of nationality,
- be secure and help to protect consumers against identity fraud,
- be consumer-centric, meaning that it enables data sovereignty,
- be usable in legal contexts and be recognised by all public authorities,
- and be able to accommodate natural persons and legal entities and, in future, objects too.

The following diagram shows the numerous ways in which digital identities could be used across a wide range of industries.



The objective should be to develop a national ID ecosystem for Germany that meets the conditions listed above and is compatible with other European ID ecosystems. Businesses and government should collaborate and possibly establish a public-private partnership to agree on functional, technical, operational, legal and commercial aspects of the data exchange.

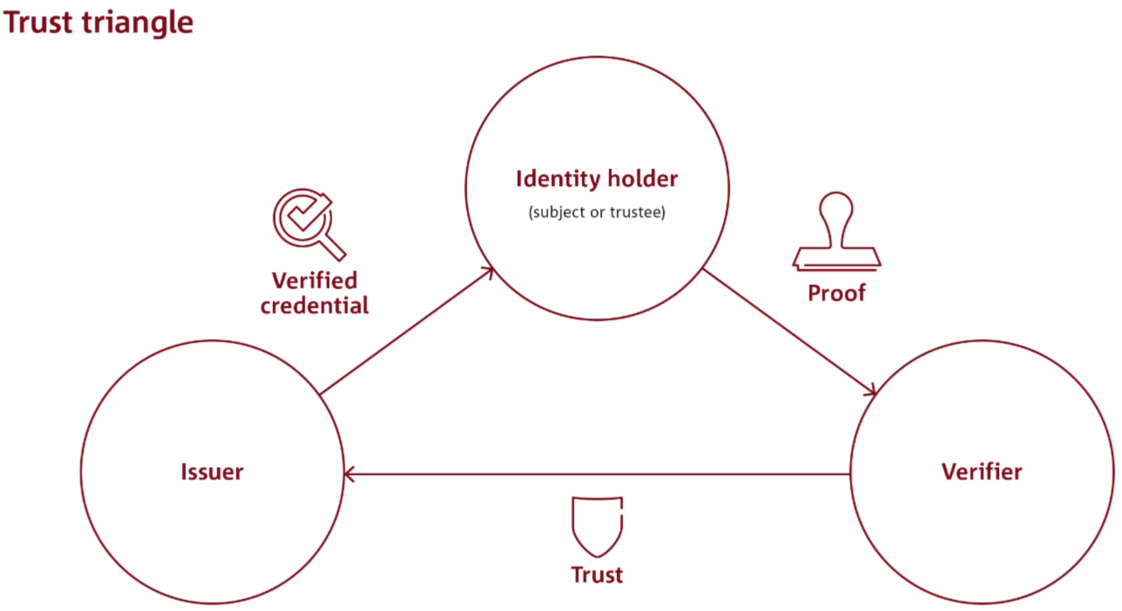
A national ID ecosystem would not, moreover, operate in competition with existing identification solutions such as video identification, national ID function or the various digital identity schemes. Rather, an ID ecosystem offers a framework for providers to create new innovations in the knowledge that data will be mutually accepted and that standard rules and technical requirements apply. A national ID ecosystem along these lines will help to establish a level playing field with fair competitive conditions for all participants.

4.1 Strengthening digital sovereignty by means of self-sovereign identities

The everyday digital life of all citizens today, be it when using social media, ordering goods from e-commerce platforms or researching specialist knowledge, inevitably generates data, the interpretation and commercialisation of which is often in the hands of a few big techs. In view of data protection rules and in the interests of the digital sovereignty of the individual, it is important to give all citizens the opportunity to decide for themselves how their data are used. This applies first and foremost to data that directly affect their own identity. Consumers should always have transparency about this point and be in control of who has access to their identity data and for what purpose.

One possible solution is offered by what is known as a self-sovereign identity (SSI for short), meaning that citizens manage their own identity data themselves and release them for use by a third party as and when needed, e.g. to set up a contractual relationship or use a service. Only the user knows all their identity data and it is the user who decides with whom these data should be shared. This approach allows "identity issuers" (e.g. businesses, public authorities) to store identity data they have verified on the end devices of users and enables the users ("identity holders") to furnish proof of their identify to "identity verifiers" with the help of these data. Identity holders may be individuals, legal entities or even objects (e.g. vehicles, trains). The data are verified using a distributed ledger technology (DLT) network, which serves only as a decentralised public key infrastructure for identity issuers and on which no personal data, not even pseudonyms (such as the user's hash value), are stored. It thus meets all data protection requirements.

The following simple diagram shows the relationship between the issuer, verifier and identity holder regardless of the technical implementation (DLT network or central infrastructure).



The benefits of an SSI approach can be summarised as follows:

- Users have full control over access to their own identity data using a facility such as an ID wallet on their smartphone.
- Identity data are transferable thanks to standardised data formats and protocols.
- Decentralised data storage protects against attacks and central system failures.

- Data of identity subjects cannot be correlated, thus protecting their privacy.
- Open standards offer greater opportunities for growth.
- Data minimisation since identity attributes are only transferred if they are really needed.

4.2 Key role for the financial industry

Experience in other countries shows that banks often play a key role in a successful ID ecosystem. There are several reasons for this.

- As regulated financial service providers, banks are legally obliged to verify the identity of their customers when entering into a business relationship, for example. The basis for this in Germany is the Anti-money Laundering Act (*Geldwäschegesetz*, GwG) and the Fiscal Code (*Abgabenordnung*, AO), which are binding on all German banks and thus represent a consistent standard for verifying data. Compliance with these regulatory requirements is monitored by the German financial supervisory authority BaFin. As a result, the banking industry has a unique pool of verified identities at its disposal, covering practically all citizens with whom a customer relationship exists.

- For online banking, banks have established secure and highly robust channels for customer-bank communication. Secure authentication procedures allow customers to digitally identify themselves to their bank in order to manage their account online and to initiate payments, for example. With the implementation of the second European Payment Services Directive (PSD2), customer authentication requirements have been raised even further and meet the highest security standards. In contrast to interactions with public authorities, for example, most customers use online banking services regularly and are therefore very familiar with the authentication procedures. Owing to their high level of security and frequency of use, these authentication procedures are an excellent means of enabling customers to manage their digital identities.

- Banks enjoy a high level of customer trust when it comes to the protection and security of their data. According to a recent survey, customer trust in banks is higher than in any other industry.[12] This means they are in an ideal position to store digital identities safely and responsibly on behalf of their customers.

In an ID ecosystem, banks could therefore assume various functions. As **verifiers** of digital identities, they could fulfil their statutory identification obligations in this way. Due to the continuous demand for identity checks in customer onboarding, they could contribute a major use case to the ecosystem with comparatively high utilisation rates.

[12] https://de.eos-solutions.com/en/data-survey-2020.html

But they could also take on a central role as **issuers** of digital identities. Banks are not only required to verify the identity of their customers and regularly ensure that data are up to date. They also have other data about their customers which, with their consent, they could make available to other users in an ID ecosystem. Take, for example, proof or confirmation of income, account balances, legal age or creditworthiness. By guaranteeing the security and integrity of the data, they could support businesses and public authorities in making an ID ecosystem more attractive and boosting the range of services available to consumers.

There is another role to consider too: banks could act as **trustees** and identity holders for their customers and manage not only the data they themselves provide in their capacity as issuers but also customer data that other issuers feed into an ID ecosystem. After all, customers already entrust their bank with highly sensitive financial and identity data.

As things stand, however, the lack of a regulatory and technical framework prevents banks and other firms from offering their customers value-added services based on secure and widely usable digital identities.

4.3 Harmonisation of the legal framework for identification processes

A prerequisite for promoting a digital ID ecosystem is cross-sectoral standards for identification processes, especially for verifying identities and reusing identification data. This goes above all for identity data collected to fulfil legal requirements. Banks are particularly affected, along with other entities subject to money laundering regulations, telecommunications companies, trust service providers and public authorities.

With a few exceptions, there are very limited opportunities for individual companies or sectors to exchange data on identities that have already been established and verified and thus to reuse identity data across industries. This is because each industry has to comply with sector-specific legal identification requirements which are not coordinated with one other. To successfully build an ecosystem of digital identities in the near future, it will therefore be necessary to harmonise these sector-specific rules and standardise the sector-specific administrative practices of the responsible supervisory authorities. This would go a long way to enabling verified identities to be reused across companies and sectors.

As a matter of fact there are numerous overlaps between the sector-specific requirements of the German Anti-money Laundering Act (*Geldwäschegesetz*, GwG), Online Access Act (*Onlinezugangsgesetz*, OZG) and Telecommunications Act (*Telekommunikationsgesetz,* TKG). This applies to the type of information to be collected (first and last name, date of birth and address of natural persons, for example), to eligible documents and to data retention requirements. But there are also differences that unnecessarily complicate or prevent the reuse of already verified identification data. These differences concern the scope of the identification data set, for example: while the GwG and OZG require information on citizenship and place of birth, the TKG does not. On top of that, verification methods explicitly permitted in addition to identity documents also differ. Identity verification on the basis of a qualified electronic signature (QES), for instance, is expressly allowed under the GwG, but not by the TKG. What is more, the requirements for establishing identity are frequently fleshed out further by administrative orders and technical guidelines issued by the relevant competent authorities. This causes additional divergence.

In principle, both the Anti-money Laundering Act and the Trust Services Act (*Vertrauensdienste-gesetz*, VDG) provide for the possibility of reusing an identity check that has already been duly carried out by a third party. Under the VDG, this third party may be a bank or another company that is legally obliged (e.g. by the GwG or TKG) to identify their contractual parties. The GwG, by contrast, only permits identification data collected by another obliged entity under the GwG to be reused.

When using identity data across sectors, trust service providers (TSPs) face operational challenges posed by the above differences and depth of detail in sector-specific requirements. Take, for example, the procedures for updating existing identity data in different sectors. It is currently unclear, for instance, whether the processes prescribed in the banking industry to ensure that customer data are up to date (know your customer, or KYC, processes) meet the relevant requirements for trust service providers, or whether changes to registration data, for example, should trigger a new identification process. In addition, a TSP has to check whether the processes and identification procedures used by each individual bank meet the requirements applicable to TSPs even if the bank has complied with all the relevant requirements (of the GwG, Fiscal Code, etc.) when an account was opened. This involves considerable time and effort for both sides and constitutes a substantial obstacle to the cross-sector reuse of identity data.

Another example is the difference in requirements across sectors for establishing identity by means of video identification procedures. Each supervisory authority sets its own requirements: BaFin, for example, in its circular 03/2017 for obliged entities under the GwG or the Federal Network Agency (*Bundesnetzagentur*, BNetzA) in its administrative order 11/2018 on VDG section 11(1) for trust service providers and its administrative order on TKG section 111(1), sentence 4 for telecommunications providers. This can sometimes place German providers at a significant competitive disadvantage compared to their European counterparts, which are not subject to these special German supervisory practices. This development has been observed with respect to German TSPs, for instance.

To eliminate the obstacles outlined above, the following adjustments need to be made to the existing legal framework:

1. There should be general equivalence of the requirements governing identification processes in sector-specific rules and regulations at national and European level. This must cover all areas in which the identification of natural or legal persons is required by

law, such as the area of combating money laundering and terrorist financing, the telecommunications sector, the public sector and trust services. If these rules and regulations have a European legal basis, full harmonisation by means of a European regulation will be necessary, as envisaged by the European Commission in the area of combating money laundering.

2. The most effective way to achieve full harmonisation would be a single cross-sectoral European legal framework forming a basis for sector-specific rules. This would also ensure that the scope of the data collected by those obliged to check identities was identical across the EU. The time-consuming subsequent verification of individual credentials, which is normally required today if data are to be reused, could then be reduced to a minimum.

3. Furthermore, lawmakers must create a framework that enables legal certainty in the relationship between the identity verifier and the issuer. This is because verifiers must, in their own interest and to fulfil their regulatory obligations, be able to rely on the fact that the identity data provided by the issuer have been duly collected in compliance with the requirements to which the issuer is subject (e.g. requirements concerning identification and updating information). Liability issues, such as liability limits, must also be considered to ensure a fair balance of interests and set effective incentives.

The upcoming revision of the eIDAS Regulation should be used to set horizontally standardised requirements at European level by means of full harmonisation and to facilitate cross-border identification processes. This could help to create a coherent EU-wide solution for the cross-sectoral use and reuse of digital identities. The existing eIDAS assurance levels ("low", "substantial" and "high") could, in addition, be used to reflect case-specific or sector-specific needs and risks along the lines of their current application in e-government. Binding rules would also be required to determine which eIDAS assurance level was necessary for which use case. The "substantial" level would be appropriate for identification in compliance with anti-money laundering regulations, as is currently required for qualified TSPs when creating a QES.

4.4 Interoperability between identity providers

The development of digital identity solutions varies across the EU: existing solutions are limited to national markets. The German market is especially fragmented; there are numerous providers, none of which has yet reached a critical mass. An ID ecosystem offers the opportunity to ensure the usability of digital identities by means of different identity schemes and thus help to boost the use of digital identities. The problem is that existing identity solutions are not compatible with one other. They were designed as self-contained solutions with their own interfaces, data credentials and frameworks. Data interoperability between individual identity providers and international networks is an important prerequisite for a fast and robust data exchange.

It is true that schemes already make use of international standards: OAuth 2.0 and OpenIDConnect are established conventions used by identification and authentication services worldwide. But they only function within each closed scheme and are rarely interoperable. As a result, internet portals sometimes support up to seven single sign-on providers. There is also an increasing trend towards the emergence of decentralised approaches to storing identity data according to the principle of self-sovereign identities using DLT. These decentralised approaches are based on standardised communication protocols (DIDcomm) and data standards for decentralised identifiers (DIDs) and verifiable credentials which have been globally defined by the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C). Their goal is interoperability across schemes and national borders.

The Self-Issued OpenID Connect Provider (OP/SIOP) is a standardisation effort currently underway to make the advantages of SSI interoperable with existing interfaces. This could offer verifiers the ability to easily integrate SSI solutions on the basis of familiar interfaces while at the same time broadening their reach.

In addition to technical interoperability, regulatory interoperability also has an important role to play. The eIDAS Regulation already represents an EU-wide legal framework for trust services issuing qualified electronic signatures and seals, for example. In the planned revision of the eIDAS Regulation, it would be desirable to legally enshrine the concept of verifiable credentials as well as issuer certification (along the lines of eIDAS TSP certification).

For an ecosystem to function economically, there is a need not only for framework agreements on functional, technical, operational and legal aspects, but also for framework conditions governing commercial aspects of the exchange of identity data. This is because identification is normally part of a value creation process: the provision of an identity service generates an economic benefit for the verifier. This service, which requires the investment of time and effort, must therefore be commercially advantageous for issuers. In other words, it must be possible to charge either the verifier or the identified party for an identity service. A contractual framework is consequently required for monetisation modalities which sets companies effective incentives to invest in the necessary infrastructure. The complexity of bilateral contracts could be reduced by developing a master agreement at the ecosystem level, for example. This will require the establishment of a governance structure to create overarching rules and agreements (such as liability mechanisms) in compliance with the existing legal framework and promote further development to meet market needs.

4.5 Close cooperation between public and private sectors

An ecosystem of digital identities promises to be successful if the public and private sectors cooperate with one another. This is demonstrated by experience outside Germany, where digital identity solutions have mostly been established through collaboration between various actors, including the state. This is the only way to create the necessary economies of scale and synergies to ensure that the overall system proves attractive and gains user acceptance.

To achieve maximum scalability and the broadest possible acceptance of an ID ecosystem across sectors, the design of the system should take account of the needs and requirements of all stakeholders in equal measure. To ensure this, close cooperation between the public and private sectors should be sought, possibly in the form of a public-private partnership where representatives of the various stakeholders (state, businesses, consumers) work together to develop an ID ecosystem and define corresponding cross-sectoral standards. Selected use cases could be used as a basis for defining and testing out technical standards, the combination of state and private eID procedures, regulatory adjustments and also processes and measures for ensuring maximum usability. In addition to pooling expertise, development costs could be shared or sponsored in the partnership, enabling user-centred innovations to emerge at relatively low cost to individual participants.

5 Outlook

The initiative to create a European digital identity ecosystem launched by the German government at the end of last year is a significant step in this direction and is strongly supported by Germany’s private banks. In a project involving representatives of selected industries and companies, high-profile use cases are to be jointly selected and swiftly implemented. At the same time, the German government has indicated that the necessary regulatory prerequisites will be met to enable developed solutions to be widely used in the relevant sectors. It will nevertheless be important to establish a platform that enables all interested parties and stakeholders to participate in and shape the ecosystem, not least with a level playing field in mind. It is also vital not to repeat the mistake of making the state online ID function the centrepiece of the ecosystem and allowing this exclusive focus to compromise the success of the initiative. It should be borne in mind that, in a market economy, it is user acceptance which will ultimately determine success or failure. In view of the high importance of private-sector use cases in such an ecosystem and today’s global interconnectedness, solutions that transcend national borders and are deployed at least at European level are indispensable in the medium term. National initiatives must rise to this challenge.