DEUTSCHE BUNDESBANK
EUROSYSTEM

Use of electronic identification means (eIDs) in electronic payments and when opening a bank account

Published by the eID working group

Composition of the eID working group

Chaired by:
Dr Heike Winter, Johannes Gerling, Karola Roth
Deutsche Bundesbank

Members:
Stephan Mietke
Association of German Banks (Bundesverband deutscher Banken e.V. – Bankenverband)

Martin Stein, Isabell Wingenbach
German Savings Banks Association (Deutscher Sparkassen- und Giroverband – DSGV)

Dr Olaf Jacobsen
National Association of German Cooperative Banks (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. – BVR)

Stephan Dumröse
Federal Association of Payment- and E Money-Institutions (Bundesverband der Zahlungs- und E-Geld-Institute – bvzi)

*Regina Deisemann, Sabine Brüggem*ann
Association of German Treasurers (Verband Deutscher Treasurer e.V. – VDT)

Julian Grigo, Rebekka Weiß
Federal Association for Information Technology, Telecommunications and New Media (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. – Bitkom)

Sebastian Schulz
Federal Association for E-Commerce and Mail-Order Business (Bundesverband E-Commerce und Versandhandel Deutschland e.V. – bevh)

Gabriele Sieck, Dr Mareike Lohmann, Agnes Speil
German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft – GDV)

Ulrich Binnebößel
German Retail Federation (Handelsverband Deutschland – HDE)

Experts from public authorities with observer status:
Barbara Buchalik, Dominic Steinrode, Julia Kowalski
Federal Ministry of Finance (BMF)

Andreas Polster
Federal Ministry of the Interior, Building and Community (BMI)

Stephan Kohzer, Rainer Schönen
Federal Office for Information Security (BSI)

Occasional involvement:
Dr Stefan Afting, Marlene Letixerant
Federal Ministry for Economic Affairs and Energy (BMWi)

Dr Stephanie Müller, Christian Kassman
Federal Commissioner for Data Protection and Freedom of Information (BfDI)

Olaf Clemens
Bundesdruckerei

Contents

Executive Summary

The digitalisation of economic activities calls for the secure electronic identification and authentication of counterparties. A key prerequisite is establishing suitable electronic means of identification (eIDs). This is all the more crucial for the provision of digital financial and payment services, which poses special challenges for verifying the identity of new customers and the authorisation of transactions.

Against this backdrop, the eID working group has looked intensively into the potential applications of eID solutions in electronic payments and when opening a bank account. This report is intended to contribute to establishing suitable eID solutions in the payments space in Germany and Europe.

The report first of all describes the key statutory provisions governing the use of eIDs in payment transactions in Germany. These include the provisions of the Money Laundering Act (Geldwäschegesetz – GwG), the second Payment Services Directive (PSD2)[1] and the eIDAS Regulation.[2]

Potential use cases for eID solutions in payments are then set out and compared with the status quo. In addition to verifying someone's identity for the purpose of opening a bank account, online accessing bank accounts and authenticating transactions, use cases also include possible applications in e-commerce and the use of eID solutions as a basis for electronic signatures.

The subsequent section provides an overview of how the public and private eID solutions available in the German market that have been deemed relevant for use in payment transactions basically work. A distinction is made here between eID solutions that directly use the electronic ID function of the German identity card (Online-Ausweisfunktion) and other relevant private sector eID solutions.

The report then goes on to look at the prerequisites for successfully establishing eID solutions and identifies existing obstacles. The working group believes that the identity card's electronic ID function stands it in good stead to support further digitalisation in payments and when opening a bank account. However, this function does not currently meet all of the market requirements and little use has thus far been made of it in practice, which is why the working group deems it necessary to also take private eID solutions into account.

That said, both the public electronic ID function and private eID solutions still face key obstacles which will need to be overcome if they are to enjoy broad acceptance across Europe in payments and when opening a bank account. Against this backdrop, the report sets out eight recommendations for action. These are:

- **Promote market growth in the area of eID solutions:**
  In light of the low take-up of eID solutions in Germany to date, all suitable approaches – both public and private – that foster greater use of eIDs are to be welcomed and supported.

- **Make it easier to actively use the identity card's electronic ID function:**
  In order to make the identity card's electronic ID function more relevant in people's everyday lives, it should be made simpler to reactivate identity cards whose electronic ID function is deactivated,

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

and in the near term, more specific use cases should be created in administrative procedures and – where possible – in private sector applications.

– **Open systems for the use of eIDs on smartphones:**
  Regulatory and supervisory bodies should press for the establishment of open systems and interfaces for the use of secure and user-friendly eID solutions on smartphones and ensure a level playing field.

– **Expand electronic identification procedures in conformity with the law:**
  The dialogue between BaFin and the obliged entities with respect to a practicable application of the regulatory requirements of the Money Laundering Act should be continued in order to facilitate the use of electronic identification procedures found on the market without jeopardising the integrity of the financial system or domestic security.

– **Increase cooperation between the private and public sectors in identifying users of private and public online services**
  In order to ensure that eID solutions are as relevant as possible in people's daily lives, every effort should be made to increase cooperation between the private and public sectors in identifying the users of private and public online services. In this context, it should be checked to see whether the current approval procedures for private eID providers accessing public authorities' services could be simplified.

– **Review legal provisions with respect to everyday implementability in digital processes:**
  In order to reap all the benefits of using eIDs, it is particularly important that, in addition to identity verification, all other relevant business processes can also be carried out digitally. In order to promote the use of eID solutions, legal requirements should therefore, as a rule, be examined as to whether and how they could also be sensibly implemented in digital business relationships in a manner that is suitable for everyday use.

– **Commit to an EU-wide level playing field for the use of eID solutions in customer onboarding and the provision of trust services:**
  Initiatives launched at the EU level to harmonise the framework conditions for electronic identification and the provision of trust services pursuant to anti-money laundering legislation should be pursued with the objective of establishing EU-wide harmonised standards that enable the secure and user-friendly use of eIDs and trust services in the EU-wide financial sector and preserve the European level playing field.

– **Simplify notification under eIDAS for private eID solutions:**
  The eIDAS interoperability framework is an important building block for the cross-border use of eIDs in the EU. The barriers to notification pursuant to eIDAS are, however, seen as very high by parts of the private sector, and some of these barriers are reportedly higher in Germany than in other EU Member States. In order to make it possible for the eIDAS framework, which was originally designed for public administrative procedures, to also play an instrumental part in deepening the digital single market, it should be checked whether private sector concerns could be taken into account to a greater extent and the notification of private eID solutions simplified.

The eID working group will continue to monitor developments in the German market for eID solutions with regard to the above recommendations for action.

1 Introduction

The digitalisation of economic activities is increasingly calling for secure electronic identification and authentication of counterparties and the legally binding issuance of declarations of intent in electronic form. Therefore, establishing secure and user-friendly electronic means of identification (eIDs)[1] is an elementary requirement for the further successful development of the digital economy. This is all the more crucial for the provision of digital financial services, which poses special challenges for verifying the identity of new customers and the authorisation of transactions. Furthermore, to strengthen the European digital single market, the EU-wide interoperability of national eID solutions is also of particular importance.

German lawmakers recognised the need for secure eIDs at an early stage and, roughly ten years ago, laid the foundations for a public eID solution with the revised version of the Act on Identity Cards and Electronic Identification[2] (Personalausweisgesetz – PAuswG) of 18 June 2009. All identity cards newly issued as of 1 November 2010 can, in principle, be used to prove the holder's own identity in electronic transactions at the highest assurance level. The introduction of identity cards with a built-in electronic ID function was well received by the public, with many having high expectations of it. However, although more and more economic transactions have been going digital since 2010, use of the electronic ID function has not become widespread. Similarly, so far no comparable private sector eID solutions have been able to successfully establish themselves in the German market.

General conditions for the use of eID solutions in online payments and when opening a payment account have improved in recent years, with the coming into force of the eIDAS Regulation[3] on 1 July 2016 and amendments being made to the Money Laundering Act[4] and the Act on Identity Cards and Electronic Identification in June 2017 and July 2017, respectively. Additional elements include the obligation pursuant to the Online Access Act (Onlinezugangsgesetz)[5] to guarantee digital access to all relevant public services by 2022, as well as the requirements for strong customer authentication and the authorisation of electronic payment transactions pursuant to the second Payment Services Directive,[6] which have applied since September 2019. Fresh impetus for the establishment of eID solutions in online payments is therefore currently emerging – not least on the back of new private sector eID solutions and other factors – and this deserves to be harnessed and forged in the public interest.

---

1 Article 3 of the eIDAS Regulation defines "electronic identification" as meaning the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. It defines "electronic identification means" as a material and/or immaterial unit containing person identification data and which is used for authentication for an online service. This definition has been used for the purposes of this report.
2 Act on Identity Cards and Electronic Identification (Personalausweisgesetz – PAuswG).
3 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
4 Act on the Detection of Proceeds from Serious Crimes (Geldwäschegesetz – GwG).
5 Law for the Improvement of Online Access to Administration Services (Onlinezugangsgesetz – OZG).
6 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

2 Objectives of the working group

The objective of the eID working group, chaired by the Bundesbank, is to promote the use of secure, data protection compliant, user-friendly and interoperable electronic means of identification and authentication in cashless payments and when opening bank accounts remotely. In specific terms, this report aims to examine the conditions under which versatile eID solutions – i.e. solutions not confined to the field of payments – can be used for identification in conformity with the Money Laundering Act and as a basis for means of authenticating and authorising online payments.

Identification means uniquely identifying the payment service user. Authentication means verifying the user's identity or the authorised use of a certain payment instrument, including the use of the user's personalised security credentials (Section 1(1) No 23 of the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz). Authorisation, as defined by Section 675j of the Civil Code (Bürgerliches Gesetzbuch), means the consent (approval or subsequent approval) of a payer to a payment transaction. In electronic payments, these three procedures can coincide temporally and procedurally.

The working group's focus is on use cases for natural persons and technical procedures that use the electronic ID function of the German identity card. Other private sector eID procedures which may be suited to the aforementioned use cases are also taken into account. Ensuring EU-wide interoperability of the eID solutions under consideration also plays a central role in the working group's deliberations. Video identification procedures, which are now widely used, are not examined by the working group.

3 Legal framework

A wide range of specific rules need to be adhered to when providing digital financial and payment services. For the purposes of the working group, the main focus is on the provisions of the Money Laundering Act and the second Payment Services Directive. The Money Laundering Act governs, in particular, the requirements for the identification of customers opening a bank account in Germany. Implementation of the second Payment Services Directive and the accompanying implementing legislation saw strong customer authentication (SCA) generally become mandatory as of 14 September 2019 for online account access and for initiating electronic payment transactions.[7]

The general framework for the use of electronic identification means and electronic trust services within the EU is governed by the European eIDAS Regulation and the implementing legislation accompanying it. These provide a uniform framework for the cross-border use of electronic trust services in Europe and an interoperability framework for the identification schemes [8] notified to the European Commission by Member States for public services. Without being legally binding for the private sector, they are often generally used as a point of reference for eID solutions as well.

7 Strong customer authentication pursuant to the second Payment Services Directive and accompanying implementing legislation requires authentication based on the use of two independent elements categorised as "possession", "knowledge" and "inherence". In the case of electronic remote payment transactions, SCA must further include a dynamic link to a specific payment amount and a specific payee.
8 Article 3(4) of the eIDAS Regulation defines "electronic identification scheme" as "a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons".

3.1 Provisions of the Money Laundering Act

The Money Laundering Act, the current version of which, dated 23 June 2017, transposes the fourth EU Anti-Money Laundering Directive[9] into German law, sets strict requirements for obliged entities when verifying the identity of contracting parties as part of the general due diligence requirements. Use of the German identity card's electronic ID function for this purpose and of other electronic identification schemes with assurance level "high" notified pursuant to eIDAS is expressly permitted in the current version (more details are provided in Section 4.1). The same applies to use of a qualified electronic signature (QES – a trust service under the eIDAS Regulation, see Section 3.3) for identity verification purposes. At the European level, implementation of the revised fourth EU Anti-Money Laundering Directive[10] by 10 January 2020 at the latest will result in eIDs and corresponding trust services within the meaning of eIDAS being expressly permitted in all EU and EEA Member States.[11] The requirements under the Money Laundering Act are specified in greater detail in the Interpretation and Application Guidance of December 2018 published by the Federal Financial Supervisory Authority (BaFin).[12]

3.2 Requirements under the second Payment Services Directive

The second Payment Services Directive generally makes strong customer authentication (SCA, see Section 4.2) mandatory for online access to bank accounts and the initiation of electronic payment transactions. In the case of electronic remote payment transactions, SCA must further include dynamic elements linking the transaction in question to a specific payment amount and a specific payee.

Authentication pursuant to the second Payment Services Directive is designed to ensure that the payment service user is the legitimate (authentic) user who, by using the personalised security credentials, gives their consent to (authorises) the transfer of funds and access to account information. The second Payment Services Directive does not stipulate that a user whose identity was verified when the account was opened must (once again) prove their identity to the payment service provider in order to access the account or authorise transactions.

The SCA requirements set forth in the second Payment Services Directive are transposed into German law by way of Article 55 of the Payment Services Oversight Act. Further details on requirements and procedures for the application of SCA and its exemptions as well as measures to protect confidentiality and integrity of the personalised security credentials are governed, pursuant to Section 55(5) of the Payment Services Oversight Act, by the directly applicable provisions of Commission Delegated Regulation (EU) 2018/389 supplementing the second Payment Services Directive with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

---

9 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

10 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

11 Specifically, Article 13(1)(a) of the fourth EU Anti-Money Laundering Directive, which stipulates due diligence measures regarding customer identification, is amended as follows: "identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council [eIDAS Regulation] or any other secure, remote or electronic identification process regulated, recognised, approved, or accepted by the relevant national authorities".

12 BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act applies to all obliged entities under the Money Laundering Act which are subject to BaFin supervision pursuant to Section 50(1) of the Money Laundering Act. This document can be found at https://www.bafin.de/SharedDocs/Downloads/EN/Auslegungsentscheidung/dl_ae_auas_gw_2018_en.html

3.3 eIDAS Regulation of the European Union

The eIDAS Regulation creates uniform framework conditions for the cross-border use of electronic trust services in the EU and the European Economic Area (EEA).[13] It also provides a technical and regulatory interoperability framework for the cross-border use of national identification schemes notified to the European Commission in the field of public services. It thus supersedes the EU Electronic Signatures Directive (Directive 1999/93/EC) and, together with the Trust Services Act (Vertrauensdienstegesetz), replaces the Digital Signature Act as an implementing act.

The eIDAS Regulation establishes uniform rules for trust services; electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication and lays the legal foundations for their validity and application in the EU and the EEA. As regards trust services, a distinction is made between non-qualified and qualified trust services,[14] with qualified trust services being subject to particularly strict requirements. These trust services provide an important basis for approving a large range of electronic transactions in the EU and the EEA in a secure, legally binding and efficient manner. For the most part, however, electronic payment transactions are not based on the trust services pursuant to eIDAS but on individually agreed means of customer authentication which must meet the requirements of the second Payment Services Directive (see Section 3.2). The trust service of the qualified electronic signature is one of several options for facilitating identity verification in conformity with the Money Laundering Act (see Sections 3.1 and 4.1).

For trust services pursuant to eIDAS, the eIDAS Regulation specifies requirements for trust service providers,[15] their supervision and the cooperation among the supervisory bodies of the Member States. Trust service providers whose head office is situated in the EU are regarded as qualified if a conformity assessment body confirms that they fulfil the relevant requirements laid down in the eIDAS Regulation and qualified status has been granted by the competent supervisory body. Qualified trust service providers are authorised by law to provide their services throughout the EU.[16] In a further key move towards making trust services a more user-friendly feature of people's everyday lives, the eIDAS Regulation greatly simplified the requirements for QES. For example, where creating the signatures once meant that end users had to use signature cards and suitable readers, it is now possible for a qualified trust service provider to create what are known as remote electronic signatures on behalf of the signatory. This makes it considerably easier for users to create a QES and also enables cloud-based remote electronic signatures using a mobile phone, amongst others. One condition for creating a QES as a remote signature is the secure identification of the signatory by the remote electronic signature service provider.

Moreover, the eIDAS Regulation regulates the cross-border use of identification schemes for public services in the EU and the EEA. It does this by creating a technical and legal interoperability framework for the common use of national identification schemes in the European eIDAS network which have been

---

13 These are specified in Chapter III of the eIDAS Regulation.

14 In the case of electronic signatures and electronic seals, a further distinction is made between the advanced and qualified categories, with qualified corresponding to the highest assurance level.

15 The eIDAS Regulation distinguishes between general, non-qualified trust service providers and qualified trust service providers. The latter are subject to particularly strict requirements and more stringent supervision. This is to ensure a high level of trust amongst users in all trust services provided by qualified trust service providers. They are authorised by law to offer qualified trust services (e.g. qualified electronic signatures, seals or certificates) throughout the EU.

16 Trust services provided by third country trust service providers shall be recognised as legally equivalent to qualified trust services as long as they are recognised under an agreement concluded between the Union and the third country in question or an international organisation.

notified to the European Commission.[17] At the same time, eIDAS obliges public sector bodies to recognise notified identification schemes of other Member States.[18]

The private sector is not obliged to recognise notified identification schemes, but has the option of voluntarily connecting to the eIDAS network[19] and taking advantage of interoperability across Europe; where applicable, the private sector may also submit proposals for national solutions regarding eIDAS notification as identification schemes to the European Commission following review by the Federal Government via the national Single Point of Contact (in Germany: Federal Ministry of the Interior, Building and Community).[20]

As regards the notification of national identification schemes, the eIDAS Regulation distinguishes between assurance levels low, substantial and high, and lays down the corresponding requirements.[21] The exact requirements for each assurance level are specified in greater detail in Implementing Regulation (EU) 2015/1502[22] accompanying the eIDAS Regulation. The assurance levels are not binding for eID solutions used outside the eIDAS interoperability framework.[23] Nevertheless, they often serve as a point of reference, including in cases where eID solutions are used in the private sector.

Overall, the eIDAS Regulation lays the foundations for secure, user-friendly and legally binding cross-border electronic communication in digital business relationships across the EU.

---

17 Beyond specifying minimum technical specifications and procedural rules underpinning the technical interoperability of national eID procedures, the interoperability framework of the eIDAS network is supplemented by additional services from the Connecting Europe Facility designed to assist Member States in implementing the eIDAS network.

18 Member States can notify their electronic identification means to the European Commission. Though notification is voluntary, the notifying Member State assumes liability for any damage caused, intentionally or negligently, to any natural or legal person and which can be attributed to a failure to comply with the obligations specified in the context of a cross-border transaction. Since 29 September 2018, all Member States have been obliged to open up their own administrative procedures to notified electronic identification means of other Member States if the administrative procedures in question require electronic identification at assurance level substantial or high.

19 The national identity card portal of the Federal Ministry of the Interior, Building and Community (https://www.personalausweisportal.de/EN/Business/business_node.html;jsessionid=587022A44348285BEC9984D1111D0A17.2_cid322) provides good insights into how the eID function of German identity cards can be incorporated in business transactions. Step-by-step guidance can be found at https://www.personalausweisportal.de/EN/Business/Service-Providers/Service-Providers_node.html. There is also a detailed guide on how to connect to the eIDAS network at https://www.personalausweisportal.de/DE/Verwaltung/ eIDAS_Verordnung_EU/eID_handlungs-und_umsetzungsbedarf/eID_handlungs_und_umsetzungsbedarf_node.html. Although this guide is geared towards public authorities, much of the information it contains is also relevant for private sector service providers wishing to connect.

20 As a rule, all providers of private identification schemes are free to submit their solutions for eIDAS notification to the European Commission through the Federal Ministry of the Interior, Building and Community. To this end, it would be useful if interested providers registered their solutions for an upstream conformity check performed by the Federal Office for Information Security similar to those carried out as part of the procedure for granting private providers of identification and authentication solutions access to the interoperable user accounts in the central and state government portal network (https://www.personalausweisportal.de/DE/Wirtschaft/Zulassungsverfahren/zulassungsverfahren_node.html). Further information regarding eIDAS notification and the relevant set of rules can be found at https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html.

21 The requirements concern the issuance and security of identification means, amongst others.

22 Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

23 The Money Laundering Act, which is particularly relevant for this report, does not use these classifications either.

Key elements of the eIDAS Regulation for the eID working group

Figure 1

Key elements of the eIDAS Regulation

Cross-border use of eIDs by public authorities

- eIDAS aims not to create a single EU-wide eID solution, but to ensure **interoperability of national eID solutions.**
- For this purpose: **establishment of a regulatory and technical interoperability framework** for national eID solutions.
- **Notification of national eID schemes** to the European Commission allows them to be technically connected to the eIDAS network and lays the foundations for their recognition in administrative procedures in other Member States.
- **The private sector** is not obliged to recognise notified eID schemes, but has the **option to connect voluntarily to the eIDAS network** to benefit from interoperability across Europe.
- **Assurance levels low, substantial and high** developed for the eIDAS interoperability framework are not binding for eID solutions used outside the eIDAS interoperability framework, but are often used there, too, as a point of reference.

Uniform regulatory framework for trust services in EU and EEA

- eIDAS creates **uniform framework conditions** for the cross-border **use of trust services** in EU and EEA, and lays the foundation for them to be applied with legal certainty.
- Moreover: **definition of regulatory requirements for trust service providers,** their supervision and the cooperation among national supervisory bodies.
- **Passporting:** qualified trust service providers authorised in one Member State are allowed to offer qualified trust services in all EU and EEA Member States.
- The **trust service of the qualified electronic signature (QES)** is particularly relevant for the working group as, if combined with a reference credit transfer, it can be used for identity verification in conformity with the Money Laundering Act (see Section 4.1).

4 Possible applications of eID solutions in electronic payments and when opening a bank account

eID solutions can be used in electronic payments and when opening a bank account, in particular for identification, authentication and authorisation processes. Furthermore, eID solutions enriched with additional personal information could also be used to conveniently transfer payment and invoice data stored in a user profile to counterparties for payment transactions in e-commerce, say.

4. 1. Possible use cases for identification

The most important potential use case for identification is the identification of the contracting party as part of the general due diligence requirements for obliged entities pursuant to Section 10(1) No 1 of the Money Laundering Act. Section 12(1) No 2 of the Money Laundering Act expressly allows the use of electronic identity proofing pursuant to Section 18 of the Act on Identity Cards and Electronic Identification or to Section 78(5) of the Residence Act (Aufenthaltsgesetz) for the identification of natural persons, i.e. the eID function of the German identity card (see Section 5.1). Pursuant to Section 12(1) sentence 1 Nos 3 and 4 of the Money Laundering Act, identity proofing is also permitted on the basis of an eIDAS notified electronic identification scheme of assurance level high or on the basis of a qualified electronic signature pursuant to Article 3 No 12 of the eIDAS Regulation plus a reference transaction.[24]

In addition to such explicitly cited forms of electronic identification, Section 13(1) No 2 of the Money Laundering Act also allows the use of other procedures authorised by the Federal Ministry of Finance that are suitable for identification and have a security level equivalent to the appropriate examination of the document presented physically. [25]

Besides identification by payment service providers, eID solutions also play a significant role in e-commerce, which is not regulated by the Money Laundering Act. Identity misuse, for example, is a matter of exceptional concern for online retailers. Reliable electronic identification is very relevant, in particular, for payment method control and deciding whether prospective buyers can be offered a means of payment containing a credit risk.

Status quo

Notwithstanding the described reliability of electronic identification means, the identification of natural persons, even in digitally initiated business relationships, still often continues to take place in the traditional way by coming to the branch in person, an identity check performed by the post office, or by video.

Opportunities for applying eID solutions

eID solutions might be a secure and user-friendly alternative to the existing available methods for identity verification in line with the Money Laundering Act. The digital initiation of business processes, especially opening a bank account, could be made significantly easier with a further reduction in the unwanted use of paper-based and analogue processes.

---

24 If identity verification is based on a qualified electronic signature, the obliged entity is to validate the qualified electronic signature pursuant to Article 32(1) of the eIDAS Regulation. Moreover, for the purposes of additional verification, a so-called reference transaction is to be executed from a suitable bank accountbank accountbank accountbank account (see Section 12(1) sentence 2 ff. of the Money Laundering Act).

25 Section 13(2) No 2 of the Money Laundering Act further states that the Federal Ministry of Finance may, in consultation with the Federal Ministry of the Interior, by means of a regulation not requiring the consent of the Bundesrat, define procedures that are appropriate for identification under anti-money laundering and counter terrorist financing law pursuant to subsection (1) No 2.

Specifically, the members of the working group believe that there is currently still considerable potential for improvement by eliminating existing media breaks in the context of both B2C and B2B (e.g. merchant onboarding in acquiring, verifying the identity of authorised representatives of an enterprise).

eID solutions, augmenting personal data on request with additional information such as payment data or invoice and delivery addresses could also play a major role in e-commerce. For example, given consent by the user, payment information and the invoice and delivery address could be transferred to the online retailer with simultaneous verification of the buyer's identity. This would prevent fraud and, at the same time, provide users with a secure and convenient option for transferring payment and invoice data.

4.2 Strong customer authentication (SCA) when accessing the bank account or other online user accounts

Access to the bank account could be another potential use case for eID solutions. Since 14 September 2019, strong customer authentication (SCA) pursuant to Section 55(1) No 1 of the Payment Services Supervision Act has been the obligatory standard for this. This means that, as a rule, customer authentication is based on the use of two independent elements (two-factor authentication) categorised as:

- knowledge (something only the user knows);
- possession (something only the user possesses);
- inherence (something the user is).

Status quo

Up to now, account servicing payment service providers (ASPSPs) have normally been using proprietary or sector-specific authentication procedures which they themselves make available to their customers. In addition to a PIN or a password, the prescribed second factor is generally made possible by the provision, say, of TAN generators, photoTAN or mTAN procedures or by linking a mobile device with a bank account. The banks' own procedures for logging into an account can usually also be used to authenticate transactions (see Section 4.3).

Potential applications of eID solutions

The electronic ID function and other eID solutions on the market (see Chapter 5) offer the possibility of SCA compliant with the second Payment Services Directive and would therefore come into consideration as a cross-institutional means of authentication when logging into online banking applications. Users could benefit from this by no longer having to familiarise themselves with individual banks' means of authentication and, possibly, having to carry the necessary relevant hardware with them; instead, they would be able to make use of a universal procedure that they could, in principle, also use for secure authentication outside the realm of payments.

Apart from the fact that they would obviously have to provide a high level of security and user convenience, the question of whether eID solutions for regular logging into online banking applications actually can offer added value also depends on whether the procedures could be used not just for logging into the bank account but also authenticate transactions, and how moving away from in-house procedures would impact the flexibility of the ASPSPs in the event of authentication means being blocked, say.

Further use cases for secure eID solutions in online banking might consist in identity proofing the customer when they apply for access to online banking (given an existing business relationship) or when the customer changes to another security procedure offered by the ASPSP or when changing key customer data, say, after relocation. eID solutions could also be employed when informing an insurance company of a change in account details, e.g. via its online customer portal. In the case of payment of a claim or compensation

for loss or injury, in particular, the correct identity of the account holder has to be ascertained and checked in a legally watertight manner to prevent a transfer to the wrong account that may even be initiated with criminal intent.

Fundamentally, beyond the use cases in payments, there are a great many other areas where eID solutions can be used for authentication purposes, such as the electronic retrieval of sensitive data, for logging into online user accounts – say, with public services or an insurance company – or as backup authentication if a password has been lost or the user and/or access data of an existing user account have been altered.

4.3 Strong customer authentication (SCA) when initiating electronic payments

Since 14 September 2019, pursuant to Section 55(1) No 2 of the Payment Services Supervision Act, strong customer authentication (SCA) has also been obligatory for initiating electronic payments initiated by the payer. Furthermore, in the case of electronic remote payment transactions, "dynamic linking" of the SCA to the specific payment amount and payee is required as well (Section 55(2) of the Payment Services Supervision Act).[26]

Status quo

As described in Section 4.2, up to now, ASPSPs have, as a rule, been using proprietary solutions employing, for instance, TAN generators, photoTAN or mTAN procedures or the linking of a mobile device with a bank account – which are used both for logging into an account and to authenticate payments transactions.

Potential applications of eID solutions

Cross-institutional eID solutions could, in principle, also be used to authenticate transactions. Looking ahead, they could also serve as standardised and competitively neutral procedures for authenticating payments in a very wide variety of payment situations (e.g. for the authentication of instant payments at the point of sale). In technological terms, the electronic ID function of the German identity card, for example, offers the possibility of authenticating transactions.[27] BaFin has so far not examined whether this function is in conformity with the second Payment Services Directive, however.

The cross-institutional use of eID solutions for authenticating transactions is likely to mean that users would have to rely on fewer authentication procedures in their daily lives.

For ASPSPs, one of the things on which the attractiveness of using external procedures ultimately depends – much like their use for logging into online banking applications (see Section 4.2) – is how much flexibility the use of third-party solutions would leave them in the technological and organisational design of the authentication procedures and risk management operations.

4.4 Application for issuing a direct debit mandate

eID solutions could also play a part in the legally watertight authentication of SEPA direct debit mandates which are issued online.

---

26 Exemptions from the requirement for SCA are regulated by Articles 10 to 20 of Commission Delegated Regulation (EU) 2018/389 (regulatory technical standards for strong customer authentication and common and secure open standards of communication) under the second Payment Services Directive.

27 The electronic ID function of the German ID card expressly provides for transaction-related information (see Federal Office for Information Security Technical Guideline TR-03112-7, Part 7, 3.6.3, TransactionInfo: "This element MAY contain transaction-related information, which MUST be displayed in the eID-PIN dialogue before the PACE-protocol is performed."). This means that it is possible to link a transaction, say, to the display of an amount or of a payee; these elements are then also incorporated into the transport protocol.

Status quo

In line with an understanding reached by the German SEPA Council and a joint declaration by the German Federal Ministry of Finance and the Bundesbank from 2013, it is indeed possible simply to issue a direct debit mandate online,[28] but the onus is on the payee to substantiate and prove that they are in possession of a mandate issued by the payer. Since 2015, the rulebooks for the SEPA direct debit procedure provide that, in addition to the mandate being given in writing, the mandate may be an electronic document which is signed using a "legally binding method of signature". What is crucial for the acceptability of the possible methods of signature conceivable in this context is whether the bank of the payer can take sufficient precautionary measures to ensure that the identity of the mandate issuer and of the payer are the same.

Possible application of eID solutions

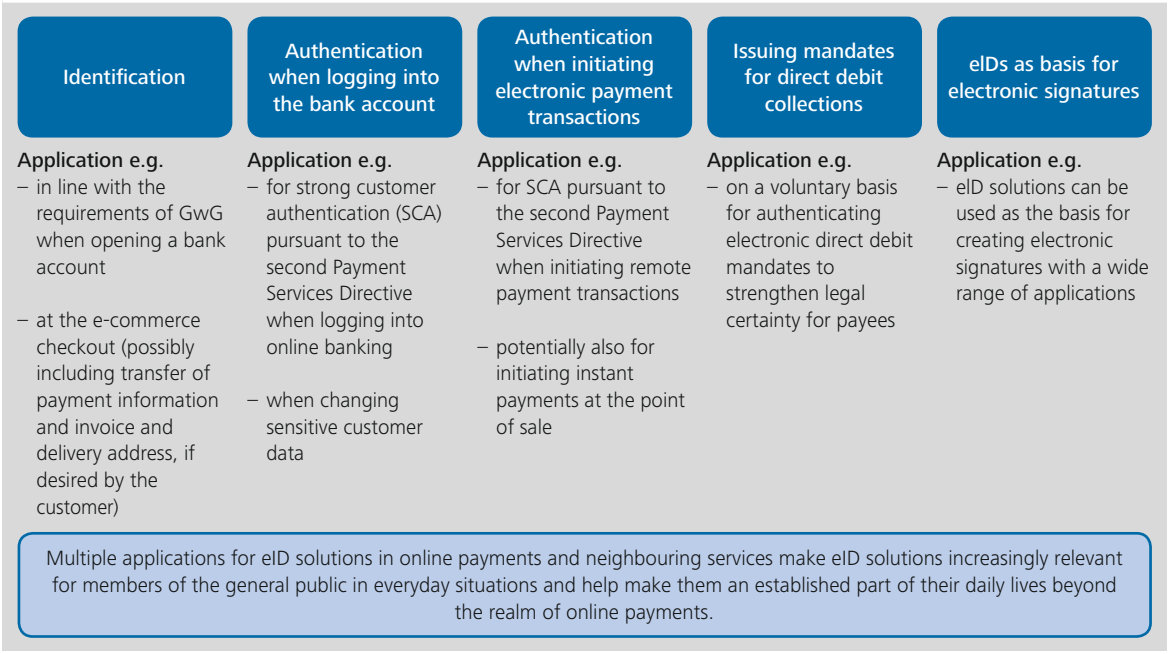
The voluntary use of a legally secure and user-friendly eID solution when issuing an electronic direct debit mandate might represent one possibility of creating a user-friendly Europe-wide solution for electronically issuing direct debit mandates online with a clear audit trail, thus reducing existing legal uncertainty on the part of payees. eID solutions could be employed, in particular, for the issuance of mandates for recurrent or regular direct debit collections. For the electronic ID function of the German identity card, there are, for example, already several practically tested solutions for customer authentication when issuing SEPA direct debit mandates.

4.5 eID solutions as a basis for electronic signatures

Besides the possible use cases listed above, eID solutions can be used generally as the basis for creating electronic signatures for a wide range of uses. This is because it is a prerequisite for an electronic signature that there is prior secure identification of the signatory for the signature service provider. The potential applications of electronic signatures in the financial sector are fundamentally very wide-ranging but are not to be discussed in further detail in this report.

28 The bank of the direct debit submitter decides whether it will accept mandates which have been issued online. The contractual arrangements between the payee and its payment service provider are the decisive factor.

Possible use cases for eID solutions in online payments Figure 2



5 Relevant eID solutions on the German market

Having a comprehensive understanding of the eID solutions found on the market and how they basically work is key to promoting the establishment of suitable procedures and being able to identify and suitably address existing challenges in using them. For this reason, the following section provides an overview of the eID solutions on the German market that are relevant for the purposes of the working group.

eIDs can take very different forms, and security and assurance levels sometimes vary greatly. In view of the specific technical security requirements for payment transactions and the relevant provisions of the Money Laundering Act described above, eID solutions appear to be particularly relevant for the purposes identified by the working group if they:

– (potentially) [29] permit identification in conformity with the Money Laundering Act;[30]
– could be used for strong customer authentication.

In this analysis, the eID solutions on the market are broken down as follows:

(1) eID solutions that directly use the German identity card's electronic ID function;
(2) other relevant eID solutions.

5.1 eID solutions that use the German identity card's electronic ID function

Since 1 November 2010, German identity cards have been issued with a chip which enables the use of the electronic ID function. Also, electronic residence permits issued since 2011 have included the electronic ID function.[31] By the end of October 2020, all old identity cards will have been exchanged for new identity cards which offer the electronic ID function.

The Act for the promotion of electronic identity proofing (Gesetz zur Förderung des elektronischen Identitätsnachweises), which entered into force on 15 July 2017, contains a series of simplifications with the aim of promoting user-friendliness and the acceptance of the electronic ID function among service providers, such as online retailers and credit institutions, and identity card holders. These include issuing every new identity card with the electronic ID function enabled,[32] simplifying the issuance of authorisation for service providers to use the electronic ID function, establishing a new function allowing on-site reading of identity card data[33] and authorising identification service providers who provide electronic identification services for third parties based on the electronic ID function. For example, service providers now also have the ability to access identification services based on the electronic ID function (eID as a service) via identification service providers[34] and incorporate them into their own online services. A number of providers are already active in this new market.[35]

While some of the identification services offered are directly integrated into the online service vis-à-vis which identification is to take place, other solutions direct customers to the website of the eID solution provider for the purpose of identification and then back to the respective online service.

---

29 According to Section 13(1) No 2 of the Money Laundering Act, the use of other procedures for identification approved by the Federal Ministry of Finance having a security level equivalent to the appropriate examination of documents presented physically is possible. BaFin takes that view that additional other suitable procedures of this kind can be permitted exclusively by way of a regulation pursuant to Section 13(2) No 2 of the Money Laundering Act (i.e. by means of a regulation of the Federal Ministry of Finance in consultation with the Federal Ministry of the Interior; see Section 5.1.3.2. of BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act of December 2018). Electronic identification means for which future permission of this kind appears possible should also be included in future analysis.

30 An in-depth review of the individual solutions depending on the specific intended use would be required to establish whether individual solutions categorised as "other relevant eID solutions" would indeed be suitable for identification in conformity with the Money Laundering Act and to ascertain whether additional applications would be suitable in online payments. Such a review – of all conceivable eID solutions for all conceivable use cases – is, however, expressly not the aim of this report.

31 The statements made in the following regarding the identity card's electronic ID function therefore also apply to the electronic residence permit's electronic ID function.

32 Previously, the identity card's electronic ID function was deactivated by default at the time of issuance and people had to explicitly consent to activation. Deactivation is now no longer envisaged.

33 The on-site reading function enables personal data stored on the chip to be read for the purpose of identity verification against the identity card, subject to the consent of the identity card holder, in cases where the identity card holder is physically present, without PIN entry or any further action by the identity card holder. This speeds up the collection of personal data, and errors arising from manually transferring data are avoided. Authorities and companies wishing to offer this function require public authorisation (a key certificate) for on-site reading and an appropriate reading device as well as software.

34 Section 2(3a) of the Act on Identity Cards and Electronic Identification defines identification service providers as service providers whose service consists of providing a third party with a case-specific identification service by means of electronic identity proofing pursuant to Section 18 of the Act on Identity Cards and Electronic Identification.

35 An overview of the identification solutions based on the electronic ID function currently on the market can be found at https://www.personalausweisportal.de/DE/Wirtschaft/Anwendungsbeispiele/Identifizierungsloesungen/identifizierungsloesungen_node.html

Service providers who wish to use the electronic ID function do not require their own or hosted eID server infrastructure. The identification service providers certified by the Federal Office for Information Security and authorised by the Federal Office of Administration, Authority Awarding Authorization Certificates[36] enable simple and secure electronic identification using the electronic ID function at the eIDAS assurance level high and meet the requirements of the Money Laundering Act.

One prerequisite for the use of the electronic ID function is that this function is activated on the identity card. This has usually been the case for identity cards issued since July 2017. In addition to their PIN, identity card holders also require eID Client software (integrated into the application or as an additional app) on their smartphone, tablet, PC/Mac or terminal. While an additional dedicated reading device was required to read the data stored on the chip up until a few years ago, the data can now also be read using the NFC function of a suitable smartphone or tablet. This has also been possible for Apple smartphones (iPhone 7 or higher) since the end of September 2019.

The electronic ID function ensures strong customer authentication by using the two factors "knowledge" (PIN request) and "possession" (possession of identity card, cryptographically proven by means of chip authentication) – as well as the end-to-end encryption of data from the client to the server (chip and terminal authentication). Owing to strong identification at assurance level high, it is the most technically secure method for the creation of a QES in the form of an eIDAS remote signature,[37] meaning that identification service providers who are also qualified trust service providers or who work with qualified trust service providers can also provide QES based on the electronic ID function. What is more, at least one service provider on the market reportedly provides solutions for PSD2-compliant online access to the bank account and transaction approval.

Through notification to the European Commission, mandatory recognition of the German electronic ID function by EU Member States in electronic public services if the latter require electronic identification at assurance level substantial or high has been in place since 29 September 2018.

To ensure that the entire resident population and workforce in Germany (with the exception of non-EU citizens without an electronic residence permit, long-term tourists and other visa holders) are fully equipped with a secure electronic identification means, current draft legislation envisages the introduction of the "eID card" from 1 November 2020 – a chip card for EU citizens with the electronic ID function but without the visual identity card function and without biometric data.

The identity card's electronic ID function, as a public and competitively neutral eID solution, represents an important element for secure digital identification in Germany.

On top of the electronic ID function, the Federal Government is helping develop a secure mobile eID at assurance level substantial by funding the OPTIMOS 2.0 project (see the box). The idea behind this new identification means is both user-friendly and sufficiently secure deployment in everyday applications in the private and public sectors.

36 Section 21b of the Act on Identity Cards and Electronic Identification sets out the requirements for authorisation to provide identification services based on the identity card's electronic ID function for third parties as an identification service provider within the meaning of Section 2(3a) of the Act on Identity Cards and Electronic Identification.
37 Obtaining a corresponding signature certificate is necessary for this. At present, though, there is only one provider in Germany who provides the necessary certificates and the remote signature service for the electronic ID function.

OPTIMOS 2.0 project

The idea behind OPTIMOS 2.0[38] is to define an open, workable ecosystem of secure identities for mobile services and to demonstrate the benefits it offers using, for example, secure scalable eID applications in the eID, eGovernment, Internet of Things and mobility market sectors.

Today's consumers use their smartphones to access numerous services requiring a high level of security. For example, they unlock car sharing vehicle doors, open bank accounts and register new addresses with city authorities. To do this, they usually set up an identity (eID) directly with the provider of the service, which then has to be verified in a trustworthy, and mostly time-consuming, process. Digital technologies with an adequately high protection level which offer this functionality ad hoc from a smartphone have been lacking thus far. In addition to logging in/registering with service providers, secure eIDs can also be used on site with near field communication (NFC) technology. To do this, the user holds the mobile device near another object fitted with an NFC chip, such as the door handle of a hotel room. This makes eID very simple to use.

The OPTIMOS 2.0 project will create an open ecosystem that provides the technologies for secure eID services. These technologies will equip eID service providers to offer mobile eID services with the assurance level substantial and high pursuant to the EU regulation on electronic identification and trust services for electronic transactions (eIDAS). The ecosystem developed in the project will be notified to the EU as having assurance level substantial, meaning that it can be used across the whole of Europe.

Providers of mobile services wishing to store sensitive data other than the eID on smartphones can benefit from the open ecosystem: for example, airline companies can store boarding passes, transport companies a personal annual season ticket, and car sharing companies and hotels digital car or room keys. Until now, storing these application-specific data securely on customers' smartphones has been a complex challenge for every service provider. Given the many different types of mobile phone and the multitude of mobile operator, there is a wide variety of hardware. The OPTIMOS 2.0 project aims to create a platform that relieves service providers of the time-consuming task and ensures a high level of hardware-based security at the same time.

OPTIMOS 2.0 is a research project funded by the Federal Ministry for Economic Affairs and Energy as part of the "Smart Service Welt II" programme. The Federal Ministry of the Interior, Building and Community and the Federal Office for Information Security are closely involved in the project.

38 Further information on the OPTIMOS 2.0 project may be found at https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SmartServiceWeltProjekte/Wohnen_Leben/SSWII_Projekt_OPTIMOS_20.html

5.2 Other relevant solutions

Recently, the German market has also seen an increase in eID solutions being offered that are not necessarily based on the electronic ID function of the identity card. While these eID solutions differ considerably from one another in some cases in terms of their intended uses and their protection or trust levels, some providers are targeting areas of application with specific requirements for technical and organisational security. Some of these eID solutions are already being implemented for primary identification in conformity with the Money Laundering Act and for more of the use cases in online payments listed in Chapter 4.

The relevant solutions generally function, as it were, as "eID platforms" or "eID intermediaries", meaning they collect identity data[39] and disclose these data – with the owner's consent – to third parties[40] or arrange for the data to be transmitted without gaining possession of them themselves. The eID solutions considered here use proprietary IT infrastructures, which are independent of the electronic ID function of the identity card or other notified identification schemes.[41] Given that the electronic ID function of the identity card is not used for every identification, these solutions use authentication means other than those of the electronic ID function of the identity card, meaning that they can also use biometric information evidence, for example.[42] This can make these solutions more user-friendly and increase their suitability for everyday use, but it can also lead to the procedures having a lower level of technical security. As a result, these solutions which do not use a hardware component such as the chip of an identity card do not reach eIDAS assurance level high.[43]

One essential condition for putting these eID solutions to good use in the vast majority of the use cases identified by the working group – alongside adequate technical and organisational security[44] of the processes used – is secure and reliable initial identification of the user by the solution provider ("enrolment process"). Procedures in conformity with the Money Laundering Act for initial identification are of particular importance for the working group in this regard.

---

39 In addition to recording identities in conformity with the Money Laundering Act, some of the solutions on the market also have the option of creating a "simple" eID user profile with the service for which it is not necessary to record the user's identity in conformity with the Money Laundering Act. However, the focus of attention here is on the user profiles recorded in conformity with the Money Laundering Act.

40 The manner in which the identity is disclosed to third parties varies among the different eID solutions and sometimes even from one use case to the next within one and the same solution. In some cases, the eID platforms themselves save the identification datasets, and in others they merely access datasets stored at other institutions.

41 In principle, the underlying technical infrastructure can be very multifaceted and employ not just traditional technologies but suitable innovative ones as well.

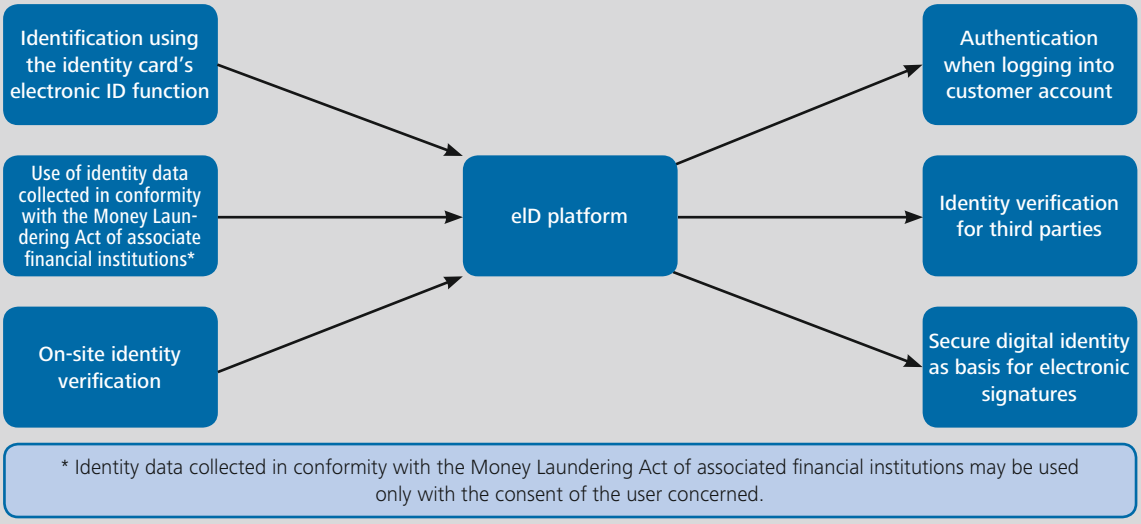
42 Conformity with data protection provisions should be observed in particular when using biometric authentication means since, pursuant to Article 9 of the General Data Protection Regulation, biometric data belong to the special categories of personal data, the processing of which is only permitted subject to special requirements.

43 Secure primary identification upon issuance and additional security requirements regarding the holder's sole control over the identification means are essential requirements for achieving assurance level substantial.

44 The assessment of what level of technical and organisational security would be appropriate in the processes depends on the specific use case or purpose and will not be discussed in any further detail here.

Schematic overview of how "eID platforms" work

Figure 3



A great many such procedures exist in the market (e.g. on-site identification, video identification procedures, use of identities recorded in conformity with the Money Laundering Act of cooperating firms, or use of the electronic ID function). Furthermore, many providers offer their customers more than one procedure to choose from for initial identification.

In principle, the eIDs created in this way are suited to many different use cases and can generally be integrated into the online services of service providers, such as online retailers, using appropriate interfaces. Depending on the purpose and sensitivity of the data transmitted, it may be the case that one and the same service provider will offer different authentication means (simple authentication with username and password vs. two-factor authentication). Furthermore, many of the service providers offer additional services such as the creation of a QES or the specific confirmation of certain pieces of personal data, e.g. for age verification.

Since various eID solutions are run using technically independent systems, interoperability between different solutions cannot be taken for granted. Thus far, the Federal Government has not notified any of these private sector solutions as identification schemes to the European Commission. Notification would be a requirement for use of the eIDAS network's interoperability framework.

6 Prerequisites for successfully establishing eID solutions, existing challenges and potential unwelcome developments

6.1 Prerequisites for the successful establishment of eID solutions

It goes without saying that the use of eID solutions in the use cases described in Chapter 4 crucially depends on satisfaction of the respective direct technical requirements and legal and prudential supervisory rules[45] and on there being appropriate security standards in place for the use case in question and the sensitivity of the data being processed.

However, it will only be possible to harness the full potential of eID solutions for online payments and people's increasingly digital lifestyles if eID solutions emerge which are not confined to specific use cases but offer the general public the possibility to use a single preferred eID solution, or just a small number of them, to identify and/or authenticate themselves to a large number of service providers without constantly having to re-register. For this reason, thought will need to be given not just to the direct challenges presented by individual use cases, but also to a series of general market forces and user requirements if eID solutions are to be successfully established on a broad basis:

Two-sided market: On the side of the online service providers, the integration of specific eID solutions depends on whether the procedure is available to customers on a sufficiently broad basis. On the customer side, however, there will only be an incentive to sign up for a solution if it can be used in enough different ways ("chicken-and-egg problem").

This conditionality determining the success of certain services is the hallmark of two-sided markets of the kind generally also found in the world of payments. This is why solution providers find it extremely difficult initially to establish new eID solutions if both sides of the market are to be won over into using them. However, for procedures which are based on familiar and already widespread elements, such as the identity card's electronic ID function,[46] or solutions which apply the existing authentication means used in online banking, this problem is not so pronounced.

Overcoming today's "chicken-and-egg problem" by making a clear commitment to the use of eID solutions and swift implementation on the part of public and private service providers will by key to the successful establishment of eID solutions on the German market.

User-friendliness: eID solutions will only be successful if they are user-friendly. In general, both sides of the market expect them to be as easy to use as possible, though this can clash with security requirements for the procedures in some cases. In order to prevent a lack of user-friendliness from undermining the successful widespread use of eID solutions, there should be a balance between user authentication requirements and the specific security standards for the services used. This conflict of aims crops ups frequently, and providers must therefore decide on a case-by-case basis – and in line with statutory and supervisory provisions – how appropriate eID solutions can be found for the respective use case. Equally, users need to find solutions which suit them best – solutions which lend themselves to everyday use while at the same time satisfying their needs, especially in terms of data security and data protection. eID solutions

45 Including and in particular those on data protection and national security and those safeguarding the integrity of the financial system.
46 One special feature of the identity card's electronic ID function is that although the vast majority of people have identity cards containing the electronic ID function, many of the identity cards issued up to 2017 still have this function deactivated (see Section 8.1).

which allow users to toggle the setting between user-friendliness and security depending on the use case and risk situation may prove advantageous from a user's point of view. The establishment of secure smartphone-based eID solutions, such as those envisaged in the OPTIMOS 2.0 project (see the box above), could also significantly enhance the user-friendliness of eID solutions.

Relevance in everyday life through versatility:
What is also important, especially for eID solutions which rely on the "knowledge" factor (e.g. a PIN) to authenticate users, is that these solutions are used quite regularly, as otherwise it is highly likely that users might forget or mislay the information they need for authentication and be unable to use their eID (for a time). Any such eID solutions could quickly become irrelevant in people's everyday lives.

It would appear, then, that eID solutions stand a particularly good chance of gaining a foothold in the market if users deploy them in as varied and as frequent a manner as possible.[47] This assessment is consistent with the findings of a recent eGovernment Monitor survey in 2018, which show that the public want eID solutions which can be used for both private and public purposes, and also with experiences in other countries where eID solutions have been successfully established (e.g. common identity solutions for the private and public sector in Scandinavia). The increased use of eID solutions in public administrative procedures could therefore also act as a key catalyst for the use of eIDs in the private sector (see the box).

In the financial sector, a combination of particularly sensitive services and legal regulations means that there are strict requirements for the unique identification and authentication of customers in many instances (see Chapter 4). Electronic identification in conformity with the Money Laundering Act is a key element here, but the need to identify customers in this manner does not arise regularly during the course of a traditional business relationship between a customer and a financial institution; this has clearly hampered the successful establishment of eID solutions for this purpose so far. It would be a good idea to design an effective process in which identification is done digitally and not using a time-consuming procedure on paper. This would also eliminate the need to provide printed copies of identity cards, which would be a welcome move in terms of data protection.

However, as business relationships go increasingly digital, comparison websites – including those for financial services – grow in importance and consumer behaviour in general undergoes major change, there is a tendency for many financial market business relationships to become more short-lived or be conducted in parallel, as consumers engage in context-specific business relationships with a variety of financial institutions. Looking ahead, this is likely to significantly increase the need for remote identification in conformity with the Money Laundering Act and for universal customer authentication instruments. In addition, making more frequent use of eID solutions to satisfy the requirements under the Money Laundering Act[48] to keep documents, data or information obtained concerning the contracting party up to date could contribute to the increased use of remote identification means in conformity with the Money Laundering Act.

---

47 The representatives from retail noted that the use of eID solutions in B2C trade also appears to be particularly suitable in this regard. eID authorisation could help bricks and mortar purchases at self-service checkouts via an app or online in webshops become relevant in everyday life if simple, user-friendly processes are developed.

48 Amongst other requirements, Section 10(1) No 5 of the Money Laundering Act states that obliged entities are to ensure that the relevant documents, data or information used for identification of the contracting party are updated at appropriate intervals, taking into account the respective risk. Further information on this can be found in Section 5.5.2 of BaFin's Interpretation and Application Guidance of December 2018.

Yet for all this, eID solutions which guarantee a relatively high assurance level still face the challenge of achieving enough interactions to make them a feature of people's everyday lives.

Many members of the general public log into online user accounts several times a day (e.g. email account, social media account, e-commerce). For many products, though, it is not so important to uniquely identify and securely authenticate users, so it is often the case that proprietary access data based on a username and password are granted which can be immediately replaced in the event of loss. Providers may see this as a feasible way forward, but the drawback for users is that private password management becomes more unwieldy and cumbersome over time, which can sometimes also be to the detriment of security. This might present providers of services with no particular security level with another field of application for universal eID solutions as a replacement for single sign-on services, allowing them to overcome their customers' increasing reluctance to acquire and store additional login data.

Potential additional services for payments

Another step that might help eID solutions become commonplace in the world of payments would be to add suitable services tailored to payments. Automatically transferring the necessary payment data and invoice and delivery address information at the buyer's request when their identity is verified at the e-commerce checkout or directly importing the IBAN when SEPA direct debit mandates issued online are authenticated voluntarily are elements which could be decisive in this regard. The possibility of creating (qualified) electronic signatures in combination with eID solutions could additionally boost the relevance of eID solutions for some of the potential areas of application outlined in Chapter 4.

eID solutions at public authorities as a potential catalyst for wider use

As processes increasingly go digital, public authorities are coming under mounting pressure to offer electronic public services that allow identification and authentication as well as, for some services, the submission of legally binding declarations of intent to be carried out electronically. Furthermore, the Online Access Act stipulates that, by 2022, central, state and local governments must offer the option of using all public services online and link the administrative portals of central and state governments in a portal network.

On top of this, since 29 September 2018 all EU Member States have been required, under the eIDAS Regulation, to open their own administrative procedures to notified eIDs from other Member States if their own administrative procedures require electronic identification at assurance level substantial or high.

In this context, central, state and local governments are stepping up their efforts to expand the public authorities' range of online services. For this purpose, too, the requirements for using the identity card's electronic ID function have been made much simpler (see Section 5.1). Furthermore, citizen and corporate accounts are being developed that enable access to public services at all three assurance levels (high, substantial, low) following primary identification.

The greater use of eIDs in electronic administrative procedures could make eIDs a more important part of people's day-to-day lives and thereby act as a catalyst for the wider deployment of eID solutions in the private sector as well. It should therefore be checked to see whether the newly established citizen and corporate accounts could, in future, also be made available for accessing associated non-public services and whether in turn certain public services could also be used with private eID solutions.

6.2 Obstacles to the widespread and consistent use of the German identity card's electronic ID function

One reason for the poor take-up so far of the electronic ID function is that this function is currently only activated for only around 42% of identity card holders. It can be assumed, however, that this percentage will increase to approximately 60% by the end of 2020 due to the function being activated by default on identity cards issued as of July 2017. This would mean the number of identity cards in circulation with the electronic ID function activated would then be substantial at around 36 million identity cards, while roughly 25 million cards would not have an activated electronic ID function. However, it would be wrong to idly wait until all the identity cards issued up to July 2017 with the electronic ID function deactivated are routinely replaced by identity cards with this function activated by mid-2027 if the aim is to promote the cards' use in digital transactions as soon as possible. Instead, members of the public should be encouraged to have their previously deactivated electronic ID function reactivated. This is the only way to ensure that identity cards across Germany are equipped with the electronic ID function as quickly as possible.

Activating disabled electronic ID functions is proving to be a relatively time-consuming task, and identity card holders are charged a fee for this service,[49] which means that a significant number of reactivations cannot be expected without some supporting measures.

Furthermore, some members of the public are still unaware of the options and attractions of using the electronic ID function that are already available. The first time they see their identity card is usually in municipal administration offices, so this is an especially important opportunity to explain the possible applications of the electronic ID function.

The initial need to use a dedicated terminal to read the identity card data – seen by many as a very complicated procedure – is another factor which has undoubtedly impeded the take-up of the identity card's electronic ID function. Thus, the option of using NFC-enabled smartphones to read the data on the identity card's chip (see Section 5.1), which has been available for a couple of years now, is an extremely important step towards increasing the function's user-friendliness. Whilst it was previously not possible to use the electronic ID function with an iPhone, the unlocking of this device's NFC interface[50] at the end of September this year is likely to make it noticeably easier for this user group to use the electronic ID function.

However, even if the electronic ID function can be accessed with a smartphone, the identity card's relevance for many potential use cases is still curtailed by the fact that, in order to read the data on the identity card's chip, the user needs to handle the identity card and the smartphone (positioning the identity card chip close to the smartphone's NFC interface) whilst also opening the eID application or the "AusweisApp" on the smartphone's screen at the same time.

Although this relatively fiddly procedure using an additional hardware component (identity card chip) is designed to ensure the solution's technical security, it still reduces the attractiveness of using the identity card for a large number of everyday applications for which a somewhat lower level of security employing simpler procedures would be sufficient. In this case, eID solutions which do not use an additional hardware component – potentially at the cost of reduced technical security – but which store the necessary data in a secure location directly on the smartphone, for instance, could be at an advantage due to simpler and quicker usability.

For this reason, the aim for identity cards, too, is to transfer the chip cryptography from the card chip into a secure element on the smartphone (eSIM, eIUCC) so that this element can be used independently as an eID client or even as an NFC token at a terminal.

Beyond these technical enhancements to the identity card, the creation of further specific use cases for the electronic ID function in public authorities and by private sector service providers is a key success factor in ensuring the widespread use of the electronic ID function in many everyday applications.

6.3 Obstacles to the use of eID solutions not based on the identity card's electronic ID function

The statutory and supervisory provisions governing the vast majority of use cases outlined in Chapter 4 grant private sector players a relatively high degree of leeway in terms of which specific technical solutions they wish to use. In theory, this allows for the

49 The electronic ID function can only be reactivated using special hardware at the municipal administration office and this process costs members of the public €6. Although this fee is comparable to others in similar contexts, it may still be an extra obstacle for members of the public to have their electronic ID function reactivated.
50 See https://www.personalausweisportal.de/SharedDocs/Kurzmeldungen/DE/2019/Online_Ausweisen_bald_mit_IPhone.html

use of many different eID solutions. One exception to this is identification in conformity with the Money Laundering Act (see Section 4.1).

Identification in conformity with the Money Laundering Act is not straightforward for eID solution providers that do not use the electronic ID function or any of the other procedures named explicitly in the Money Laundering Act. This basically leaves just two options for these providers. First, the Money Laundering Act, specifically Section 17, generally allows due diligence requirements to also be performed by "third parties" (pursuant to Section 17(1) Nos 1-3 of the Money Laundering Act) and other suitable persons and companies that eID solution providers may engage as they see fit. Performance of these due diligence requirements by third parties is subject to strict provisions, however.[51]

Second, the Money Laundering Act also permits disclosure of an identification dataset collected at an earlier point in time, although this only applies to disclosure between two obliged entities under the Money Laundering Act.[52] The option of disclosing identification data in conformity with the Money Laundering Act to obliged entities under the Money Laundering Act thus effectively remains reserved to eID solution providers that are themselves obliged entities under the Money Laundering Act.

Section 8.4 of BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act makes it clear, furthermore, that such disclosure of identification datasets is subject to a series of additional preconditions. For example, identification datasets recorded at an earlier point in time may only be used in this manner by the third parties[53] which performed the initial identification, the data must have been collected within the past 24 months, and their origin must be documented. Section 8.4 of BaFin's Interpretation and Application Guidance outlines a number of other requirements.[54]

Also, possible recourse to identification using a QES (together with a reference credit transfer) as explicitly permitted by the Money Laundering Act is made more difficult in practice by the fact that, in this case, the transaction needs to be made from a suitable bank account for the purpose of additional identity verification (more information on this can be found in Section 12(1) sentence 2 et seq. of the Money Laundering Act).[55]

---

51 The provisions on outsourcing due diligence requirements under the Money Laundering Act, including customer identity verification, are governed by Section 17 of the Money Laundering Act and outlined in greater detail in Section 8 of BaFin's Interpretation and Application Guidance. Only those suitable obliged entities named in the exhaustive list under Section 17(1) Nos 1-3 of the Money Laundering Act who are themselves obliged under the Money Laundering Act qualify as a "third party". Whilst obliged entities under the Money Laundering Act may engage "third parties" without a separate contractual basis, outsourcing to other suitable persons and companies requires an outsourcing agreement and is only possible subject to the conditions set out in Section 17(5)-(9) of the Money Laundering Act.

52 Further information on this topic can be found in Section 8.4 of BaFin's Interpretation and Application Guidance to the German Money Laundering Act.

53 "Third parties" pursuant to Section 17(1), (2) and (4) with the exception of member organisations or associations (Section 17(1) No 3 first alternative of the Money Laundering Act). Further information on this can be found in Section 8.4 of BaFin's Interpretation and Application Guidance.

54 According to Section 8.4 of BaFin's Interpretation and Application Guidance, amongst other requirements, the third party (within the meaning of Section 17(1) Nos 1-3 of the Money Laundering Act) must have collected the data of the contracting party in order to establish a separate business relationship within the meaning of Section 1(4) of the Money Laundering Act in accordance with anti-money laundering regulations. Disclosure of data collected on the basis of simplified due diligence requirements is not permitted. Furthermore, at the time of use of the identification data, the validity date of the identification document may not yet have expired, and the obliged entity must be notified of the date of "initial identification".

55 The Federal Office for Information Security notes in this respect that using a QES for identification cannot be distinguished technically from using a QES to issue a declaration of intent. As a result, the Federal Office for Information Security cautions that particular care should be taken when using a QES for the purposes of identification in order to avoid undesirable side effects such as the initiation of unintended legal consequences. More information on this topic can be found inter alia in Technical Guideline TR-03107-1 "Electronic Identities and Trust Services in E-Government", Section 2.2, p. 10.

As described in Section 6.1, the ability to use eID solutions in as many different situations as possible is key to their success. If individual eID solutions are partially or entirely unsuited for identification in conformity with the Money Laundering Act, this could therefore be a major obstacle to their widespread use, including for use cases beyond the scope of the Money Laundering Act.

Comparison of the chief characteristics of the electronic ID function of the German identity card and other relevant eID Figure 4

eID solution	Usability for identification in conformity with the Money Laundering Act	EU-wide usability	Coverage of many and varied use cases	Major obstacles to successful implementation
Electronic ID function of the German identity card	Use explicitly envisaged in the Money Laundering Act. Unrestricted usability.	Notification to the European Commission and connection to the eIDAS interoperability framework form the basis for EU-wide usability in public administrative procedures. The eIDAS interoperability framework can, in principle, also be used for private sector purposes.	A broad spectrum of different use cases can be covered in principle. Use as the basis for QES and for initiating payment transactions technically possible. Given the electronic ID function on identity cards, electronic residence permits, and eID cards for EU citizens, combined with the eIDAS-eID framework, customer coverage in Germany and the EU is very high, in principle, in terms of final users. In practice, however, the electronic ID function has not come into play, particularly for use cases where security requirements are relatively low. Not possible at present to transfer additional data such as payment information or a delivery address.	Relatively limited usage to date ("chicken-and-egg problem"). Drive to create concrete use cases is therefore a key factor for success. Electronic ID function currently deactivated for many people. Reactivating this function or activating it for the first time is relatively time-consuming for citizens (only possible at municipal administration offices for a fee). Identification and authentication at the highest security level require additional hardware and/or software. This may limit the solution's attractiveness for everyday applications with relatively low security requirements. Lower flexibility in terms of adapting to market needs could make the solution less attractive for some private sector uses.

eID solution	Usability for identification in conformity with the Money Laundering Act	EU-wide usability	Coverage of many and varied use cases	Major obstacles to successful implementation
Other relevant eID solutions	Disclosure of recorded identities for the purpose of identification in conformity with the Money Laundering Act in the case of third parties is only possible under the conditions listed in Section 6.3. Reliable initial identification in conformity with the Money Laundering Act ("enrolment"; see Section 5.2) particularly important here.	To date, none of the private sector solutions found on the market has been notified in accordance with the eIDAS Regulation. Looking ahead, then, EU-wide usability could be seen as a challenge. For eID broker solutions which use the identity data collected by ASPSPs, a SEPA API access scheme may yield opportunities for EU-wide interoperability above and beyond the eIDAS interoperability framework (see the box entitled "Cross-border use of eID solutions").	A wide variety of different use cases are covered in principle. Use as the basis for QES and for initiating payment transactions generally possible. Individual solutions offer use-adapted security demands for authentication. Additional data can, in principle, be added relatively easily at the customer's request. This makes such solutions more user-friendly and relevant for everyday situations. Identification in conformity with the Money Laundering Act only possible subject to certain conditions (see Section 6.3).	Relatively limited usage to date ("chicken-and-egg problem"). Problems facing solutions that use online banking access data reduced, however. Drive to create wide variety of use cases is a key factor for success. Possible lack of suitability for identification in conformity with the Money Laundering Act restricts scope of use and thus validity as a "universal eID solution".

6.4 Further challenges and potential unwelcome developments

Individual members of the working group indicated that a lack of innovative momentum in public procedures could present another significant challenge to the successful establishment of suitable eID procedures in Germany, and called for an approach that was not solely focused on public procedures. Rather, they felt, the establishment of suitable private eID solutions also deserved support so that their innovative power could be harnessed for the German market, thus potentially enabling a broader spectrum of possible uses to be covered.

It was also noted that the ability to map out all the relevant business processes digitally was essential for the successful digitalisation of business relations. For instance, legal requirements should generally be assessed on whether and how they could also be implemented into digital transactions meaningfully and in a manner suited to everyday use.

Aside from this, many of the private sector representatives in the working group saw a major problem in the differing requirements for the technical and organisational security of the underlying processes for trust services between individual EU Member States, especially in terms of the QES, which is of particular relevance to the working group. One major point raised in this regard concerned a decision by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway in June 2018,[56] which

56 See Decision of the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, Notice No 208/2018, p. 931, available at https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/VerfügungIdentmethoden/Erstverfuegung2018.pdf?__blob=publicationFile&v=4

restricts authorisation of the video identification procedure to the creation of single-use certificates. Whilst in several other EU Member States, identities recorded by video identification procedures could be used multiple times to create a QES, in Germany this is reportedly confined to the issuance of ad hoc certificates for one-time use. This, it was said, is disrupting the level playing field between qualified trust service providers within the EU.[57] It has been observed that (qualified) trust service providers are migrating abroad, or that German enterprises are preferring to have trust services issued by foreign providers in order to then use them in Germany for purposes including identification in accordance with Section 12(1) No 3 of the Money Laundering Act. This, it was reported, is undesirable for the development of the nascent sector of German and European identity service providers.

Differences between the requirements laid down in the anti-money laundering legislation of individual Member States for eIDs may pose an additional challenge to the EU-wide usability of eIDs. Given the lack of standardisation, and country-specific requirements and interpretations of eID and anti-money laundering provisions, it is barely feasible, as things currently stand, to implement eID solutions across the EU, the working group heard. A European Commission expert group is currently examining this issue, and aims to simplify cross-border electronic identification within the EU[58] (see the box entitled "Cross-border use of eID solutions").

Moreover, although technical interoperability of national eID solutions is supported by the eIDAS interoperability framework, this only applies to identification schemes notified to the European Commission, meaning that private sector eID solutions in Germany have been unable to take advantage of the framework thus far. Although notification of private sector identification schemes is fundamentally possible, it is subject to a series of requirements.[59] In practice, such requirements could present decisive obstacles for private sector eID solution providers notifying their own schemes. Individual members of the working group therefore see a danger that the market needs of the business community for cross-border identification are not being adequately considered.

As it can also be assumed that demand for eID solutions that are suitable for everyday use will continue to rise, including across borders, this could strengthen the market position of global tech players like Facebook, Google and Amazon. These firms already offer their customers highly accessible eID solutions which are not confined to national markets. For the most part, the solutions on offer to date are limited to use cases with relatively low security requirements, but it is likely that more will be added to the range. If corporate groups from outside Europe come to assume a dominant market position in the key field of eID solutions, this might not only call into question the "digital sovereignty" of Germany and the EU, but also be a concern from a data protection perspective on account of the data-based business models which these groups run.

Interoperability between the different private sector eID solutions – a factor which cannot be fathomed at present, not least at a national level – might be another unwelcome development which may, in future, result in a fragmentation of the German eID solutions market. Looking to the future, a situation

57 See, for example, Bitkom's statement on this topic from May 2018, which refers to a draft version of the Federal Network Agency's decision: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Position-zum-Videoidentverfahren-als-national-anerkannte-Identifikationsmethode.html

58 More detailed information on the Commission expert group on electronic identification and remote know-your-customer processes can be found at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3571&NewSearch=1&NewSearch=1

59 One reason why the requirements are relatively strict is the mandatory recognition of notified identification schemes by public sector bodies of other Member States and the assumption of (co-) liability for notified schemes by the notifying Member State.

where people are forced to use a variety of different eID solutions at assurance level substantial or high in their day-to-day lives, though unforeseeable at the current juncture, should be avoided in the interests of user-friendliness.

On the other hand, however, insufficient interoperability between eID solutions may also result in a single private sector solution gaining the upper hand and other solution providers being crowded out of the market amid intense network effects, producing a private monopoly in the market. In the interests of both society and the national economy, a situation where the German market is heavily reliant on a single private sector eID solutions provider should be avoided. The majority view among the members of the working group, however, was that unwelcome developments such as these were not foreseeable at the current juncture, and that priority should be given to establishing suitable eID solutions in the German market in the first place. That being said, the question of the interoperability of eID solutions ought to be borne in mind nonetheless, both at the national level and across the EU.

Public initiatives such as the further development of the electronic ID function, and, in particular, the creation of an open mobile eID ecosystem (see the OPTIMOS 2.0 project and the "Schaufenster Sichere Digitale Identitäten" innovation competition[60]), as well as considerations to open up public sector citizen and corporate accounts for private sector purposes, thus represent very welcome measures. This is because they could provide people with an alternative to private eID solutions in private sector use cases as well and thus create a balance in the event of unwelcome market developments. Furthermore, they currently also appear to be better suited to ensuring EU-wide interoperability.

60 https://www.digitale-technologien.de/DT/Navigation/DE/Foerderaufrufe/Sichere_Digitale_Identitaeten/sichere_digitale_identitaeten.html

Cross-border use of eID solutions

The cross-border usability of eID solutions is an important prerequisite for the efficient and convenient handling of digital administrative procedures and business processes in the EU.

The eIDAS interoperability framework requires the recognition of national eID schemes notified to the European Commission by public sector bodies in all Member States and offers the technical infrastructure necessary to make these schemes interoperable (see Section 3.3). Despite its primary focus on administrative procedures, the eIDAS network is also open to the private sector. First, private online service providers can connect to the network to enable simple digital identification for customers from other EU countries as well. Second, private eID solution providers can put their eID schemes forward for notification so as to achieve binding recognition of their eID solutions by public authorities within the EU Member States and potentially facilitate their acceptance outside administrative procedures as well. The eIDAS interoperability framework is therefore an important building block for the cross-border use of eID solutions in the EU.

Another opportunity to create a standardised eID solution that can be rolled out across Europe may lie in the work currently being conducted by a working group set up by the Euro Retail Payments Board[61] to develop a SEPA API access scheme. Such an API scheme would establish common rules and technical standards for participating payment service providers on the use of customer data via APIs. In addition to the initiation of payments, it could also be used by ASPSPs to confirm customers' identities to third parties. This would be subject to the customer wishing to be verified to third parties and authenticating themselves using their means of access for online banking.

Besides technical interoperability, however, divergent anti-money laundering rules represent a further major obstacle to the cross-border use of eID solutions in the European financial sector. For instance, it may be the case that eID procedures permitted in one Member State cannot be used in another Member State because, by way of example, they do not satisfy the local legal requirements governing identity verification. The further harmonisation of anti-money laundering rules in the EU is therefore an essential prerequisite for the cross-border use of eIDs in the European financial sector and for the successful continued integration of the digital single market for financial services. The expert group on electronic identification and remote know-your-customer processes[62] set up by the European Commission aims, inter alia, to draw up proposals for a future European framework to meet anti-money laundering due diligence requirements by the end of 2019.

A great deal of importance is likely to be attached to the targeted implementation of these recommendations.

The topic of eIDs is also being explored by the Financial Action Task Force (FATF), which sets international standards for combatting money laundering and the financing of terrorism. The FATF is currently developing international guidelines for the use of eIDs in the financial sector.

---

61 The Euro Retail Payments Board (ERPB), chaired by the ECB, is tasked with fostering the integration, innovation and competitiveness of euro retail payments in the European Union. The ERPB replaced the SEPA Council in 2014 and comprises seven associations on the demand side and supply side of the European retail payments market, respectively. They are joined by five representatives of the national central banks of the euro area and one representative from the national central banks of the non-euro area EU Member States. More information is available at https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html

62 For more detailed information, see https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3571&NewSearch=1&NewSear ch=1

7 Recommendations for action

Promote market dynamics: general openness to eID solutions

The aim of the eID working group is to drive forward digitalisation in the field of cashless payments and make the seamless provision of online-based payment services a reality. To achieve this, it needs to be possible to accomplish two tasks online: first, user-friendly, secure payment authentication and authorisation, and second, first-time identification in conformity with the law upon commencement of a business relationship with a payment service provider. This requires the further development and establishment of marketable eID solutions that enjoy a high level of customer acceptance, e.g. by covering a broad range of applications. The German identity card's electronic ID function stands it in good stead, because it is a special case as a public solution and other eID solutions can be based on it. However, it does not currently meet all of the market requirements for the various applications that have been identified, and little use has thus far been made of it in practice.

Given that neither public nor private eID solutions are widely accepted in Germany as of yet, the eID working group expressly welcomes viable private sector approaches to using eIDs besides the identity card's electronic ID function. To this end, the legal framework needs to be open to accommodating new technologies. At the European level, too, the availability of interoperable eID solutions in all Member States, as well as their cross-border usability and interoperability, ought to be facilitated. It is only in this way that a single market in this area can emerge.

Requirements for the active use of the identity card's electronic ID function

Identity cards have been issued with an electronic ID function since 2010. However, it will be 2027 at the earliest before all German citizens possess an identity card with an activated electronic ID function, as many of the identity cards issued up to July 2017 have this function deactivated.

Furthermore, the electronic ID function has thus far had comparatively few specific use cases, which has substantially diminished how relevant it is to the general public in their daily lives.

In order to encourage use of the electronic ID function and ensure widespread availability to the general public prior to 2027, the process of activating the identity card's deactivated electronic ID function needs to be simplified. To this end, it would be necessary to explore ways in which the general public can be motivated to activate the deactivated electronic ID function and whether, if need be, it would be possible to entrust additional bodies with the task of reactivation. In addition, the fee for reactivating this function could be abolished. Reactivation of the electronic ID function should be coupled with a broad-based publicly financed information campaign publicising the identity card's online and offline applications. It is also important, in the near term, to expand the range of specific use cases for the electronic ID function in administrative procedures and, wherever possible, in private sector applications so as to make the electronic ID function more relevant in people's everyday lives.

Open systems for the use of eID solutions on smartphones

Smartphones play a prominent role with respect to the simple, user-friendly use of eID solutions in daily life. ***Regulatory and supervisory bodies should therefore press for the establishment of open systems and interfaces for the use of secure and user-friendly eID solutions on smartphones and ensure a level playing field.***

Expand electronic identification procedures in conformity with the law

The Money Laundering Act governs the analogue and electronic customer identification processes that may be used by obliged entities pursuant to the Money Laundering Act. The current dialogue between BaFin and the obliged entities with respect to a practicable application of the regulatory requirements – taking into account the specifics set out in Section 8.4 of BaFin's Interpretation and Application Guidance in relation to the German Money Laundering Act of December 2018 – should be continued ***in order to facilitate the use of electronic identification procedures found on the market without jeopardising the integrity of the financial system or domestic security.***

Increase cooperation between the private and public sectors in identifying users of private and public online services

In order to make online applications more secure and ensure that eID solutions are as relevant as possible in people's daily lives, every effort should be made to increase cooperation between the private and public sectors in identifying the users of private and public online services.

In particular, the private sector and public authorities should work together to explore whether and under what conditions, from a security and data protection perspective, especially, private eID solutions could also be used to provide access to public authorities' online services and, conversely, public user accounts on the portal network linking central, state and local government portals ("citizen and corporate accounts") could be used to provide access to private sector online services. ***In this context, it should be checked to see whether the current approval procedures for private eID providers accessing public authorities' services could be simplified.***

The factor offering the greatest potential in the public sector is the digitalisation of corporate enquiries, as these are received much more frequently than citizens' enquiries. Uniform rules or standards for creating a digital corporate identity online and specifying authorised persons are not yet in place, however – it would make sense to establish guidelines for standardisation based on market participants' initial experience in order to generate solutions that can be applied nationwide and to accelerate implementation.

Review legal provisions with respect to everyday implementability in digital processes

In order to fully exploit the added value of using eID solutions in digital business relationships, it is particularly important that, going beyond payment transactions and identity verification, all other relevant business processes can also be carried out digitally. ***In order to promote the use of eID solutions and the continued successful digitalisation of business relationships, legal requirements should therefore, as a rule, be examined as to whether and how they could be sensibly implemented in digital transactions in a manner that is suitable for everyday use.***

Commit to an EU-wide level playing field for the use of eID solutions in customer onboarding and the provision of trust services

In accordance with the eIDAS Regulation, qualified trust service providers from other EU countries may provide their eIDAS-compliant trust services in Germany, just as German providers may operate in other EU countries. As a rule, therefore, the same requirements should also apply to all trust service providers in the EU.[63] However, it would appear that the European level playing field that is actually intended is not always guaranteed in practice. For example, market participants report significantly more stringent German requirements for the provision of trust services, particularly for the QESs that are also relevant to the use cases presented in this report (see Section 6.4). They report that trust service providers are migrating abroad and German firms are preferring to employ foreign providers to render trust services in order to use them in Germany for purposes including identification in conformity with the Money Laundering Act.

Market participants also point to differences between individual Member States in terms of the anti-money laundering rules for eIDs. In addition to being a concern from a competition perspective, this poses a serious challenge to the EU-wide usability of electronic identification means. These private sector assessments need to be followed up on at the national and European level, and appropriate solutions need to be found. ***Initiatives launched at the EU level to standardise the framework conditions for electronic identification and the provision of trust services pursuant to anti-money laundering legislation should be pursued with the objective of establishing EU-wide harmonised standards that enable the secure and user-friendly use of eIDs and trust services in the EU-wide financial sector and preserve the European level playing field.***

Simplify notification under eIDAS for private eID solutions

In addition to EU Member States' divergent requirements for identification under anti-money laundering legislation described above, the frequent lack of technical interoperability also presents a challenge to the cross-border use of eID solutions. Taking the approach of establishing an interoperability framework by means of eIDAS for national eID solutions notified to the European Commission is an important step in this regard. The barriers to notification pursuant to eIDAS are, however, seen as very high by parts of the private sector, and some of these barriers are reportedly higher in Germany than in other EU Member States. ***In order to make it possible for the eIDAS inter-operability framework, which was originally designed for public administrative procedures, to also play an instrumental part in deepening the digital single market, the issue of whether private sector concerns could be taken into account to a greater extent and the requirements simplified for notification of private eID solutions in line with EU-wide rules should be examined.***

63 The requirements set out in the eIDAS Regulation concerning trust services – unlike the directly applicable provisions governing the cross-border use of identification schemes in administration – need to be transposed by national legislators into national law. In Germany, the national law is the Trust Services Act.