31 July 2018

## BUSINESS PROPOSITION OF EIDAS-BASED EID

# Banking sector

**Value Proposition of eIDAS-based eID**

CEF eID SMO

Version 1.0

European Commission

**This study was carried out for the European Commission by Deloitte.**

**Internal identification**

Framework Contract BUDG16/PO/01 (DIMOS IV Lot 1)

COM/DIGIT.D3/2017/01-035

## DISCLAIMER

By the European Commission, Directorate General for Informatics.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

# Introduction

# 01

The objective of this paper is to provide an analysis of the potential reuse of eIDAS-based eID in the banking sector.

Over the past year, the European Commission has been exploring how electronic identification under eIDAS could be leveraged by the banking sector to comply with Know-Your-Customers' requirements under the fourth Anti-Money Laundering directive (4th AMLD) and to guarantee strong authentication requirements of parties in the context of the revised Payment Services Directive (PSD2).

In parallel, banks are playing an increasing role as identity providers of electronic identity. The regulatory obligations and security needs to which they are subject in terms of identity verification have placed banks and financial institutions in a strategic position. More and more institutions are exploring how they could leverage the procedures that they have put in place to verify customers' identity for other parties, acting as identity providers.

eIDAS-based eIDs offer the possibility to provide a strong authentication of users (natural and legal persons), based on ID information endorsed by governmental authorities across Europe.

We have therefore identified two use cases to be explored in this paper:

- Banks as service providers - Identification of customers for Know-your-Customer (KYC) purposes under the Anti-Money Laundering and Payment Service Directives
- Banks as identity providers – Provision of eIDAS verified digital identities

More precisely, this paper aims at:

- Understanding how the banking sector can leverage eIDAS-based eIDs as service providers and as identity providers;
- For each use case:
  - Understanding the needs of banks and the regulatory requirements to which they are subject;
  - Identifying the key challenges faced by banks and financial institutions regarding the current processes;
  - Exploring how eIDAS-based eID could add value to the existing identification process, as well as possible limiting factors to this;
  - Recommending key steps to envisage a reuse of eIDAS-based eID in the specific use case;
- Drawing conclusions on the business proposition of eIDAS-based eID in the banking sector.

In order to better understand the opportunities and challenges of the sector regarding customer identification, six interviews with banks and financial institutions were conducted between February and April 2018. The analysis was complemented by desk research.

# What is eIDAS-based eID?

# 02

EU Member States are currently supporting the uptake of electronic identification (eID) to enable secure and seamless electronic interactions between businesses, citizens and public authorities, within the context of the eIDAS Regulation (EU 910/2014).[1] Member States' commitment on ensuring the implementation of the eIDAS Regulation was also reflected in the Tallinn Declaration on eGovernment[2].

Electronic identification is the process for a person or business to prove who they claim to be in an online environment. Information is shared thanks to an eID means containing the identification data, usually taking the form of a smartcard, an identifier/password system or a mobile app. Over the past decades, EU/EEA countries have been providing to their citizens these types of solution, mainly to access eGovernment services (e.g. declare tax online).

The eIDAS Regulation foresees that if an EU/EEA Member State offers an online public service to citizens/businesses for which access is granted based on an electronic identification scheme, then they must also recognise the notified eIDs[3] of other Member States as from 29 September 2018 for the purposes of cross-border authentication for that service online.

Although, the main focus of the Regulation is to grant access to online public services cross-border, Member States are also encouraged to support the voluntary reuse of eIDAS-based eIDs by the private sector[4]. Each Member State remains free to set the conditions for the reuse of its national eIDAS infrastructure by the private sector and the sharing of the minimum data set of its national eID scheme with private service providers.

[1] 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, see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[2] Tallinn Declaration on eGovernment, signed at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017.

[3] By notified eIDs, we mean all eID schemes that have completed the notification process. The notification process refers to the selection, peer review and official addition of national eID schemes to the eIDAS Network. Notification ensures that the eID schemes connected to the eIDAS Network satisfy the conditions of quality and security set out by the eIDAS Regulation.

[4] Recital 17 of the eIDAS Regulation.

# Key trends regarding identification in the banking sector

# 03

Electronic transactions are booming in the banking and financial sector. According to the ECB, the importance of paper-based transactions is decreasing steadily, currently representing only one out of nine transactions in Europe.[5] Securing electronic transactions and guaranteeing a strong identification of parties on a remote basis has therefore become crucial for banks. More and more resources are being dedicated to improving online onboarding processes, and the number of local branches of European banks are being reduced. In 2016, 9,100 local branches were closed and staff reduction represented 50,000 positions.[6]

## Remote visual onboarding associated to biometrics

For many years, banks have been obligated to introduce processes aimed at performing identity proofing and verification. This consists of verifying whether the person requesting the service is who they claim to be, and collecting some key ID information for anti-money laundering and risk assessment purposes (e.g. ability to pay back, fraud). This process typically involves a bank agent verifying manually the ID document provided by the new potential customer.

With the development of online banking, banks have developed solutions based on video-conferencing systems to perform identity checks for Know-your-Customer purposes. However, the conditions for performing such remote controls rely on the provision of each national anti-money laundering regulation.

[5] ECB, Payments statistics for 2016, September 2017, https://www.ecb.europa.eu/press/pdf/pis/pis2016.pdf?be9989f6bd72483ebe27d8dfae1f0362

[6] https://www.reuters.com/article/us-europe-banks-closures/eu-banks-close-branches-cut-jobs-as-customers-go-online-idUSKCN1BN2BV

There are different levels of remote video-conferencing systems:

- Connection with a trained human operator who performs the same type of test that he/she would in a local branch;
- Connection with a trained human operator assisted by some degree of technology: e.g. a detection system for forged documents, facial recognition comparing the customer's face to the ID picture;
- Automated system without a human presence, which makes a risk assessment based on different technologies.

In some countries, video-conferencing is not allowed. In others it is allowed on the condition that there is a human presence assisting with the verification.

In Germany, banks can for example develop video-conferencing systems which integrate a human operator.[7] In Spain, the SEPBLAC authorization allows, since March 2016, banks to use video-conferencing systems to verify the identity of clients for Know-your-Customer (KYC) purposes, allowing for complete online onboarding of new customers.[8]

This type of solution requires the presence of trained operators that must be available 24/7 to avoid service disruption. This constraint means that either high costs fall on the banks to make this service available 24/7 or that the service may result in lengthy procedure when compared to current state of the art user experience for online services. Additionally, there are still risks associated with the capacity of the operator to effectively detect forged ID documents and match the person to their documentation.

Hence, banks are exploring how to further secure the system by completing the human interaction with supporting detection technologies and even completely automate the onboarding procedure without any human interaction. Some of the solutions currently investigated are automated biometric face recognition integrated with the video-conferencing systems that would compare the ID document picture to the face of the customer, as well as automated forged document detectors, allowing operators to make a better assessment of the risks linked to the authentication. Another solution would be to provide a strong authentication of users thanks to their eIDAS-based eIDs (cf. next chapter).

## Private sector led Single Sign-On and mobile IDs

Banks and financial institutions are offering their services in a highly competitive environment. Good user experience of their services is therefore crucial to attract and retain customers.

Recent research by Signicat, an identity provider, has shown that 40% of consumers abandon a banking onboarding process due to excessive time needed to complete the onboarding process and the necessity to provide supporting personal information.[9]

Mobile banking is one of the most striking transformations: in the US "[43%] of all mobile phone owners with a bank account had used mobile banking in [2016], up from 39 percent in 2014 and 33 percent in 2013".[10]

Proving one's identity remains a challenge and a burdensome process when the level of assurance requested is high. As a consequence, banks are exploring solutions that would require the lowest effort possible from customers.

One of the first solutions has been to develop Single-Sign-On solutions for the banking sector. At the moment, Google and Facebook solutions are leading the market. However, these solutions are based on self-declared identities that are not verified to the standards requested by banks and other financial institutions.

Recent initiatives have therefore emerged to provide SSO solutions to big European companies based on the concept of derived identity, allowing for stronger assurance on the ID information shared as part of this solution and the authentication process. Derived identities are based on a primary identity that has been issued based on a physical breeder document (e.g. birth certificate). National ID cards and passports are considered strong primary identities, since they are based on thorough identity proofing procedures involving the physical presence of the person. The derived identity created on top of the primary identity can be more user friendly and offer more functionalities (e.g. Facial recognition, mobile digital identity, cloud solution) while benefiting from the security and assurance provided by the primary identity.

One of these initiatives is Verimi,[11] an identity platform that has succeeded in partnering with strong economic German actors such as Lufthansa, Deutsche Bank, Deutsche Telecom, Allianz, Daimler, etc. The solution gives the possibility to store the derived identity of personal-related data from various official documents (e.g. Passport, ID, driving license) and reuse it to prove one's identity online, while ensuring a smooth user experience.

[7] Example of videoconferencing systems in Germany: https://www.targobank.de/service/videoidentifikation/index.html

[8] https://www.icarvision.com/en/banks-and-digital-transformation--sepblac-authorizes-the-identification-of-clients-by-videoconferencing

[9] Signicat, The Rise Of Digital Identities: Plugging the 'digital gap' in financial services onboarding, https://www.signicat.com/wp-content/whitepapers/signicat-AML-white-paper.pdf

[10] https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf

Signicat's IDAaaS technology is giving financial service providers and e-commerce businesses the ability to verify new customer identities using electronic identity (eID) and digital verification of paper ID. IDAaaS also enables them to take advantage of a range of other solutions such as facial recognition.[12]

The advantage of Single Sign-on solution is the mutualisation of the identity proofing procedure that can otherwise be burdensome and costly for banks and other companies requested to provide KYC controls. However, national regulations are still in some cases hampering banks seeking to reuse identity verification processes performed by other actors. Legislation will therefore have to evaluate whether this type of practice constitutes a real advancement for users and banks.

## Encryption of identity data associated with blockchain technology

Banks are interested in the encryption aspect of blockchain technology. Banks are processing an important amount of personal data from their customers and counterparties. Protecting this information from malicious intent is becoming more expensive every year considering the increasing cyber threat and the amount of information collected on individuals and organisations.

Blockchain and encryption have caught the interest of banks as a way to improve identity management and offer secure digital identity storage. Encryption allows for a digital version of a personal safety deposit box in a bank where the accumulation of keys and protections guarantees a high level of protection of information stored in the vault. Blockchain technology introduces the distribution of information in several locations, allowing for a strong protection should one storage facility be compromised.

Key advantages for banks of encrypting personal data and using blockchain technology:

- Avoid single point-of-failure and a massive centralized repository of personal data that presents a target for hacking;
- Allow for a single source of truth: credentials and attributes only have to be changed once in a unique ledger;
- Reduce time needed for KYC and identity verification significantly thanks to the trust introduced by the blockchain technology in the information contained in the ledger;
- Reduce costs and hurdles linked to identity theft.

The market for identity management solutions based on blockchain is relatively new and composed of a multitude of companies. Winners of the competition to lead the market have not yet emerged. Yet, to be truly efficient, blockchain technology requires either a large uptake of a single solution, or more efforts on the interoperability of the different solutions.

Over the past months, some pilots have been announced by major banks to test blockchain technology for payment as well as for clearing and settlement. In the case of identity management the adoption is slower, but more and more projects are expected in the upcoming months. The US bank Capital One has for example recently announced that they were acquiring the digital identity and fraud alert startup Confyrm, providing better protection for customers against fraud and identity theft.[13] IBM and French bank Crédit Mutuel have also recently completed a proof-of-concept based on Hyperledger blockchain, supporting the KYC process and allowing customers to provide proof of identity to third parties, such as local utilities and retailers.[14]

[11] https://verimi.de/en/

[12] https://www.signicat.com/news/signicat-secures-second-round-horizon-2020-funding-develop-id-assurance-service/

[13] https://medium.com/capitalonetech/confyrm-joins-capital-one-to-fuel-consumer-identity-services-at-scale-29307910cc2b

[14] https://www.ibm.com/case-studies/e829728o57617x05

# Banks as service providers: strong authentication of customers

# 04

The main function of banks is to provide financial services to their customers. This section focuses on the key requirements and challenges that banks faces when identifying their customers under a procedure called Know-your-Customer (KYC) and how eIDAS-based eIDs could support it.

## Identification requirements for the banking sector

The identification requirements imposed on the banking sector mainly aim at avoiding fraud and anti-money laundering practice. In order to recoup information and better track suspicious activities, banks have been increasingly requested by public law enforcement authorities to conduct customer identification. Several EU directives are defining key principles linked to customer identification, which are then transposed into 28 national legislations refining the provisions and sanctions applied in case of non-compliance.

## Anti-Money Laundering Directive (4AMLD and 5AMLD)

EU Member States have been introducing procedures to prevent the use of the banking system by criminals and/or terrorists. The European Union has taken strong action in this field and is regularly updating its Anti-Money Laundering Directive. The 4th Anti-Money Laundering Directive (4AMLD), strengthened the requirements for parties making a transaction and/or payment to be properly identified.[15] The 5th Anti-Money Laundering Directive, which amends the 4th



[15] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

Anti-Money Laundering Directive, was published in the Official Journal of the European Union on 19 June 2018. The Member States must transpose this Directive by 10 January 2020.[16]

Article 13 of 4AMLD clearly requests that due diligence be performed for "identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source". The directive also requires the identification of the beneficial owner[17], the obtaining of information on the purpose and intended nature of the business relationship, and scrutiny of the transactions undertaken within the framework of this relationship.

Requirements under 4AMLD have evolved since 3AMLD to integrate key evolutions in the banking and financial sectors linked to remote identity verification based on video-conferencing systems. The Directive has also introduced higher levels of assurance required with regard to the attributes collected about customers, as well as the fines applied in case of non-compliance.

The 5AMLD strengthens anti-money laundering provision. Recital 22 also makes an explicit reference to the use of eIDAS-based eID to perform accurate identification and verification of natural and legal persons. Article 13 of the 4AMLD is amended to specify that eIDAS-based eIDs are recognized as a valid solution to identify customers and obtain ID information about them. Additionally, annex III is modified to recognize eIDAS-based eID as a way to secure non face-to-face business relationships or transactions.[18]

Consequently, the reuse of eIDAS-based eIDs by banks and financial institutions is encouraged to perform the strong identity proofing and authentication required under 5AMLD. The Directive does not prescribe which level of assurance of the eID Schemes is required. The current status quo among the members of the KYC expert group[19] established in Spring 2018 by the European Commission, is that eID schemes qualifying for level substantial and high could be reused. The minimal LoA required would depend on the assessed risk of the customer.

## Payment services directive (PSD2)

The EU Directive no. 2015/2366 on payment services in the internal market (PSD2) requires under article 97 that payment service providers (PSP) apply strong customer authentication. With the exception of low value or repetitive transactions, authentications must be based on two-factor authentication solutions (or more) when the payer "accesses his payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse". [20]

The requirements of the strong customer authentication were developed by the European Banking Authority (EBA) and published in November 2017. The final Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and secure open standards of communication (CSC)[21] will apply as of September 2019 and complement the dispositions of PSD2.

The eIDAS Regulation is mentioned twice in the Delegated Regulation on Regulatory Technical Standards:

- Recital 27 encourages the PSP to take into account eIDAS-based eIDs as a way to improve user confidence and ensure a strong customer authentication (as per article 97 abovementioned);
- Article 34 requires that account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments be able to identify themselves towards the account servicing payment service provider by relying on qualified certificates for electronic seals or website authentication defined under eIDAS.

Although the first element refers to eIDAS-based eIDs, which constitute the focus of this paper and applies to interaction with customers, the second element is referring to the second part of the eIDAS Regulation, which regulates trust services and only concerns professional parties to the transaction.

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.156.01.0043.01.ENG&toc=OJ:L:2018:156:TOC

[17] 'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_72_2017_REV_1&from=EN

[19] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36277&no=1

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

[21] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

Only eIDAS-based eIDs with authentication procedures based on "two or more elements which are categorised as knowledge, possession and inherence"[22] are compliant with PSD2. Under eIDAS, there is an obligation to utilise at least two authentication factors from different categories for eID schemes of LoA substantial or higher. As a consequence, all eID schemes notified under substantial or high level of assurance under eIDAS are automatically compliant with PSD2 to ensure strong customer authentication. Some eID schemes notified as low level of assurance could also be compliant providing that they fulfil the multi-factor authentication criteria described above.[23]

The use of eIDAS-based eIDs to perform strong customer authentication is only a recommendation. PSPs remain free to introduce any other solution that would match the strong authentication requirements as defined by the RTS.

## EU Payment Account Directive (PAD)

The EU Payment account directive has made it compulsory for banks to open their services to legally resident customers applying from another EU country. The implementation of this directive, which entered into force in August 2016, has shown the key limitations of the European banking and financial sector when conducting cross-border identity verification of customers.

To conclude, although eIDAS-based eIDs are recommended both in AML and PSD2 legislations to perform strong customer identification, there is no obligation to reuse this solution. The EU Payment account directive is not referring directly to the eIDAS Regulation but is putting pressure on banks and financial institutions to support the on-boarding of customers located in another Member State, which is one of the use cases supported by eIDAS.

It is actually highly likely that the businesses will implement 5AMLD and PSD2 requirements with different processes. Yet it remains pertinent to analyse the value of reusing eIDAS-based eID for strong authentication of customers, either for KYC in the context of anti-money laundering checks or as part of the securing of electronic payments.

## Current challenges linked to identity verification

Identity proofing procedures are difficult to implement for banks. Some of the key challenges that they are facing are:

- **Cost of the procedure**: identity proofing requires human resources, risk assessment analysis and the development of new technologies to remain up-to-date with the new strategies constantly developed by fraudsters.
- **Cost linked to non-compliance:** both AML and PSD2 legislations request Member states to put in place financial sanctions for non-compliance with the provisions of the national law. Amounts differ between countries. As an example, banks and financial institutions face a fine that must not exceed the double limit of 100 million euros or 10% of their total revenue.[24] Last year, the French administrative authorities (ACPR) condemned a payment institution to pay a fine of €80,000 for non-compliance with some of the AML requirements under French law, notably regarding the duty to verify the identity of its customers.[25]
- **Absence of primary identity documents:** identity proofing procedures are usually based on the verification of a primary identity document issued by a state authority on the basis of a breeder document (e.g. birth certificate). However, in some countries and notably in the UK and Ireland, citizens do not necessarily own such documents and there are no national base registries referencing the identity of national residents. Consequently, banks need to rely on alternative attributes and procedures to obtain some assurance regarding the identity of their customers. In the UK, information about a customer's physical verified address is therefore very important despite the digitisation of transactions.
- **Differences in the KYC procedures defined by national legislations:** the absence of a harmonised approach with regard to the practice of KYC procedures between EEA/EU Members States has a high cost for banks with European activities, as they need to adapt their compliance procedures to 28 local rules instead of applying a pan-European approach. Some restrictive laws with regard to remote on-boarding also limit the ability of banks to offer services across-border, due to the impossibility of performing identity proofing remotely.

[22] Article 4.1 of PSD2 RTS, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

[23] The level of assurance of notified eID schemes under eIDAS is based on an assessment of the reliability and quality not only of the authentication mechanism but also the proofing and ID verification procedure, the entities in charge and the procedure of issuance of the eID means, the authentication mechanism, as well as technical and security specifications. Failure to reach substantial criteria for each elements assessed will automatically result in the classification of the eID scheme as low LoA.
Cf. article 8 of the eIDAS regulation and 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.

[24] https://www.legifrance.gouv.fr/eli/ordonnance/2016/12/1/ECFT1628231R/jo

[25] https://acpr.banque-france.fr/sites/default/files/medias/20170403-decision-sanction-lemon-way.pdf

- **Fight against fin-crime and identity fraud:** banks are facing two common types of fraud regarding identification: individuals using fake identities to create an account in order to access credit (and not reimburse it), and people impersonating real identities to defraud other people.
- **Disruption of the user experience across borders:** Today, the experience of users seeking to move to another country while keeping their bank is still poor. International banks generally still fail to provide a seamless experience to support the mobility of their customers, and local branches usually treat clients arriving from another country as new customers. The identity proofing and verification process has to start from scratch as attributes cannot be shared easily.

## Assessment of the reuse of eIDAS-based eID

Although legislation may be a strong driver for the financial sector to adopt eIDAS-based eID as a mean of strong authentication, both 5AMLD and PSD2 only suggest the use of this specific solution and do not rule out alternatives. The added value of eIDAS-based eID for the banking and financial sector therefore remains to be demonstrated.

This section assesses under which conditions eIDAS-based eID could be used to perform identity proofing and verification. A typical use case that requires Know-your-customer due diligence is the opening of a bank account by a new customer. eIDAS-based eID could be used to support strong authentication of foreign (and national[26]) new customers and allow for the automated transfer of identity attributes from the eIDAS minimum-data set.

To support the analysis, we have taken into account the results of two pilot programs:

- The STORK 2.0 eBanking pilot tested between 2014 and 2016 the possibility to use eIDs to open a bank account in another country and collect key information to perform KYC procedures. The STORK infrastructure was an interoperability system developed prior to the eIDAS Regulation and was an initial attempt to introduce the mutual recognition of eID schemes.[27]
- The CEF Pilot "Opening a Bank Account Across Borders with an EU National Digital Identity" is being implemented by a consortium composed of HSBC, Barclays, Government Digital Service, OT-Morpho, Orange and OIX UK. They investigated the possibility for an EU citizen to open a bank account in the UK using a French digital identity (Mobile Connect) prior to moving to the country. The assumption was made that the French eID scheme would be notified under eIDAS.[28]

Additionally, we have also taken into account the findings of our interviews with representatives of banks and financial institutions, as well as the conclusions of a major study contracted by the European Commission and produced by PwC, in the context of the 4AMLD: "eID and digital onboarding: mapping and analysis of existing onboarding bank practices across the EU."[29] The final version of the 5AMLD adopted in May 2018 have also been integrated to our analysis.

The study differentiates between different concepts contributing to the on-boarding of customer and KYC procedure:

- The verification phase consists in determining whether all the expected requirements to perform KYC are met and can be divided into 3 additional steps:
  - Authenticity check of the documents to determine whether the document can be considered as a trustworthy source of information;
  - Identity check comparing the customer against the ID document produces, usually thanks to the picture provided;
  - Anti-fraud check determining that the person or the ID document is not involved in fraudulent activities.
- The collection phase consists in collecting and documenting the ID attributes.

The two EU legislations requesting strong customer authentication differ in the frequency with which the authentication and level of assurance are requested:

- AML legislation requests a strong authentication of the customer at the time of on-boarding. The ID proofing and attribute collection can be considered as occasional, and can be supported by eID schemes qualifying for a level of assurance substantial or higher depending on the risks presented by the customer.
- PSD2 legislation requests payment providers to use strong authentication of the customers when accessing their services. This process is expected to take place on a daily basis and whenever a payer conducts a transaction. The level of assurance regarding this authentication must be based on a double authentication mechanism, which is one of the element assessed under the peer review procedure of pre-notified eID schemes under eIDAS.

[26] Identification of national new customers does not enter into the scope of the eIDAS regulation. Yet we assume that if Member States allow for the cross-border consumption of identities from the eIDAS network by the private sector, it is highly likely that consumption of identities based on the local eID scheme will also be allowed.

[27] STORK 2.0, D5.2.5 eBanking Pilot Final Report, February 2016, https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=84:d525-ebanking-pilot-final-report&Itemid=176&start=10

[28] OIX, Opening A Bank Account Cross Borders With A Digital ID, September 2017, http://oixuk.org/wp-content/uploads/2017/10/Pre-Discovery-Market-Intelligence-master-copy-2.pdf

[29] https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf

This difference is actually crucial with regard to the acceptable burden that the identity proofing must represent compared to smooth user experience.

## Added value of eIDAS-based eIDs

The different experimentations conducted on the reuse of eIDAS-based eID to identity customers allow us to list a series of concrete value-adds for banks and customers. These can address many of the identity verification challenges currently experienced by banks, as listed previously.

Key advantages for banks of using eIDAS-based eID for on-boarding purposes:

- **Increased security:** the data shared is endorsed by a governmental entity. Risk of fraud and identity theft is reduced thanks to the use of strong authentication, compared to visual authentication of ID papers by bank agents (paper identity fraud is still widespread) in a local branch or within a remote KYC video-conferencing system;
- **Improved accuracy of the data:** data is shared on an automated, standardized and electronic basis meaning fewer errors due to manual data entry;
- **Time savings:** increased speed of the identity verification process;
- **Cost savings:** reduction of face-to-face onboarding costs due to the automatic transfer of information allowed by the eIDAS-based eID remote strong authentication;
- **Reduced legal and reputation risks:** with the reduction of fraud and errors, banks are less likely to suffer from legal and reputational risks linked to failed operation and weak procedures;
- **Larger customer base:** current identification verification processes makes it difficult and costly for banks to onboard new foreign customers. Consequently, many banks are reluctant to offer some services to foreigners and/or provide a full new onboarding process for clients coming from a foreign branch of the same bank. The eIDAS-based eID trust framework provides confidence foreign customers' eIDs and should thus result in greater business opportunities for banks wanting to offer competitive cross-border services. The STORK 2.0 eBanking Pilot reports that "according to SIBS's estimates, it is expected to have a potential market of 1 million open account processes per year in Portugal".[30]

In parallel, banks' customers also benefit of the improved services in terms of quality and time efficiency. Additionally they also benefit from:

- **Better service to customers:** the time and cost savings linked to the use of eIDAS-based eID instead of a full onboarding and identity verification process means that bank agents have more time to dedicate to activities that add more value for customers. The eBanking STORK 2.0 pilot points out that according to Barclays, current onboarding procedures consist of 25% of time spent to receive financial advice, while 75% of the rest of the time is spent on registration formalities. eID could shift this ratio to 95% of the time spent discussing financial needs during a 25 minute appointment with a financial advisor.[31]
- **Reusable eID mean:** customers also benefit from a better user experience thanks to the possibility to use one eID mean to access several service providers;
- **Protection against identity theft:** the use of stolen ID paper-based documents by fraudsters is difficult to monitor. The use of eID allows users to check the audit log of the use of their eID and authorise a revocation of the authentication certificates of the stolen document, making it unusable in the future and thus limiting the negative consequences of the identity theft.

## Current challenges

Although there are clear advantages to using eIDAS-based eID to perform strong authentication and identity proofing of customers, it is not necessarily the perfect answer to all of the challenges banks are facing.

Several issues have been identified which currently present barriers to further adoption of eIDAS-based eID by banks. Having said this, none of these issues completely rules out the use of eIDAS-based eIDs to support banks in complying with AML and PSD2 legislations. On the contrary, they simply constitute a list of key points to be clarified in the upcoming months.

### Pricing and billing

At the moment, there has been no official communication by EU Member States on the approach that the different countries intend to adopt regarding the terms of access to the national eIDAS-Node by private sector service providers. Consequently, there is also little possibility to refine a possible commercial model for private service providers and identity providers.

[30] STORK 2.0, D5.2.5 eBanking Pilot Final Report, February 2016, https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=84:d525-ebanking-pilot-final-report&Itemid=176&start=10

[31] STORK 2.0, D5.2.5 eBanking Pilot Final Report, February 2016, https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=84:d525-ebanking-pilot-final-report&Itemid=176&start=10

As mentioned in Use Case 2 of this paper, banks may act as identity and attribute providers (providing ID information) as well as service providers (consuming ID information). In order to create the correct incentives for each party to participate in the eIDAS ecosystem, it remains to be seen what cost model will be adopted regarding possible attributes exchanged on banks' customers. Currently, banks are calling on data service providers to collect some attributes about prospective clients against remunerations. Information exchanged as part of the eIDAS Network could disrupt to a certain extent the current situation.

The STORK 2.0 eBanking study has listed some key concerns about pricing of the attributes:

- Attributes may have different pricing in different countries, e.g. credit scores may be fairly easy to obtain in the UK while this information does not exist in France. Address may be considered in the UK as an important attribute to perform due diligence while it could have less importance in Belgium;
- Some Member States may consider that attributes exchanged as part of the eIDAS Network should be free considering that this is personal information owned by the user, not the companies collecting and storing them;
- Income resulting from the billing of attributes exchanged may be marginal compared to management costs;
- Different approaches regarding the billing:
  - Fee per each transaction
  - Annual fee per volume of transactions

Both in the STORK 2.0 eBanking pilot and the CEF Opening of a bank account project, attributes were exchanged for free. It is therefore difficult to draw any concrete conclusions.

Overall, the lack of a common approach at the EU level puts the eIDAS Network at risk of having cherry-picking behaviours, where service providers would potentially choose to connect to the eIDAS-Node offering the cheapest possibility. Evolution of the situation in this direction will depend on the decision of EU Member States to allow or restrict the access of foreign private service providers to their eIDAS nodes. In the results of its eIDAS pilot, Mobile Connect suggests the creation of a commercial federation service acting as a commercial contracting organisation supporting and manage billing for cross-border private use cases.[32]

Discrepancies between attributes collected and the eIDAS minimum dataset

KYC processes are not harmonised at the European level. Each Member State remains free to translate the EU provision into local legislations. As a consequence, the type of data collected and the procedures to apply to the banking and financial sector differs from one country to the other. Additionally, banks and financial institutions may introduce additional checks on top of the regulatory requirements, notably linked to the cultural context of the country.

The study "eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU" specifically maps existing and potential KYC processes implemented across Europe, as well as their equivalence to eIDAS levels of assurance.[33]

Attributes collected as part of the on-boarding processes can be divided between identity attributes and KYC specific attributes.

The minimum data set of eIDAS is composed of key identification attributes: Name, Unique identifier, Date of birth, Place of birth, Address, Gender, Name at birth. This dataset may be completed by sector-specific attributes. Yet the latter is limited to attributes supporting the identification of customers and can in no case concern attributes aimed at evaluating the eligibility of the customer for the service, or performing KYC checks to detect fraud and risks (e.g. credit score). As part of this strategic paper, we therefore would only consider the potential contribution of eIDAS-based eID to support the verification of the customer ID, the authentication and the collection of identity data. Additional processes must be in any case be put in place by the banks and financial institutions to collect KYC attributes.

[32] Mobile Connect, Mobile Connect for Cross-Border Digital Services - Lessons Learned from the eIDAS Pilot, February 2018, https://www.gsma.com/identity/mobile-connect-cross-border-digital-services-lessons-learned-eidas-pilot

[33] DG CNECT, Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU, April 2018, https://publications.europa.eu/en/publication-detail/-/publication/139abc5b-49c6-11e8-be1d-01aa75ed71a1/language-en

The study on eID for online onboarding references the attributes that are most often collected to support the KYC processes.

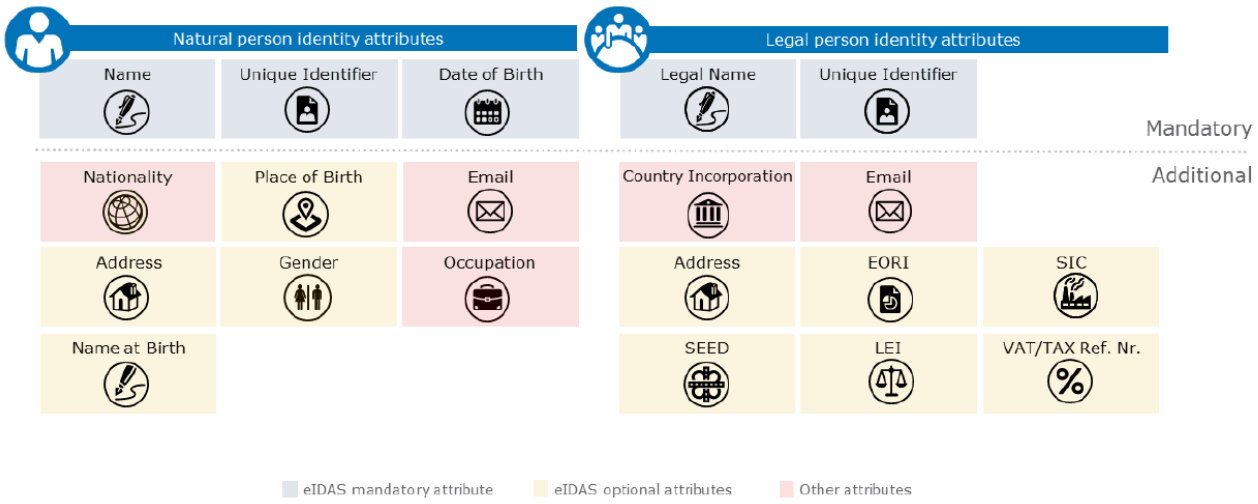


Figure 1 – Natural and legal person identity attributes collected as part of the on-boarding process[34]

Although most required identity attributes are included in the eIDAS minimum dataset (compulsory and optional attributes), some gaps remain, notably nationality, email and occupation for natural persons, and country incorporation and email for legal persons.

Although the STORK 2.0 infrastructure allowed for the exchange of documents as part of the cross-border authentication process, it is not the case for the eIDAS Network architecture. As such, eIDAS can only be used for collecting identity attributes, and not KYC attributes. However, a strong authentication of the customer under eIDAS could support access to more functionalities supporting KYC procedures that banks and financial institutions remain free to implement. Strong authentication could therefore allow the possibility of sharing additional information, e.g. credit score, salary or employer.

## Lack of clarity on the liability regime of service providers and attribute providers

Article 11 of the eIDAS Regulation sets some key principles regarding the liability regime and key responsibilities in case of damage caused intentionally or negligently to any natural or legal person:

- Notifying Member States should ensure that the person identification data uniquely representing the person in question is attributed at the specific assurance level defined and it should guarantee the availability of the eIDAS Node to provide the authentication;
- The identity providers are liable for the correct attribution of the means to a unique person;
- The organisation operating the eIDAS Node needs to correctly confirm identification data.

However, the STORK 2.0 eBanking pilot points out that all aspects of the liabilities under eIDAS remain to be interpreted in accordance with national liability rules, which may in practice limit the liability of the Member States and national public authorities.[35]

Additionally, the regulation does not cover other "parties to a transaction" which means that liability of service providers, in our case banks, remains completely regulated by national liability rules.

For the hypothesis of the adoption of sector specific attributes where banks act as attribute providers, not only are the attributes not covered by the eID scheme defined LoA, but the rules on liability of damage caused regarding this data may differ from country to country. This situation means that banks may have to cover themselves with insurance premiums.

[34] Source: DG CNECT, Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU, April 2018, https://publications.europa.eu/en/publication-detail/-/publication/139abc5b-49c6-11e8-be1d-01aa75ed71a1/language-en
Please note that the diagram has been modified to remove "Nationality" as one of the attribute covered by the eIDAS minimum dataset in line with the most recent version of the eIDAS SAML Attribute Profile, see https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20SAML%20Attribute%20Profile%20v1.1_2.pdf?version=3&modificationDate=1528362598014&api=v2

[35] STORK 2.0, D5.2.5 eBanking Pilot Final Report, February 2016, https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=84:d525-ebanking-pilot-final-report&Itemid=176&start=10

Finally, for service critical infrastructures, the results of the STORK 2.0 eBanking pilot stressed that banks often request the adoption of Service Level Agreements in order to clarify liabilities and responsibilities with third party data and services.

### Concerns about eIDAS-based eID user experience and citizen uptake

eIDAS-based eIDs are still at the moment based on solutions with limited user experience that are not in line with the trends of the banking and financial sector. For example, smartcard eIDs are still in use while mobile is increasingly becoming the key channel of access to online banking services. While smartcards may be compatible with mobile in certain cases (e.g. via NFC chips), many cards in use do not employ this technology. Furthermore, Apple is still restricting the use of NFC readers on its products.

eIDAS-based eIDs across Europe may have complicated or difficult application, activation and management processes at the national level, which reduce active use. For example, there may be a need to own extra hardware to operate the eID (e.g. a card reader), which may be undesirable to the user. Furthermore, some countries have a specific approach to eID which may intentionally or unintentionally limit active use, e.g. in Germany, certificates contained on the eID need to be activated by opt-in, and as a consequence, a large percentage of the German population does not own a functioning eID. Additionally, not all countries have a strong heritage of eID use, and so uptake amongst their populations is relatively low.

If one adds to these points the fact that there is limited awareness among European citizens of the possibilities offered under eIDAS, and currently inconsistent design approaches and levels of user experience across Member States for the process of authenticating cross-border, we can argue that eIDAS eID may have limited appeal to banks right now. Banks must emphasise user experience in the services they offer to remain competitive, and may not want the potential customer base for any new solution they implement to be limited to those Europeans who possess a notified eID. Derived identity solutions may provide a partial answer to this problem, and will be discussed in the next section.

### Lack of understanding by banks on the eIDAS trust framework

Currently, banks do not have enough understanding of the potential benefits of eIDAS for them. For example, they do not have sufficient visibility on the relative trustworthiness/security of eIDAS-based eID schemes. To them the landscape appears very fragmented (different technologies, different identification means, private vs public sector ownership, etc).

### Many EU banks remain focused at the local level, not requiring cross-border authentication

There is a key difference of interest in the solution provided by eIDAS-based eIDs based on the main market of the banks. Several banks interviewed have mentioned that their key markets remain local, meaning that most of their new customers possess local identification means (e.g. residence permit) or a local digital identity. The number of new customers that would benefit from the mutual recognition of their notified eID schemes may therefore be marginal.

### Organisational structure of the banks

We have seen that the banks with the most to gain potentially from eIDAS-based eID are those with a more global customer base. However, these organisations are often very large, with siloed functional areas and decentralized decision-making. This has implications on the ability of these organisations to efficiently assess and decide on the adoption of eIDAS-based eID. For example, a decision on adoption may need to involve departments focused on innovation, cyber security, compliance and customer experience.

## Recommendations

There is a real case for the banking and financial sector to explore the use of eIDAS-based eID for strong authentication and identity proofing of customers.

In the context of AML legislation, the direct use of an eIDAS-based authentication process can be envisaged considering that the KYC process is a one-off procedure at the time of onboarding. While additional attributes may be requested by banks to complete national requirements or shared via sector specific attributes, eIDAS-based eID authentication would provide banks with a high level of assurance with regard to the identity of the newly on-boarded customers and their main ID attributes. Alternatively, banks could also rely on derived identities that have been verified by an eIDAS-based eID (cf. next chapter). The choice between the two solutions highly depends on the usability and uptake of the eIDAS-based eID solution used in the specific country.

In the context of PSD2, the use of eIDAS-based eIDs is less evident, at least at the moment, considering the limited user experience of these solutions. Strong authentication of customers would have to be performed each time they conduct an electronic transaction, which can occur several times a day. Therefore, unless the eIDAS-based eID solution used in the specific country has a high user experience and has been tailored to the needs of the banking sector, we would rather suggest to use a derived identity solution verified by an eIDAS-based eID (cf. next chapter).

## For the European Commission

The European Commission has already taken action to explore to what extent eIDAS-based eID can be used to perform KYC procedures. Following on from the study on eID for digital onboarding, the European Commission has decided to set up an Expert Group on electronic identification and remote Know-Your-Customer processes[36], jointly managed by DG CNECT, DG FISMA and DG JUST. The first meeting took place on 9 April 2018 and the 2nd one on 10 July 2018, gathering regulators, supervisors, identity experts as well as stakeholders of the banking industry and consumer organisations. The objective of this group is mainly to provide expertise and recommendations to the European Commission relating to electronic identification and remote Know-Your-Customer processes based on eIDAS, for the purposes of digital onboarding and supporting the adoption of guidelines. The European Commission also aims at seeking greater transversal alignment and cooperation between pre-existing expert groups in the field of identity and KYC processes. Finally, participants are encouraged to exchange best practice in order to "facilitate the emergence of interoperable and legally recognised portable remote Know-Your-Customer processes across the Union".[37]

In addition to continuing this important collaboration, we encourage the European Commission to:

- Continue its efforts to clarify the position of EU/EEA Member States on the conditions set for the private sector to consume eIDAS-based eID, notably for private identity providers developing derived identity solutions. Such information should be widely communicated to the private sector when available in order to seek greater alignment between the expectations of private Service Providers and the actual possibilities offered by the eIDAS Regulation.
- Support the Member States in coming to a common agreement on the commercial model to be established for private sector use of eIDAS-based eID, and facilitate the establishment of a unified mechanism for managing billing.
- Supplement missing attributes required to complete the identification of the customer with the definition of additional sector-specific attributes that could be forwarded by Member States whenever an authentication request under eIDAS is triggered. This decision would have to be agreed upon by the national experts of the eIDAS Cooperation Network, following a discussion within the eIDAS eID technical subgroup.
- Explore the potential of the CEF eDelivery building block for the sharing of documents supporting the identity of customers and/or the collection of KYC attributes by banks and financial institutions.

## For EU/EEA Member States

Currently there remains a lack of clarity from the EU/EEA Member States with regard to the conditions that will be set for private Service Providers to consume eIDAS-based eIDs in a cross-border context.

Overall, we encourage Member States to:

- Allow private sector reuse of the national eID scheme if the intention is to support the reuse of eID in the banking sector, and set out clear conditions and guidelines for this (including a commercial/contractual model). High uptake of nationally issued eIDs are generally observed in countries that have built strong cooperation with the private sector.
- Consider the adoption of sector-specific attributes based on the minimal information necessary to perform KYC checks. Agreement on the specific dataset will have to be reached at the eIDAS Cooperation Network level following an opinion of the eIDAS eID technical subgroup.
- Consider the possibility for the public sector to act as attribute provider in the eIDAS ecosystem of those KYC pieces of information for which public authorities are considered as trusted sources (e.g. social security number or tax number)
- Provide clear information to banks on the added value of eIDAS-based eID, as well as how they can integrate the national eID scheme authentication process with their online services. Educate banks on the peer-review process and assurance requirements of eIDAS as a way to reassure them regarding security.
- Work towards user experience improvements in eID at the national and cross-border level, as discussed in the report 'The user experience of eIDAS-based eID: Looking ahead'. [38] This will encourage citizen uptake of notified eIDs and cross-border use thereof, and will make eIDAS-eID more appealing as a solution to banks.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36277&no=1

[37] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36277&no=1

[38] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Final+report%3A+The+user+experience+of+eIDAS-based+eID%3A+Looking+ahead

## For banks and financial institutions

Overall, we encourage banks to:

- Consider eIDAS-based eID as a solution to be explored in order to improve identity proofing and strong authentication of customers, at least for procedures that are occasional and require a high level of assurance.
- Seek ongoing cooperation with the European Commission and EU Member States on the topic of identity management, and regularly share key pain points that could be addressed at the EU level.
- Consider conducting more production pilots on the use of eIDAS-based eID in the sector.
- Work closely with the EU Member states to define a commercial/contractual model to exchange ID attributes, and to clarify liability questions.
- Explore potential partnerships and consortiums to create a national private sector node to support the exchange of information between banks across borders, and to evaluate the cost of implementation and operation.
- Conduct a real cost estimation of eIDAS-based eID integration as a means of verifying current digital identity solutions compared with current face-to-face onboarding.

# Banks as identity providers: eIDAS verified digital identities

# 05

Historically it has been the role of government to provide a legal and secure identity to citizens. Over the past 15 years, it has become of utmost importance to provide citizens with an equivalent digital identity with which they can transact online. However digital identity management is no longer a unique prerogative of governments but can also involve to different extents private sector actors.

Identity Providers (IdPs) are the stakeholders that provide the means of electronic identification to a person whose identity has been established. The provider of the electronic identification can be a public administration or a private sector provider.

If the state is in charge of regulating the infrastructure, the interaction between identity providers and the operation of the eID scheme, we are talking about a **PUBLIC-LED ECOSYSTEM**. Today, we observe two types of approach:

- **Sovereign eID schemes:** The national eID scheme set-up and implementation is driven by the government. The use of digital identity may be restricted to eGovernment purposes or open for reuse by the private sector (banks, telecom, hotel, airlines, etc...)
- **Federation of identity providers regulated by the government:** The government sets up an interoperability framework with different private sector identity providers in charge of providing the identity verification. Again, it can be restricted to access to eGovernment services or open for reuse by the private sector.

In a **PRIVATE-LED ECOSYSTEM**, a series of private sector identity providers offer solutions for electronic identification for online public and/or private services:

- **Private identity solutions:** Private identity providers can develop their own digital identity solutions and put in place a more or less stringent verification mechanism to ensure that the digital identity generated is based on a real ID (derived identity). In some case, private identity providers decide to create their own trust framework in the form of a federation of identity providers. Governments may recognize these private identity solutions for accessing to online public services.[39]
- **Self-declared identities:** Users self-declare their identities, for example using their Google or Facebook accounts. There is no verification of whether the users are who they claim to be.

Banks can therefore act as identity providers within a federation of identity providers regulated by the government, or they can contribute to a private-led federation, or they can develop their own digital identity solution such as online banking credentials.

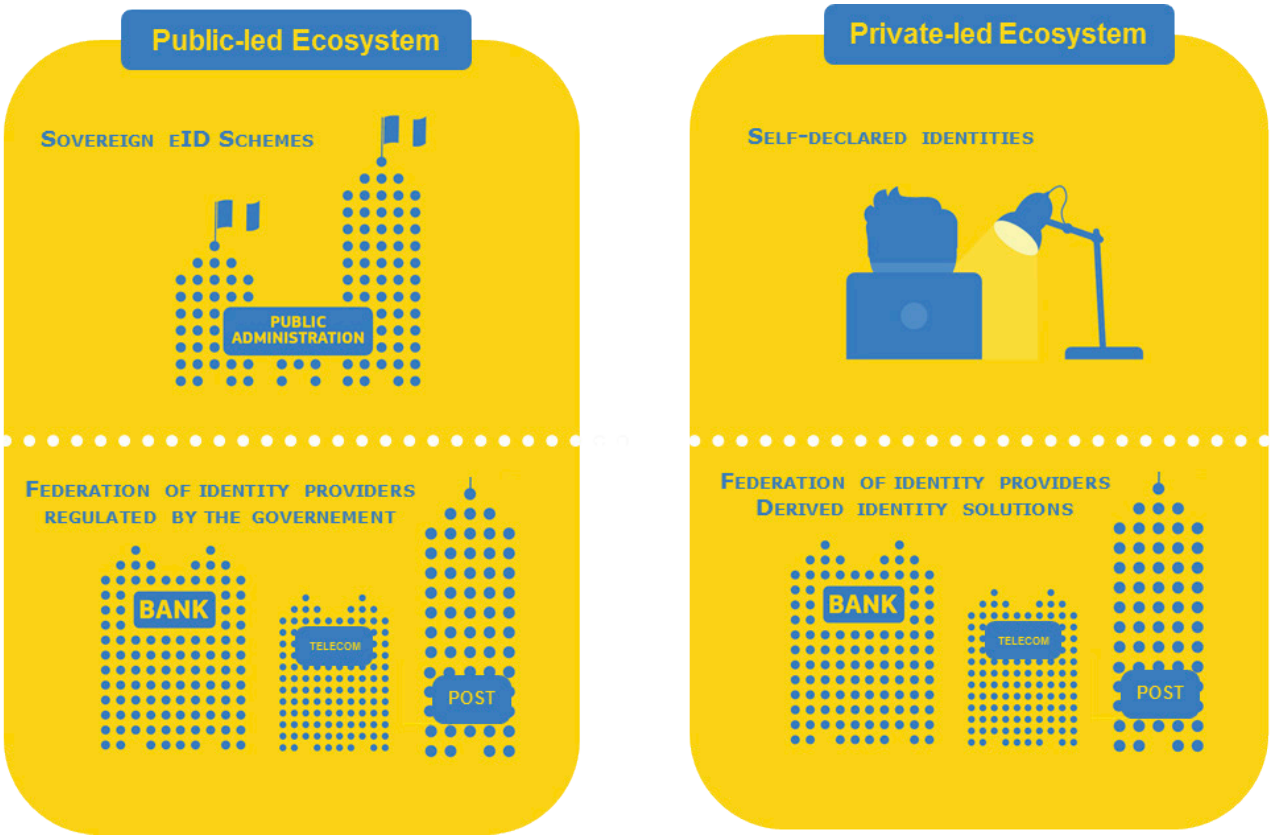


Figure 2 – Public-led vs. private-led eID solutions ecosystems

[39] For example, BankID scheme has been recognised has an identity provider for accessing Swedish eGovernement services: https://www.bankid.com/en/om-oss/nyheter/nu-ar-bankid-med-som-leverantor-till-offentlig-sektor

## Assessment of the reuse of eIDAS-based eID by banks acting as identity providers

Banks can be identity providers and can leverage eIDAS-based eIDs in different ways:

### Banks as part of a federation of identity providers regulated by the government

In this case, banks are part of a nationally-issued eID scheme initiated by a government. The government has the possibility to notify the eID scheme under eIDAS in order for it to be recognized by other European countries to access online public services.

This approach was adopted by the UK's Governmental Digital Service when developing its GOV.UK Verify eID scheme.[40] Out of the seven certified companies offering identity verification, one is a bank (Barclays).

Key advantages for banks to participate in public-led eID scheme federations:

- Leverage existing identity verification procedures put in place for regulatory compliance by the banks and monetize it through participation in the federation of private identity providers. Creation of a new profile is either paid by the state or directly by the user;
- Attract new customers: users seeking a governmental identity can be captured and redirected toward other services offered by the banks. Users satisfied with the eID service and experience will be more inclined to seek additional services from the bank;
- If allowed by the state, the eID scheme can be reused by the bank to grant access to private online services. In this case, banks will benefit from a strong authentication solution based on information guaranteed by the state.

The difference between participating in an eID scheme that has or has not been notified under eIDAS is not striking at the moment when considering banks as identity providers (only). The most obvious advantage is the increased attractiveness of the notified eID scheme for users compared to others, when considering the possibility of reusing it cross-border. Yet the understanding of the advantages of notified eID schemes is still too low among the general population to really influence their choice.

In this type of approach, banks are dependent on the government regarding the decision to notify the scheme under eIDAS. They also have to agree with the terms and conditions set by the government regarding the remuneration model (actual costs of eID creation and management vs. remuneration), the regulation of the cost model and amount of digital identity creation, conditions of reuse by private service providers.

### Banks as part of a private-led federation of identity providers or offering online banking credentials

In this scenario, banks are acting as identity providers outside the remit of a public-led eID scheme:

- Either as part of a private-led federation of identity providers.
- Or as provider of online banking credentials to their customers.

In some countries, the eID scheme developed by banks has become the solution used to access eGovernment services. For example in Sweden, the BankID network was created by a group of eleven banks. BankID is now the main identification solution used in Sweden to access private and public online services.[41] The solution counts 7,5 million active users (more than 75% of the population in Sweden).

In this scenario banks are providing an electronic identity that can be directly reused to access their online banking services. The advantage of participating in a private-led eID scheme is therefore the same as participating in a public-led federation (e.g. monetising existing identity verification procedures, and attracting new customers). Most importantly it allows for a mutualisation of the onboarding costs of its own customers (one onboarding procedure is required while the digital identity can be reused among different service providers) with other private organisations. This translates into saving for the private organisations involved in the federation but also into a better user experience for customers who can reuse their digital identities with many service providers.

In the case of a bank offering an eID scheme to access its own online services only, costs linked to onboarding cannot be mutualised but the bank is freer with regard to the solution it wants to develop.

The key drawback for the private approach is that it does not benefit from the trust and legitimacy of the public-led federation, where the state is endorsing and validating the identity of users. The level of trust in private-led eID solutions is thus highly dependent on the procedures set-up to perform identity proofing and verification.

Governmentally issued eIDs are highly trusted. The trust framework introduced by the eIDAS Network ensures that one's identity is recognised as being secure and accurate beyond the remit of national borders.

[40] https://www.gov.uk/government/publications/introducing-govuk-verify

[41] https://www.bankid.com/en/

Private-sector led solutions currently do not benefit from such levels of trust in the eIDs that are delivered. The procedures for performing identity proofing and verification are considered as a weak point for two reasons:

- First, the absence of a trust framework between private-sector solution providers means that even if a bank put a highly secure and stringent procedure in place, there is no guarantee that other stakeholders will trust the level of assurance of the identity.
- Second, as strong identity proofing and verification procedures are often hard to setup, the creation of a first digital identity is in many cases based on the production of a national ID document or passport. The data is entered manually in the system or by optical reading (automatic extraction or reading of MRZ) that can result in data entry errors. It is also possible that users produce forged ID documents. A recent experiment from the German Federal Office for Information Security presented during the July 2018 KYC expert group has shown that remote onboarding procedures by video can be prone to such frauds: the governmental team managed to trick a remote digital onboarding systems with a German eID card printed with a conventional laser printer associated to an holographic filter to reproduce the visual security features of the smartcard. Additional tricks, such as the use of Silicon masks[42], advanced countering make-up, and other biometrics credential hacking[43] should be deeply assessed. Such errors could result in high liability costs for banks.

eIDAS-based eIDs could improve the identity proofing procedures of private identity providers by allowing for a verification of the identity information by a strong authentication endorsed by the government.

When customers intend to obtain a derived identity to access online private services or upon the creation of an online banking credential, the digital identity could be "verified" by authentication with an eIDAS-based eID, either at the time of the eID creation or later when a stronger level of assurance is needed. Other private service providers would recognize this "trust mark" providing a higher level of assurance with regard to the identity.

Depending on the needs of the service providers, a control authentication can be imagined to guarantee that the information from the derived identity remains valid.

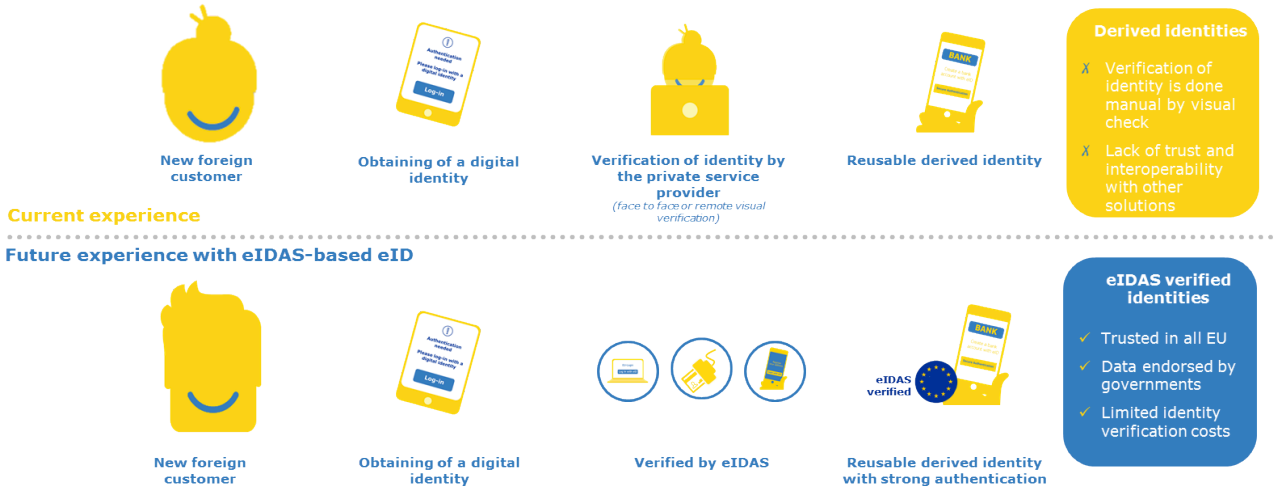


Figure 3 – How eIDAS-based eID could improve identity proofing by private identity providers

[42] https://www.youtube.com/watch?v=2yuXTZGbJ38

[43] https://media.ccc.de/v/biometrie-s8-iris-en#t=77

Additionally, banks would save a significant amount of resources linked to identity verification of customers (needed for KYC and other regulatory purpose). The use of eIDAS-based eIDs is expected to grow steadily with the development of eGovernment services and more user friendly eIDs based on mobile solutions. eIDAS verifications could be progressively introduced by identity providers, with integration costs compensated for by the savings achieved through remote and secure authentication of users.

## Recommendations

Banks are currently conducting identity verification of their customers on a daily basis and in many cases are supporting the creation of online banking credentials, hence acting as identity providers.

Private-led eID solutions are emerging and becoming stronger every day in Europe with the aim of reducing onboarding costs for service providers and improving the customer journey by avoiding multiple identity verifications.

However, the eIDAS trust framework can add a degree of legitimacy to the identity solutions currently offered by banks.

### For the European Commission and EU/EEA Member States

- Work towards clarity and an eventual agreement on the conditions to be set for reuse of eIDAS-eID by the private sector, in the limit of willingness of EU Member States:
    - For banks participating as identity providers in public-led federations designed to access eGovernment services, this may allow them to reuse the eID scheme to which they contribute for access to their own services, rather than just eGovernment services.[44]
    - For banks participating as identity providers in private-led federations or providing online credentials to their own customers, this may allow them to use eIDAS-based eID to 'verify' the digital identities they provide. This will enhance the legitimacy of their solutions and may save onboarding and identity verification costs for a growing segment of their users.
- Develop specific communications to explain to banks the advantages of using eIDAS-based eID as a way to increase trust in private-led eID schemes.

### For banks and financial institutions

- Engage in open dialogue with the European Commission and national governments to encourage the authorisation of the consumption of eIDAS-based eIDs by the private sector, at least in the context of derived identity verification.

[44] For example, banks acting as identity providers under the public-led federation UK.GOV Verify eID scheme cannot reuse the UK national eID scheme to authenticate customers during KYC procedure for opening a bank account. The UK.GOV Verify scheme is at the moment restricted to eGovernment applications.

# Conclusion

# 06

eIDAS-based eID already has many ingrained links with the banking sector. In some European countries, digital identities created in the banking sector have become nation-wide identity schemes used to access eGovernment services. In other countries, banks already participate in a federation of identity providers contributing to a government identity scheme. As such, we have found that there is genuine interest by banks in understanding better what eIDAS-based eID can offer them.

In the role of service provider, banks can potentially use eIDAS-based eID to more quickly and securely identify customers for KYC purposes, under the AML and PSD Directives, as well as reach a broader customer base. In the role of identity provider, banks may be able to use eIDAS-based eID to 'legitimise' the digital identities they already offer.

However, there are many issues that must first be addressed or clarified before meaningful gains are made. Firstly, it is important that as many EU countries as possible notify their eID schemes under the eIDAS Regulation, and then make these available for use by the private sector.

Currently, identity verification is costly for banks but well integrated. To justify new investment in the eIDAS infrastructure, the tangible added value of eIDAS-based eID will still need to be demonstrated. This will involve clarifying the position of the Member States on pricing the use of the eIDAS Network, determining whether additional attributes can be exchanged by banks, and conducting detailed estimations of cost savings.

Furthermore, more effort needs to be invested into communications. Banks currently do not have a full understanding of how eIDAS can help them. Similarly, awareness and uptake of eIDAS-eIDs by citizens is on average low.

Overall, we recommend increased dialogue between the European Commission, EU/EEA Member States and banks, to discuss, agree and act on these issues.

## European Commission

Business proposition of eIDAS-based eID: Banking Sector

2018 – 28 pages