10 November 2016

EBF_023879

E-IDENTIFICATION
EBF POSITION & RECOMMENDATIONS

More than 315 million Europeans use the internet every day, yet less than 4% of online services are offered across national borders.

Making the EU's single market fit for the digital age is a strategic priority and setting the right regulatory framework for this to happen is vital to enable Europe to use this opening and to foster the development of global digital players.

In the financial sector, the change in expectations and behaviour of customers in the digital era and the uptake of online and mobile services represent a new challenge, as well as an opportunity to reach out digitally to millions of new customers.

Boosting economic growth and removing the barriers to e-commerce and electronic banking by preserving trust and security should be one of the main priorities of the European Commission's Digital Single Market Strategy.

Many positive opportunities are provided by the Regulation on electronic identification and trust services for electronic transactions in the internal market adopted on 23 July 2014 (eIDAS). It is an important enabler for secure cross-border electronic transactions, permitting citizens to use their own national electronic identification schemes (eIDs) to access public services in other EU countries in a seamless, faster, secure way, and creating a recognised legal framework for the usage of electronic trust services. For the Financial Sector, the eIDAS presents huge opportunities in terms of rapid onboarding of customers as well as the capacity to engage cross-border, contractually, with new customer markets in a secure environment and reduce fraud and operational costs. For banks and other players in the financial services, it is critical to improve the customer experience by developing innovative products and services adapted to customers' needs while preserving trust and security.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

However, even if the eIDAS Regulation creates an interoperability framework for the national eID systems to be recognised by public bodies across the EU, it remains up to Member States to define: a) the electronic identification schemes and embedded information established for citizens of their State and b) the terms of access to the online authentication of government eIDs by the private sector.

We believe that sufficient uptake in the private sector is one of the critical elements in ensuring the success of the eIDAS Regulation and both of these above-mentioned measures may lead to a lack of true cross-border interoperability of national eIDs.

Further consideration should be given to the following objectives to allow citizens and businesses to benefit from the Digital Single Market fully and to ensure equal access to products and services for all citizens.

Currently we observe inconsistencies between eIDAS, which promotes e-identification in order to access online products and services and carry out online transactions securely, and the 4th AML Directive, which favours face-to-face customer due diligence and considers non-face-to-face relationship as a "high risk" (thus requiring Enhanced Due Diligence). In view of this, **we welcome the European Commission's proposal amending the 4thAnti-Money Laundering Directive (AMLD)**[1] which proposes the identification of customers and the verification of their identity on the basis of electronic identification means. **The reference to Regulation (EU) 910/2014 (eIDAS) appears to be a step in the right direction**.

Nonetheless, certain legal uncertainties may remain and an uneven playing field might occur in practice.

As previously mentioned, it is up to the Member States to define the electronic identification schemes which will be available at national level for their citizens. At present there is a lack of clarity around the implementation of electronic identities in the Member States. This may contribute to the fact that on the one hand citizens in certain Member States can and will be able to access the digital single market fully, whilst, in other Members States they will not. For instance, in some Member States an eID solution will be available, whilst in others it will not. This situation will lead to an uneven playing field for citizens and services providers. Other factors could also substantially weaken the capacity of the EU banks to operate effectively cross-border. A clear example of this is the current divergence in the implementation of the AMLD across Member States. A more consistent approach would enhance the security for the whole digital market, and at the same time help to ensure a level playing field for financial entities who wish to operate across European Markets. For instance, in relation to remote onboarding of customers, some EU Member States allow the use of non-face-to-face identification by means of videoconference, while others do not permit this. As a result, financial institutions in these Member States can initiate distant banking relationships (including cross-border) whereas other financial institutions are prevented from doing so in their own jurisdictions due to face-to-face identification still being required.

In terms of establishing best practice standards to be met in the identification of new customers of the individual bank, it is paramount to generate an environment in which national authorities and the financial sector can collaborate in an efficient way at a European level in order to share best practices irrespective of national interpretations.

[1] Proposal for a directive of the European Parliament and of the Council 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 Directive 2009/101/EC - 2016/0208 (COD)

Even though the eIDAS Regulation creates a coherent framework we believe that the impact will be seen later, in the longer term, as more and more electronic identification schemes will be notified and digital services promoted and adopted by Member States. The financial services' sector needs to address customers' digital expectations in the short term and therefore be able to employ other secure and robust processes approved by national competent authorities - outside of eIDAS - for remote identification of customers (digital onboarding). This potential should also be contemplated in the amended AMLD. A truly Digital Agenda must keep the door open to new technologies, standards and processes.

With the obligation to acknowledge eIDAS-derived digital identities to access public services which will become mandatory for Member States in 2018, attention is increasingly focused on making the digital onboarding a reality for retail banking customers. In this sense, and in order to boost the uptake of eIDAS, as well as the digitalisation of the Financial Sector, this working paper aims at presenting the challenges for the banking sector. The working paper proposes key recommendations on the following issues identified with the intention of facilitating cross-border access to online financial products and services for EU citizens. This approach should be supported by the adoption of these recommendations, developed further in this paper with a focus on the three points:

1. Identification papers provided by the customers and remote authentication/ validation processes;
2. Access to eIDAS schemes and the consistency between eIDAS and other legislation; and
3. E-ID lifecycle management.

KEY RECOMMENDATIONS

- **Actively encourage Member States to develop electronic identification schemes for their citizens and ensure full access to these schemes by the private sector.**

- **Enlarge the basic eIDAS identity attribute-set to include additional attributes as required for client identification in the Financial Sector** (for example making the customer's address mandatory and allowing banks to validate ID documents digitally). It would be of great value and make the publicly built solution very attractive by reducing some of the effort and costs involved in data verification.

- **Amend article 13 of the proposal amending the 4th AML Directive and other related articles to include , in the AML Directive, any other remote identification processes recognised and approved by the competent authority:**
  "Customer due diligence measures shall comprise: 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, as set out in Regulation (EU) No 910/2014 ***or any other remote identification processes recognised and approved by the competent authority****"*

- **To promote cross-border interoperability in the banking sector and ensure a level playing field across Member States (and possibly beyond in EEA countries and Switzerland), we would recommend leveraging the work carried out under the Connecting Europe Facility programme, by reusing the eID Digital Service Infrastructure (DSI) and setting up a financial sector specific DSI.**
  This financial sector specific DSI could investigate the needs of the sector regarding digital onboarding, with the objective of establishing good practices in countering money laundering, and the elements/ attributes which are required to potentially ensure the portability of Know-Your-Customer (KYC). The work carried-out could then possibly be used by national authorities as a benchmark in their dealings, with the aim of promoting cross-border activity in the financial sector and guaranteeing a common level playing field across Member States.
- **In order to facilitate remote validation of identification documents, the issuance of electronic identification documents such as biometric passports should be encouraged.**

1. IDENTIFICATION PAPERS PROVIDED BY THE CUSTOMERS AND REMOTE AUTHENTICATION/ VALIDATION

Know-Your-Customer (KYC) requirements, mandated by the existing Anti-Money-Laundering (AML) rules, which aim at preventing money laundering and financing terrorism, require banks to complete the following activities when onboarding a customer to the entity:

- Establish the identity of the customer;
- Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate); and
- Assess money laundering risks associated with the aforementioned customer for purposes of monitoring the customer's activities.

The AML rules tend to assign a higher degree of accuracy to face-to-face identifications and determine that non face-to-face interactions encompass a higher degree of risk.

In practical terms, for identification purposes the customer needs to present the necessary documents to prove his/her identity. Since 2011, all Member States have introduced the use of biometric passports equipped with enhanced security features to verify the citizenship. A biometric passport has intricately designed passport pages, complex watermarks and a data chip. These have a Near-Field Communication (NFC) chip incorporated inside, containing the details on the passport's holder identity such as digital signature data which the passport also shows visually.

The contactless chip stores the same data, which is visible on the photo page of the passport. In addition, the chip also includes a digital photo of the passport holder, which could facilitate the process of biometric comparison by using, for example, a facial recognition technology. The biometrics are considered more personal and reliable than a passport photo or a PIN, as it uses personal traits such as facial or eye maps and fingerprints as primary identification features. These biometric features were accepted by the International Civil Aviation Organization (ICAO) after analysing multiple other biometrics including retinal scan[2].The chip can be read with a proper device and could help banks validate the details which the customer gives.

The Radio-Frequency Identification (RFID) chip which is present in passports could be considered as a good starting point for verifying whether the document is genuine and that information in the chip is consistent with the printed information.

Today, many tools are available to check ID documents which may be much more effective than a simple human verification. Nonetheless, a critical point in the entire identification chain is the issuing of machine-readable documents to facilitate the authentication process (valid for face-to-face but especially remote situations).

In face-to-face identification it is possible for staff, with proper training, to identify falsified papers and to identify the customer through facial recognition techniques, comparing visually the customer and the photograph on the document. Yet, in a cross border onboarding context, or onboarding of nationals of other member states, when it comes to ID documents issued in other Member States the skills set required becomes more difficult to master at a bank level.

[2] https://www.epassportphoto.com/blog/2008/02/what-does-a-biometric-passport-indicate/

In the case of remote identification, parties are in different premises, engaged via an interface. Technological advances allow these interfaces to be sufficiently secured and have enough definition to enable a human to perform the visual recognition remotely. Video recording is already considered as an option in certain Member States such as Germany and Spain.

This said, by leveraging new technologies, it could be argued that identification is also viable in a remote situation, without requiring human visual intervention. Current interfaces have enough sensors and fields to gather sufficient data and together with morphological technologies can determine both the authenticity of the document and associate the "holder" of the document with the "owner" of the same document.

RECOMMENDATIONS

- **In order to facilitate validation of identification documents: encourage the use of official electronic document such as biometric passports.**
- **In order to facilitate digital onboarding: recognise remote authentication methods of a document such as video recording.**

2. CROSS-BORDER ACCEPTANCE AND ACCESS TO DIGITAL IDS FOR THE PRIVATE SECTOR

The eIDAS Regulation clearly presents e-identification and e-signature as a new opportunity to facilitate the establishment of non-face-to-face business relationships.

A digital identity issued under a recognised national scheme that satisfies the verification requirements of the European AMLD could be used to make opening a bank account easier, particularly for the growing number of people that arrive in a Member State. Benefits might be achieved in terms of the customer journey, and the ease in which a bank can meet its digital onboarding obligations.

This is true i) with the reuse of home State national digital ID schemes across the public and private sector (already the case in a number of states). and ii) with the use of other Member States' digital ID schemes developed and adhering to the security standards in the eIDAS Regulation for the opening of accounts at distance/ cross-border. This is mostly true where customers do not have a 'biographical footprint' because they have recently arrived in the country, where they want to have access to banking products and services and it is unlikely that their identity can be verified locally.

Divergent implementation and development of electronic identities across the European Union will inevitably create inequalities amongst its citizens and will substantially weaken the capacity of the EU to become a united global reference in the digital era.

Access to digital IDs

Only electronic identifications schemes that have been notified by Member States to the European Commission are considered acceptable through the gateway under eIDAS. A country is not obliged to establish a scheme, or to notify an existing one. Thus, an EU country may decide to continue using its national identification systems for access to its own public services and not notify it, thereby leaving its citizens without a means to access public services in other countries. Conversely, a Member State may use its national identification system to access private sector services whether at home or abroad. This provides little certainty for the private sector in considering the use of digital ID and may cause confusion amongst customers if coverage is only partial across the EU. For the eIDAS system to work smoothly at European level each country should be required to notify the European Commission of at least one of the scheme(s) it has established, and adhere to a minimum set of security standards.

There should be a possibility for cross-border acceptance of Digital IDs for the private sector and a complete access to any public eIDAS infrastructure – once a scheme has been developed – to ensure that eIDAS-derived or other national digital identity schemes are made accessible for the private sector to reuse, with no unnecessary barriers to access put in place.

The access to digital identities for consumers should also be considered. The experience to date is that the Substantial Level of Assurance 2 (LoA2) bar may be set too high for many applicants to achieve it at present. In several Member States many applicants fail to meet the requirements (for instance in the Verify ID scheme in the UK). This substantially limits the market opportunity, and may particularly impact those already financially or otherwise excluded.

Cross-border liability / reliance issues

The eIDAS Regulation includes provisions on liability for notifying Member States, which private sector service providers could take into account when considering relying upon digital identities under notified schemes, or that otherwise meet required levels of authentication. The key issues of **liability and reliance,** specifically for the private sector reuse of digital ID schemes under eIDAS, are not addressed to date. This is a potentially complex discussion which will need addressing before international application of digital IDs developed under the eIDAS standards are reusable for private sector firms.

Furthermore, a technical protocol (as for instance based on the existing Stork) will be necessary, in order to ensure the technical interoperability of the electronic identities and signatures.

Cost and commercialisation of eIDAS

The question of commercial models in the reuse of digital IDs under eIDAS remains unclear. The identification and authentication are free to an online service provided by a public sector body, but leaves Member States free to consider how they establish the regime applicable to the private sector.

Ensure consistency of European Union and national obligations with the promotion of customer digital onboarding

Even though the eIDAS Regulation can bring a coherent framework for e-identification services in the long term, the recognition of notified electronic identification schemes under eIDAS will only be mandatory as of September 2018 (notification and recognition of notified eID means by Member States started on a voluntary basis in September 2015). This situation may bring unacceptable delay from the customer onboarding perspective. Currently there are widely used, sufficiently secure and operable services which are not and might not be notified as eIDAS. A truly Digital Agenda must keep the door open to further progress. In the context of the revision of the 4th AMLD it should be ensured that current and future processes and services outside the scope of eIDAS can be accepted under the revised AMLD at least when they are approved by the competent authority.

Consequently, we would like to ask the European Commission to take an even bigger step forward on the Digital Agenda and incorporate this possibility into the current amendment of the 4th AML Directive.

- **The Anti-Money Laundering Directive (AMLD)'s implementation varies between Member States and Know-Your-Customer (KYC) practices and approaches are not consistent across the EU when it comes to different products and/or customer segments**.
  A consistent transposition of the 4th AML Directive across the European Union and a consistent approach regarding the Know-Your-Customer requirements is central to facilitating a full deployment of retail financial services in the digital single market. As such, it is not possible to determine fully the impact that the cross-border acceptance of digital identities will have on a financial services single market. Hence, there is a need to assess and perhaps address the lack of harmonisation in terms of how the 4th AMLD is transposed, and in the provision of supporting guidance. This could be

carried out under the Connecting Europe Facility programme, by reusing the eID Digital Service Infrastructure (DSI) and setting up a financial sector specific DSI.

The financial sector specific DSI could in particular look into the needs of the sector with regards to digital onboarding, with the objective of establishing good practices in countering money laundering, give practical guidance in the interpretation and implementation of AML directives and identifying what is required to ensure the portability of KYC. The guidance issued by the working group would have quasi-legislative status, in that it would be used by national authorities as a benchmark in their dealings, with the aim of promoting cross-border activity in the financial sector and ensuring a common level playing field across Member States.

In this context relevant data protection issues should also be considered, as financial entities are not allowed to use unrestrainedly the AML data of a customer acquired in a company of its same group located in another Member State. What is more, in some Member States, the exchange of data for AML purposes amongst independent banks operating in the same or different Member States is not allowed except under specific circumstances, based on national laws and/or customer consent.

- **Data provision – matching digital ID attributes and banks' KYC/AML requirements.**
  EIDAS scheme-derived information provides only some of the information required by banks to fulfil their AML and risk-based onboarding requirements. Some information that is vital to banks' KYC process has only been included as optional attributes under eIDAS.

  KYC processes require a number of further data points and checks to be performed e.g. for AML Regulation, Politically Exposed Persons (PEPS) screening, and for the banking law credit worthiness. Therefore under eIDAS, digital IDs will only provide a partial solution to the overall KYC obligations.

- **There is further potential inconsistency between the General Data Protection Regulation (GDPR), which restricts the treatment and of the use of data analysis, and banking regulations on fraud prevention and the sharing of fraud data.** Privacy issues also arise in Member State for sharing or processing customer data e.g. for video recording sessions, for customer identification (this could have an impact if a common database is used), for customer involvement in fraud cases. It is highly important to ensure that the GDPR is implemented the same way in all Members States, otherwise it could create concurrence discrepancies, especially in the use of data or biometrics.

- **Some specific existing national laws (e.g. a requirement for a face-to-face meeting to open a new account) may impact the ability to accept non-face-to-face derived digital IDs** (e.g. such as those provided under the Verify scheme in the UK where specific actions might not be allowed such as video recording during a non-face-to-face opening account process).

Other challenges

For banks that rely on a risk-based approach to onboarding, the standards-led (black box) approach under eIDAS standards will challenge the current obligations on banks to record the verification processes they have undertaken (e.g. scans of passports kept as a record). In some states banks may not be aligned with regulations that underpin the verification process.

Biometric techniques (recognition of voice, facial recognition, digital fingerprint) together with the use of protocols based on Blockchain (distributed ledger systems) should mainly contribute to the optimisation and universalisation of the authentication, avoiding violations or encroachments of identity and, consequently, high costs and bad experiences for the customers in these processes (AML, KYC). Progress must be made in the legislative development of these violations.

RECOMMENDATIONS

- **Amend article 13 of the proposal amending the 4th AML Directive and other related articles to include in the AML Directive any other remote identification processes recognised and approved by the competent authority**

  Article 13

  1. Customer due diligence measures shall comprise:

  (a) 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, as set out in Regulation (EU) No 910/2014* ***or any other remote identification processes recognised and approved by the competent authority"***

  * Regulation (EU) No 910/2014 of the European Parliament and 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 (OJ L 257, 28.8.2014, p. 73)

- **To promote cross-border interoperability in the banking sector and ensure a level playing field across Member States, we would recommend leveraging the work carried out under the Connecting Europe Facility programme, by reusing the eID Digital Service Infrastructure (DSI) and setting up a financial sector specific DSI which could, in particular, look into the needs of the banking sector regarding the digital onboarding.** This financial sector specific DSI could investigate the needs of the sector with regard to digital onboarding, with the objective of establishing good practices in countering money laundering, and the elements/ attributes which are potentially required to ensure the portability of the KYC. The work carried out could then possibly be used by national authorities as a benchmark in their dealings, with the aim of promoting cross-border activity in the financial sector and guaranteeing a common level playing field across Member States.

- **In order to promote the adoption of eIDAS by banks, enlarging the basic eIDAS identity attribute-set to include additional attributes as required for client identification in the Financial Sector would be of great value (for example making the customer address mandatory).**
  EIDAS plays an important role in supporting economic growth in the EU by leveraging ease, security and interoperability of digital cross-border services. For this reason, it is important that eIDAS finds a fast and widespread take-up across industries throughout the EU.

A good push for leveraging eIDAS take-up is to facilitate smooth adoption of eIDAS by the financial sector, which has an enormous digital footprint to make use of. To facilitate the adoption of eIDAS by the financial sector, it is important that the identity attribute-set coming with eIDAS is in synch with the identity information-set banks need when onboarding a customer, according to the AML legislation. The more complete the eIDAS attribute-set, the more attractive the eIDAS solution, as this takes away a large impediment and effort required today by banks in collecting and verifying extra data-attributes.

3. ELECTRONIC IDENTIFICATION LIFE CYCLE MANAGEMENT

Electronic Identity (eID) secure life cycle management is one of the key aspects for providing a trusted digital identity scheme, infrastructure and service. It should include processes and means for the issuance, re-issuance, delivery, suspension, reactivation and revocation of eIDs, which are secure, effective and user friendly for the customers. The eIDAS Regulation does not create any obligations for the private sector, but it defines three levels of eID assurance in the Commission's Implementing Regulation (EU) 2015/1502[3]. Each level differ from the other on the reliability, security and quality of enrolment, electronic identification means' management, authentication, management and organisation. It creates a set of European Assurance levels (high, substantial and low) and it sets out an interoperability framework.

a) Enrolment

This step is divided in several topics (point 2.1 of the Annex in the implementing Regulation cited above). Maybe the most important step is **identity proofing**, both for natural and legal persons. Enrolment also includes a section about the binding between the electronic identification means of natural and legal persons.

b) Electronic identification means of management

It covers the following points:

- Characteristics and design (authentication and safekeeping of eID);
- Issuance, delivery and activation;
- Suspension, revocation and reactivation;
- Renewal and replacement.

c) Authentication

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level.

d) Management and organisation

This section provides elements needed in:

- General provisions;
- Published notices and user information;
- Information security management;
- Record keeping;
- Facilities and staff;
- Technical controls;
- Compliance and audit.

[3] 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

RECOMMENDATIONS

- **Electronic identity lifecycle management should be considered from the perspective of the citizen and of the relying parties of the electronic identification:** The uptake of eIDAS usage depends largely on the promotion of the same scheme in each Member State (services made available, etc.) and also on the usability of the scheme from the citizens' perspective. The user experience must be a key focus in the establishment of the technical standards for the scheme. Regarding electronic identity lifecycle management, and, to ensure the required trust from the Financial Sector in the reliability of the eID for purposes of identification (fit for purpose), a clear mechanism should be established to guarantee that each node actively manages the fraudulent use of the e-ID, including capacity to receive information from users as well as owners regarding identity theft and suspicious activity, effective suspension and reactivation of the e-ID, revoking of the eID, issuance, delivery and re-issuance mechanisms, etc. It also applies to the effective termination of an e-ID upon death or proactive suspension of the usage on behalf of the owner (e.g. communication with official organisms that receive death certifications, etc.).

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp

Senior Policy Advisor - Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69