

# Online Client Identification

## Customer Identification Process in the Finance Industry

Customer Onboarding Process - Know Your Customer (KYC)



### *Summary*

The process of identifying clients online has become a priority in the financial sector. The new regulations on money laundering, projects on digital transformation and costs rationalization as well as pressure being exerted by the vigorously emerging Fintech sector, are its main drivers. This report diagnoses the current situation on this topic and offers its readers important information in the technical, legal and business fields.



# Table of contents

---

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>INTRODUCTION .....</b>	<b>3</b>
WHAT IS ELECTRONIC IDENTIFICATION? .....	5
WHY ARE THESE GUARANTEES NECESSARY? .....	5
<b>DIGITAL BANKING .....</b>	<b>7</b>
<b>BUSINESS BENEFITS .....</b>	<b>9</b>
IMPROVED CUSTOMER EXPERIENCE AND TIME TO MARKET .....	9
BENEFITS.....	11
OTHER BENEFITS .....	12
<b>MONEY LAUNDERING AND IDENTIFICATION.....</b>	<b>14</b>
THE ADVANTAGES OF ELECTRONIC AND CENTRALISED RESOURCES.....	15
<b>DEVELOPMENTS IN THE LEGAL FIELD .....</b>	<b>17</b>
EUROPEAN REGULATION ON IDENTIFICATION AND ELECTRONIC SIGNATURE (EIDAS).....	18
REGULATION ON THE PREVENTION OF MONEY LAUNDERING .....	20
CORPORATE CRIMINAL LIABILITY .....	21
<b>CONSIDERATIONS WHEN SELECTING MEANS OF ELECTRONIC IDENTIFICATION .</b>	<b>24</b>
LEVELS OF SECURITY IN EID .....	24
AUTHENTICATION / BIOMETRICS .....	25
NON-REPUDIATION IN EXPRESS CONSENT. DIGITAL SIGNATURES .....	25
<b>ABOUT US .....</b>	<b>27</b>
AUTHORS .....	27
<i>Iván Nabalón .....</i>	<i>27</i>
<i>Pura Strong.....</i>	<i>27</i>
<i>Carlos Sáez Quintero.....</i>	<i>28</i>
<i>Victor Morán.....</i>	<i>28</i>
<i>David Espejo .....</i>	<i>28</i>
<i>Leandro Pereira .....</i>	<i>29</i>
REFERENCES .....	31

## Introduction

---

Remote customer identification has been a long-sought dream for the finance industry. Up to now, companies have been held back by regulations when entering into online relationships with customers, largely by the lack of legislation and specific technology in the field. However, the need is pressing, in some cases because of the increased efficiency of online onboarding campaigns, or because of the benefits of digital transformation and cost rationalisation projects in the branch network, or because the booming Fintech industry is less constrained by regulation and boasts more aplomb in the decision-making process to that effect, thereby creating an unprecedented competitive environment. Remember, for instance, that there are already banks offering accounts and services entirely online, therefore competing in Spain with our banks.



*Electronic identification (eID) is the ability to demonstrate that a person is who he claims to be by using electronic means.*

Regulators recently ruled on this point with particular specifications on non-face-to-face relationships and especially on the characteristics that electronic means of identification must fulfil in order to be valid. This has thrust electronic identification technology into the limelight, along with the process known as *customer onboarding*, which in turn is part of an entire industry called *Know Your Customer - KYC*.

This *white paper* provides an insight into the current state of art in the finance industry and explains the business benefits and the laws that support electronic identification. The idea is for readers to gain

additional information that will help them in making decisions and also a headway with regard to projects like these.



*Know Your Customer (KYC) refers to the process that must be undertaken in legal and registered financial institutions to identify customers and ascertain relevant information before performing financial transactions with customers.*



## What is electronic identification?

Electronic identification is the **ability to demonstrate that a person is who he claims to be by using electronic means.**

This fact is demonstrated by means of a process that **links the person with an identity document**, with the requirement that this has a photograph and is of an authentic source. Identity documents issued by public bodies will usually be valid, which in the case of Spain includes the DNI (National Identity Document), the NIE (Foreign Resident Number) and passport. The identification process must verify the authenticity of the document and link to the titleholder with the identity he has declared.

## Why are these guarantees necessary?

The need to carry out an efficient identification of individuals is not a new requirement derived from the information society, but an established precedent in modern nations.

The creation of physical identification methods for national governments and administrative bodies to exercise their powers on society is a reality that became widespread during the twentieth century. Many and multiple systems have been developed to achieve this purpose. The fundamental aim is to determine that a person belongs to a group: associations; municipalities, communities, private businesses, etc.

**The main objective of identifying individuals is to create an environment of trust in which business can be conducted**, whether it is public or private. And over time, and seeing that threats in large communities or groups can be diverse and almost unlimited, there has been a surge in **preemptive identification, in an attempt**

**to prevent fraud** or criminal acts based on false identities. These cases triggered, for example, the new European regulations on money laundering and the financing of terrorism, which have had an impact on financial services.



*The main objective of identifying individuals is to create an environment of trust in which business can be conducted.*

Consequently, we have permission from regulators and the technical means to perform the electronic identification of customers and, for obvious reasons, where this process will have a more intensive application is in the "first moment of truth", as marketers say, or in other words, in the process of onboarding a new customer.



## Digital banking

---

Society is currently immersed in a true digital revolution. As happened with the agricultural and industrial revolutions, people say that this **digital revolution**, which is still in the making, **will overhaul society**. In this context, **financial institutions cannot remain impassive and 'miss the boat' that has had already caused tidal waves in other fields**, such as the music, transport and hotel industries, among others.

This digital transformation is taking place at breakneck speed, partly because the customers themselves are demanding and ultimately heading up this change. Now it is the customer who demands when and where they can interact with their bank, so they are mainly using digital channels.

If we add to all this the fact that banks' profit margins are shrinking and that new players are coming onto the scene (*Fintech* and Technology, among others), then it is essential to implement a digital strategy in financial institutions to adapt to the current situation.



*Now it is the customer who demands when and where they can interact with their bank, so they are mainly using digital channels.*

Banks are not oblivious to this fact and have stepped up their digital transformation. Classic business indicators have now been joined by brand new indicators, such as the number of online customers, to measure this digital adaptation.

All banks have transformed their services to offer them via digital channels. These new services provide a solution to the digital needs of their current customers, but how can they capture new customers?



*The digital revolution, still in the making, is overhauling society and financial institutions must adapt to this revolution.*

Two scenarios can be distinguished in the current situation: the onboarding of banked and of unbanked customers.

In both scenarios, the key lies in the identification, authentication and signature to determine whether the process can be completed from the digital channel itself or whether potential clients must be directed to other channels (losing the moment of truth in the process).

In the scenario of banked individuals, financial institutions have welcomed certain digital processes by adapting to current regulations (requiring transfers from another bank or delegating authentication to another bank at which the person is the primary account holder). This scenario is not proving to be hugely successful given its limited scope and the wariness with which other banks share customer data with the potential competition.

In the case of the unbanked, in general, the customer had to physically go to a branch or sign documents and deliver them to a courier.

It is clear that there is great room for improvement with regard to customer experience in both scenarios.

Technology can offer a range of electronic identification verification methods and ultimately enhance these processes. Today, with the latest changes in legislation, permission has been given to use video systems along with the signature of electronic certificates to close the onboarding process of the 100% digital customer.

## Business Benefits

### Improved Customer Experience and *Time to Market*

Electronic identification allows a potential customer to open a bank account or contract a high-risk financial service within seconds, thereby avoiding unnecessary trips (and wasted time) to the bank to provide ID or sign forms. The enhanced experience translates into greater convenience for the customer and greater efficiency for the bank.

The average electronic identification transaction time is measured in minutes, resulting in an economic benefit when compared to the days, or even weeks, that it takes for complex face-to-face processes at branches or through Premium courier services.

Let's look at some examples, such as the process of opening a bank account in at a street branch:

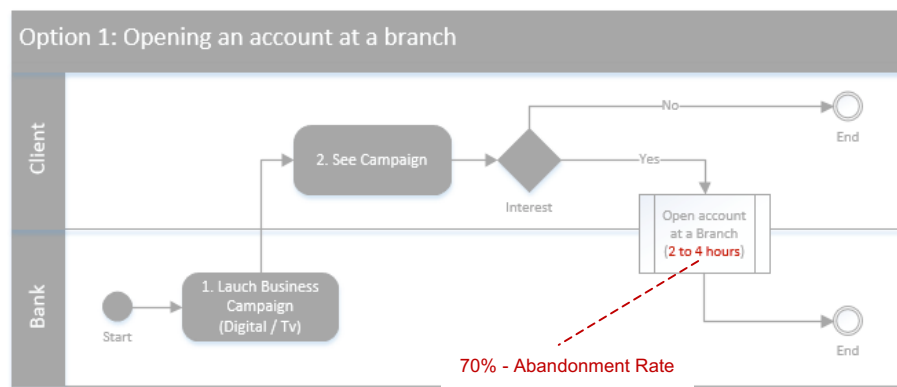


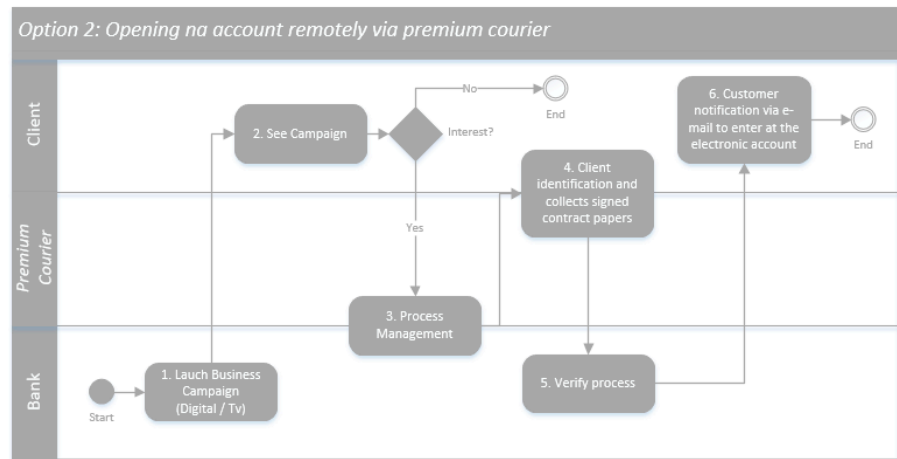
Illustration 1. Opening an account at a branch (Source: Business Case Institute)

Main disadvantages:

From the moment the customer is onboarded via a media campaign until they go to the branch, **the average abandonment rate is**

**around 70%.** With similar rates to this, the return of marketing campaigns can be improved.

**Inconvenience for the Customer:** when the customer goes to the branch, the process can take between 2 and 4 hours (journey to the branch, waiting to be attended, receiving information, identification process, printing of papers and signing).



*Illustration 2. Opening an account remotely via premium courier (Source: Business Case Institute)*

Main disadvantages:

Inefficiencies in the process: coordination and quality of courier service, waiting at home, planning deliveries. This translates to a **high cost and a user experience that could be improved.**

The **Time to Market** exceeds 15 days on average.

**Awkward process for the customer** - interactions with the courier at their home

## Experience of user with electronic identification.

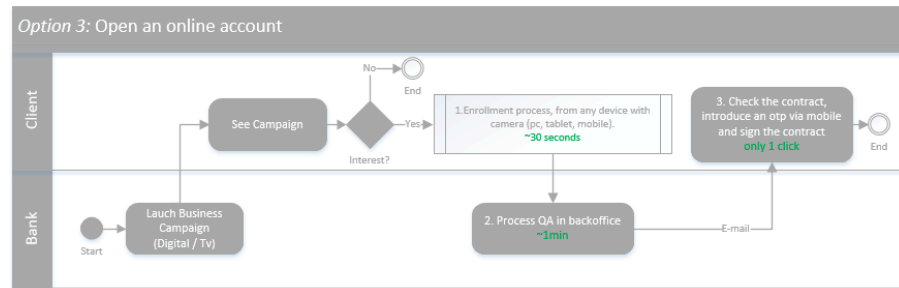


Illustration 3. Opening an account online (Source: Business Case Institute)

Main benefits:

**Comfortable and flexible process for the customer as it can be done from any device at any time.**

**The user experience is very rewarding and the process takes no more than 3 minutes on average.**

**The *Time to Market* plunges** and ends up being a question of minutes.

## Benefits

From a financial perspective, there are four ways of creating value in the company classified by the four types of **benefits** of a project, so value can be created through: **business increase, efficiency increase, costs reduction and/or legal compliance**

Implementing electronic identification led to the **identification and quantification (€) of 2 benefits:**

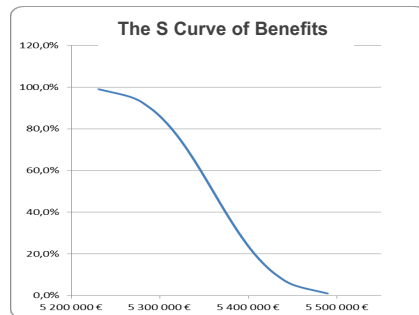
**Increased efficiency** by reducing staff time spent on the *onboarding* process.



Figure 10 — Penetration Diamond (Level 1), (Penaria, 2014)

**Costs reduction**, both current costs of the branch network and the hybrid process with the premium courier service.

Below is a detailed analysis of the involved **benefits** and **costs** to provide the **calculation of Return on Investment (ROI)** for the case of a bank with 20k new customers per year.



Risk	Benefits	Confidence
1,0%	5 230 867 €	99,0%
5,0%	5 268 698 €	95,0%
10,0%	5 288 865 €	90,0%
15,0%	5 302 472 €	85,0%
20,0%	5 313 286 €	80,0%
25,0%	5 322 564 €	75,0%

By simply considering the two benefits listed above, it can be concluded that the implementation of electronic identification achieves a **one-off profit of ~ 5.3K EUR at 3 years**, with a degree of **85% trust** and considering a **risk of 15%**.

Note 1: figures for a customer who has 20K in new accounts per year.

Note 2: the analysis and calculation of the mentioned benefits are based on real cases in companies in the finance industry, observation mechanisms and techniques, *expert judgment* and comparison with market benchmarking.

## Return on Investment (ROI)

Considering the analysis of benefits and the analysis of costs, it is possible to reach the following conclusion:

NPV (Net Present Value) =	3 042 184 €
ROI (Return on Investment) =	100,0%

## Other benefits

**Extends the natural reach of your target market**

Identification with legal guarantees from customers, without the restraints and hindrances of their current organisation, such as the need for branches wherever they conduct business, will provide a more global view of their business and facilitate geographic dispersion from day one, as physical boundaries cease to exist.

### **Increased ROI in onboarding campaigns**

Electronic identification increases the return on investment in advertising campaigns aimed at attracting new customers. Electronic identification decreases the abandon rate because a person can complete the process "there and then" and "online", without the need for complex forms and deferred processes, or the inconvenience of visiting a branch.



# Money laundering and identification

---

Financial institutions hope and trust that the presence of "criminals" among their customers is non-existent. Unfortunately, the reality is otherwise: banks are increasingly coming across individuals or entities, let's call them "undesirables", which highlights the failure to check identification in advance, and exposes the failure to comply with current legislation against money laundering.

Money laundering is the process of integrating financial income, or cash, from illegal activities in the economy, while attempting to shirk legal and tax obligations, and hide them from the authorities. Money laundering can originate in a multitude of criminal activities; not only does money laundering come from drug trafficking and the sale of illegal arms, but also from such everyday things as buying and selling shares online or triangular trading between Internet companies in Europe and tax havens, and other transactions with major profits.



*Money laundering is the process of integrating illicit financial income and hiding it from the authorities.*

There is another preconception about "dirty or black" money and that is regarding its origin. Black money does not only come from risk areas such as tax havens, Latin America or Africa. In an interconnected world with data networks, black money can come from anywhere in the world and in a matter of milliseconds.

Funds reach an entity because an individual brings them, but who then seeks to identify the individual who brings these funds? Well, financial institutions are responsible and also obliged to comply with the legislation of the Money Laundering Prevention Service

(SEPBLAC, in its Spanish acronym) with respect to customer identification, as entities subject to such obligations.



*SEPBLAC: Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences, a body of the Bank of Spain.*

What SEPBLAC requires is **customer identification** at the start of the relationship and the subsequent monitoring of suspicious transactions, to assess whether we accept it or not, while issuing the aforementioned report on suspicious transactions. Here ends the work of the financial institution, with the investigation - exclusively by the public authorities - starting at this point.

## **The advantages of electronic and centralised resources**

Electronic media and the preservation of evidence throughout the process always provide advantages in the forensic field when analysing problems. The case of identification is no exception. For example, new identification systems are based on a video recorded along with the registration process. This means that for a person to perform a fraudulent act they must stand in front of a camera and be recorded, which in itself is an important deterrent against fraud. Additionally, these systems link up to various authentication factors, always linked to third parties, such as email or a mobile phone number. In an investigation into fraud or crime, the evidence collected and stored by the electronic process provides additional evidence for courtroom trials.

The other major advantage of electronic media is that it is changing the identification model. We are shifting from the current

decentralised method to a new centralised one. Currently the weakest link of identification lies in the weakest person, who may be the busiest or least qualified, which drastically multiplies the possibilities of fraud. In this sense, the new electronic-based model moves the verification of subject's identity to a secure method that is identical for each customer, thereby ensuring consistency in data collection, control and accuracy in the verification process, and error detection, which all boost the security of the overall process and integrity in the chain of custody.

## Developments in the legal field

---

Until the approval of **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 (eIDAS), no real concern had been shown for electronic identification or the provision of services aimed at creating legal certainty regarding the remote identification of people.



*The electronic ID card has not been efficiently implemented in the social fabric.*

Although we have had them for a decade, these systems have not been efficient. ID cards have been used by the private sector to identify people in a physical terrain, but this has not happened with the electronic ID card. We could also mention the use of digital signature certificates, where the complexity of use and high cost of deploying and integrating these technologies - designed for signing documents - into identification processes has become inapplicable. Therefore, companies in the private sector needing to identify people or relate with them in virtual environments have been using physical identification systems at branches, or the so-called hybrid system: using a third party with identification capability, such as a courier or the certified post service. This obviously delays the process of onboarding customers and slows down the business operations of companies.

In addition to this transaction of the commission, the Executive Service of the Commission for the Prevention of Money Laundering

and Monetary Offences (SEPBLAC), part of the Bank of Spain, based on Article 21.1.d), which regulates business relations and non-contact operations for entities subject thereto, recently published, with effect from 1 March 2016, **an authorisation for the non-contact identification procedure via video conference.**

The approval of the Community Regulation and the SEPBLAC authorisation sheds some light on the electronic identification process, specifically regulating this circumstance and determining the processes and technical conditions to be adopted in the identification process so that they have sufficient legal certainty.

## **European Regulation on Identification and Electronic Signature (eIDAS)**

With the eIDAS regulation, the European Parliament and the European Commission have taken a firm step in the field of electronic identification, providing support which will strengthen customer relationships which require the utmost trust and with cross-border effects. Consequently, the eIDAS also helps complete the digital transformation of companies and expand their business without local obstacles in this important matter.

The benefits for the authorities are very high, since the eIDAS is the first step towards creating a single community-wide identity document, with the advantages in terms of efficiency which this would have in the field of e-government and open government.

For businesses, the possibilities are also far-reaching and its benefits obtainable in the short term because it allows companies to expand their horizons through digital channels and provide businesses with maximum guarantees throughout the region, without limitations and with a start and an end to the online channel.

A very wise move by the Commission was the creation of a regulation, since its application is direct and not, as in previous attempts, through directives. At the same time its scope is cross-border, thereby facilitating business in any European member state.



As if that weren't enough, in July 2016 the eIDAS repealed local laws and the European Electronic Signatures Directive.

*The eIDAS is the first step towards creating a single community-wide identity document with clear advantages in the field of e-government and open government.*

With regard to identification and following the model that had already been stated in the electronic signature directive, different levels of security are set for electronic identification means - low, substantial and high - in order to determine the legal effectiveness of identification. We believe that these three levels of security, as well as the specifications made through the 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, are a very wise move when putting particular specifications on the table which lead to electronic identification.

One of the main advantages revealed upon interpretation of the eIDAS is the adaptation to the times, as the security process in identification prevails regardless of the technology and type of use. While the SEPBLAC authorisation, copied from the German regulator BAFIN and now over 2 years old, requires the use of video conferencing, with the obligation of one person present throughout the process, the eIDAS puts more focus on the security of the process and less on where and how human resources should be located.

And perhaps the **greatest impact** that the eIDAS will have in business is that it will become, as current signature laws did, the **de facto standard** for the most secure trust services **in the world**. This entails an important advantage for large corporations, as they will be able to implement solutions that provide a comprehensive response to their business in the area of third-party identification and electronic signature, both for their customer relationship projects and their transformation projects of internal processes with employees, suppliers and shareholders. The scope and opportunities are therefore expanded.



*The eIDAS will become the de facto standard for most secure trust services in the world.*

## **Regulation on the Prevention of Money Laundering**

The new regulation on the prevention of money laundering and financing of terrorism, implementing Law 10/2010, places an emphasis on financial transactions which affect many companies as entities subject thereto, from traditional banking or the emerging *Fintech* industry to insurance companies or real estate activities.

This section provides details of Article 21, which stipulates how to identify individuals for non-contact business relationships.

We would like to highlight various provisions in Article 21:

Provision a) confers the ability to identify customers upon current legislation on electronic signatures. From this point we would encourage the reader to refer back to the previous article implemented by the eIDAS, the regulation itself and the implementing regulation that describes the specifications and security standards in eID means, which from now on will apply identification and electronic signature technology to undertake customer identification projects.

We would also like to highlight provision d) The identity of the customer is accredited by other secure procedures for customer identification in remote transactions, provided that such procedures have been previously authorised by the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (hereinafter, Executive Service of the Commission), as is the case of the new authorisation for customer identification by video conference, published on the SEPBLAC website on 1 March 2016. Said authorisation, much more lax in specifications than the eIDAS implementing regulation on levels of security in eID, regulates and complements customer identification.

Finally, and also to be taken into account, Article 21 requires obliged subjects, in any case and within one month of creating the non-contact business relationship, to obtain a copy of the necessary documents from the customer for the purposes of due diligence. This obligation can be conducted in a very efficient way by using identification technology currently on the market.

## **Corporate Criminal Liability**

No less important is the role that online customer identification enables regarding the improvement of the identification process, from the point of view of the criminal liability of companies and their managers.

On 31 March 2015, the Official State Gazette of Spain published the Reform of Criminal Code as amended by Organic Law 1/2015, of 30 March, in force since 1 July 2015. This amendment extended several types of crime applicable to legal entities and introduced the exemption from liability for them in certain cases. In particular:

1. The board has adopted and effectively implemented, before the crime, models of organisation and management including surveillance measures and appropriate controls to prevent crimes and reduce the risk of further crimes being committed;

2. There should be an independent representative within the legal entity with autonomous powers to monitor the operation and performance of implemented prevention model. We will refer to this representative as the Compliance Officer, without specifying for now whether this refers to one or several natural persons integrated into a department or commission.
3. The perpetrators must have fraudulently eluded the organisation and prevention models implemented in the legal entity.
4. There shall have been no omission or insufficient exercise by the 'Compliance Officer' and, therefore the legal entity, of the roles of monitoring, surveillance and control\*.

In this context, having the very latest means and technological processes, which have been verified by the authorities as optimal from the point of view of safeguarding identity, retaining documents, supporting controls and continuously monitoring the customer, enhances the image of good governance.

All this is unequivocal proof of the good work and engagement of senior management in the culture of compliance and of the appropriate management of the limited resources of the entity.

In that respect, we should consider that these new technologies can ensure compliance more efficiently and thus avoid reputational risks and unnecessary penalties, or even the limitation of business in certain geographical areas, to the extent that they help the implementation of new regulations requiring **automatic exchange of information models**, as are the **FATCA** ( *Foreign Account Tax Compliance Act*) and the **CRS** (*Common Reporting Standard*), to the requirements of customer identification and reporting established therein.

In this sense, the opportunities provided by new digital technologies in the *onboarding* process when identifying the source of the identity card, nationality and/or when performing certain cross-validations of the data contained in documents submitted by potential customers, in line with those which the entity may already have internally or obtain

thanks to external sources, shall significantly streamline these procedures.

# Considerations when selecting means of electronic identification

---

We have prepared a series of recommendations which may help when selecting electronic identification solutions.

## Levels of security in eID

There are two models and levels of security in electronic identification:

Solutions with a **low level** of security in the identification process, based on images/selfies. These solutions are being accepted as valid for accreditation processes (not identification) for dealing with low-risk customers and under no circumstances for transactions of greater than €999, according to the regulation on the prevention of money laundering. These solutions are interesting when it comes to digitising the entire identity verification process (identity card, details on the document, photographs, etc.) and are proving very popular in low-risk processes such as car or home insurance policies and consumer loans of up to 999 euros.

**High level of security in the identification process, based on video models.** These solutions are being adopted in any identification process for parties liable to any risk, because not only do they allow for the digitisation of the process but also the verification of the identity and binding nature of a subject to their identity card. These solutions are also becoming more sophisticated, further enabling the digital accreditation process, with the collection of all documents and information necessary for court proceedings (remember here the obligation set forth by Article 21 in any of the cases).

## Authentication / Biometrics

There is much confusion in the market of electronic identification solutions, with identification solutions often being mistaken for authentication / biometrics solutions.

Authentication solutions do not set out to identify people *per se*, but to show that the person who at any given time signs into an authentication system, which can be biometric (voice, pulse, fingerprint, iris, face, etc.), is who will do so again on another occasion, using either something they have or something they know.

Identification solutions set out to gain the utmost assurance of the person's identity by linking a physical person with their real identity, a process performed by connecting up with the valid identity document issued by the State to which they belong.



*Identification solutions set out to gain the utmost assurance of the person's identity by linking a physical person with their real identity.*

Identification is often a process prior and complementary to authentication, but never a substitute.

## Non-repudiation in express consent. Digital signatures

In the onboarding process we should also consider the process of formal acceptance or express consent of the contract or framework contract with the customer. A bank may identify a customer with high levels of confidence, but this, in isolation, does not guarantee a non-repudiable chain in the relationship itself, since a customer could

accept they are well identified, but not partially or fully take responsibility (repudiate) for the contractual conditions of a product, for example. And if this is the case and there is a problem which ends up in court, the liable party will be unable to defend themselves. Hence the importance, aside from identifying the customer, of implementing mechanisms of express consent and non-repudiation through digital signature mechanisms. This way we will ensure the integrity of the whole onboarding process and "non-repudiation" from the start to the end of the transaction.



# About us

---

## Authors

### Iván Nabalón



Expert consultant in the digital economy, Founder of Civitana.org and CEO of Electronic IDentification (eID, [www.electronicid.eu](http://www.electronicid.eu)).



[LinkedIn profile,](#)



Email: [ivan@electronicid.eu](mailto:ivan@electronicid.eu)

### Pura Strong



Lawyer specialising in finance, tax law and commercial law. External expert of the Spanish Service for the Prevention of Money Laundering (SEPBLAC). Financial Advisor series: 6, 66 and 7 of NASDAQ; CEO of the Bar Association; Founder of Strong Abogados and Advisor to Wong and Fleming LLP in the US. Master in Company Tax Systems (UPM); Postgraduate in Banking Law and Finances, Harvard University. CEO of the Spanish-American Advocates Association.



[LinkedIn profile,](#)



Email: [pstrong@strongabogados.com](mailto:pstrong@strongabogados.com)

## Carlos Sáez Quintero



Managing Partner of Trebia Abogados and Trebia Seguros; member of the Illustrious College of Advocates in Madrid; Master of Advanced Studies in Information Technology Law from the Complutense University of Madrid; Bachelor of Laws from the Autonomous University of Madrid; Master in Information Technology Law and New Technologies from the Carlos III University of Madrid.

He is a teacher, speaker and frequent conference giver in different masters and seminars in the legal and IT fields, and mentor of different incubation and entrepreneur acceleration projects.

[LinkedIn](#) profile,



email: [carlos.saez@trebiaabogados.com](mailto:carlos.saez@trebiaabogados.com)



## Victor Morán



Expert consultant in digital banking specialising in innovation in the finance industry. Digital Banking Manager at Everis.

Certificate in Customer Experience from AEDEC. Currently studying management programme in Financial Technology and Innovation at IEB.



Link [LinkedIn](#),



Email: [vmoranro@everis.com](mailto:vmoranro@everis.com)

## David Espejo



Founding Partner of Expert Witness Forensic & Compliance. Compliance specialist for the finance industry specialising in money laundering, market abuse, corporate criminal liability, internal control, and review of procedures. Researcher in areas

covering accounting, economics and financial irregularities.

Independent expert, ratifying before tribunals and arbitration courts (trading of swaps; floor clauses; preferred stock; non-cumulative equity-linked notes; structured products; restructuring processes; feasibility and rollover plans; money laundering; fraud; conflicts between parties; calculation of consequential damage and loss of earnings; valuations, etc.).

Monitoring Trustee for the European Commission in the refinancing process of the Spanish banking system.



[LinkedIn profile,](#)



Email: [de@expert-witness.es](mailto:de@expert-witness.es)



## Leandro Pereira

CEO of Winning Scientific Management and Founding Chairman of BCI - Business Case Institute.

With over 14 years' experience in executive management and senior management at consulting firms, he currently holds the following positions: Assistant Professor at ISCTE Business School in the areas of Business Strategy and Project Management; Director of the Executive Master in Programme and Project Management at INDEG-IUL; Chairman and Founder of PMI Portugal Chapter and Chairman of ASP Iberia (Association for Strategic Planning). Leandro Pereira holds a PhD in Project Management; a

Master of Advanced Studies in Knowledge Management; a PMP certificate from the PMI, and is a certified ROI Professional.

He actively participates in developing the area of Profit Management, being the author of the International BCBOK® Guide to the Business Case Body of Knowledge.



[LinkedInprofile,](#)



Email: [leandro.pereira@winning.pt](mailto:leandro.pereira@winning.pt)

## References

**Law 10/2010, of April 28**, on the Prevention of Money Laundering and Financing of Terrorism. (Official State Gazette 29/04/2010) (Law 10/2010).

**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. (EIDAS or EU Regulation 910/2014).

**COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 COMMISSION, 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.

**ROYAL DECREE 304/2014, of 5 May**, approving the Regulation of Law 10/2010, of April 28, on the Prevention of Money Laundering and Financing of Terrorism. (Official State Gazette 05/05/14) (Hereinafter, RD 304/2014 or Regulation 304/2014).

Authorisation of the non-contact identification procedure by video conference, of 12 February 2016, and effective from 1 March 2016. SEPBLAC.

*Know Your Customer - KYC* refers to the process that must be undertaken in legal and registered financial institutions to identify customers and ascertain relevant information before performing financial transactions with customers.