



European  
Commission

**Report on existing remote  
on-boarding solutions in the banking sector**

***ASSESSMENT OF RISKS AND ASSOCIATED  
MITIGATING CONTROLS, INCLUDING  
INTEROPERABILITY OF  
THE REMOTE SOLUTIONS***

December 2019

Banking and  
Finance

**An interactive version of this publication, containing links to online content, is available in**

**PDF format at:**

<https://europa.eu/!rj88wv>



*scan QR code to download*

**Report on existing remote on-boarding solutions in the banking sector:  
Assessment of risks and associated mitigating controls, including  
interoperability of the remote solutions - *December 2019***

European Commission

Directorate-General for Financial Stability, Financial Services and Capital Markets Union

European Commission

1049 Bruxelles/Brussel

Belgium

© European Union, 2019

Reproduction is authorised provided the source is acknowledged. For any use or reproduction of individual photos, permission must be sought directly from the copyright holders.

CREDITS

All images © European Union, except:

cover: © SIAMRAT.CH - stock.adobe.com

**Report on existing remote on-boarding solutions in  
the banking sector:**

**Assessment of risks and associated mitigating  
controls, including interoperability of the remote  
solutions**

**DECEMBER 2019**

**This report was prepared by the:**

**European Commission's Expert Sub Working Group 1, Electronic Identification and Remote Know Your Customer processes**

## **DISCLAIMER**

This report has been prepared by the project team in the context of the work of the European Commission's Expert Group on eID and remote KYC processes for the sole purpose of providing to the European Commission a snap-shot of existing remote on-boarding solutions (and the extent of their use by consumers) in the banking sector, including the identification and assessment of the risks and how these can be mitigated as well as interoperability and overall functionality perspectives at a certain point in time as it explores issues relating to electronic identification and remote KYC processes based on eIDAS.

The report has been endorsed in December 2019. It is based on information collected between June 2018 and January 2019 and it does not account for any modifications of the journeys described in this report after January 2019.

The European Commission's support for the production of this report does not constitute endorsement of the contents or conclusions. The report reflects the views only of members of the Expert Group, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

# Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>Chapter 1: Introduction</b> .....	<b>5</b>
Background .....	5
Purpose / Objectives .....	5
Scope .....	6
Limitations, Constraints and Caveats of the Report .....	6
Approach towards researching identity verification solutions .....	7
Structure.....	8
<b>Chapter 2: eID/KYC Assessment criteria</b> .....	<b>10</b>
Context.....	10
IA. Type and Content of Documents.....	10
IB. Video and Photo Capture .....	11
IC. Verification of the Validity and Authenticity of Documents .....	11
II. Identity of the Individual.....	12
III. Additional Considerations .....	13
<b>Chapter 3: Typical on-boarding journeys</b> .....	<b>15</b>
<b>Chapter 4: Overview of existing remote on-boarding solutions and the extent of their use by consumers</b> .....	<b>29</b>
The evolution of commercial remote identity verification solutions .....	29
Categorization of remote identity verification solutions .....	31
Coverage and extent of use of identity verification solutions.....	32
New and emerging innovative solutions for identity verification.....	33
Impediments to progress .....	34
Initial Conclusions .....	35
<b>Chapter 5: Risks associated with using eID and remote KYC identity verification solutions, and how those risks can be mitigated</b> .....	<b>37</b>
Introduction .....	37
Identity fraud risks .....	37
Detection and mitigation of identity fraud.....	39
Supplementary controls.....	40
Other risks associated with using identity verification solutions .....	40
How else can these risks arising in the use of identity verification solutions be mitigated? .....	42
<b>Chapter 6: Conclusion</b> .....	<b>43</b>
<b>Annex 1: Typical on-boarding journeys</b> .....	<b>47</b>

Journey 1: Cross Channel journey (Remote & Face to face Identification) .....	51
Journey 2: Remote On-boarding based on enhanced KYC measures (with or without electronic signature) .....	55
Journey 3: Entirely remote on-boarding journey supported by video conference and biometric identification (optional) .....	59
Journey 4: Entirely remote on-boarding journey supported by selfie and biometric identification .....	68
Journey 5: Entirely remote on-boarding journey resulting in a trust service delivery .....	74
Journey 6: Entirely remote journey using digital identity .....	79
Journey 7: Remote on-boarding employed by e-merchants using electronic wallet .....	95
<b>Annex 2: EU Mapping of the use of Digital Identity in bank account opening and the AML Regulations governing it .....</b>	<b>102</b>
<b>Annex 3: Detailed analysis of eID/KYC Assessment criteria .....</b>	<b>Erreur ! Signet non défini.</b>
Considerations and Regulation.....	105
IA. Type and Content of Documents.....	105
IB. Video and Photo Capture .....	108
IC. Verification of the Validity and Authenticity of Documents .....	110
II. Identity of the Individual.....	112
III. Additional Considerations .....	117
Risk Mitigation .....	118
<b>Annex 4: Existing EU Member states' AML regulations on remote on-boarding journeys.....</b>	<b>122</b>
<b>Annex 5: Digital On-boarding for Bank Accounts in Spain.....</b>	<b>176</b>



## Executive Summary

This report is the outcome of an assessment defined by the European Commission Expert Group on electronic identification and remote Know-Your-Customer processes.

Its Terms of Reference were to:-

1. Provide an overview and assessment of existing remote on-boarding solutions and the extent of their use by customers in the banking sector,
2. Identification and assessment of the risks and how these can be mitigated
3. Perspectives on the[ir] interoperability and functionality

This would serve as a basis for a follow-on report, including recommendations on best practices for remote on-boarding in the financial sector and how eIDAS and other innovative processes may be used to comply with AML requirements. In parallel a further deliverable was to make recommendations for conformity assessment principles for on-boarding systems and electronic identity management systems.

At a high level, the impetus for doing this research is best summarized through the eyes of the customer, along with the European Commission's perspective that its European citizens can be better served through addressing challenges and friction points in cross border account opening and preventing regulatory arbitrages.

A customer, either an individual or legal entity, may have cause to open a financial account in a different member state. It could be convenient for the customer and safe for the financial institution if the process for verifying the customer's identity used an electronic identity token, providing them with an instant, streamlined and low risk experience. This is far from reality today, though many of the building blocks necessary to achieve this aim are available domestically and to some extent internationally.

In the absence of an EU-wide interconnected network of electronic identity solutions<sup>1</sup> serving both public and private sector purposes, **EU customers can be identified in non-face-to-face onboarding processes, apart from methods relying on the identification made by a first bank, with commercial identity verification solutions.** These are technology intensive services sold to financial institutions to help them verify the identity of their customers. **New technologies solutions the more generally use mobile phone<sup>2</sup> connecting the financial institution with the customer but could also use desktops, and capturing images of their identity documents or data within electronic identity document, as well as capturing images of the customer's face to help verify identity and reduce the risk of fraud.**

In some cases, identification can be achieved through even more streamlined processes by drawing on the depth of data in Credit Bureaus, though these solutions are not available across all member states.

This report discovered that domestic customers are served with a variety of solutions to help identify them remotely, and many of these systems can also work across borders. However, the processes needed to fully on-board a new customer are broader than just identity checks, and other hurdles such as credit referencing, address verification, employment checks, income verification, signing, and

---

<sup>1</sup> eIDAS offers a interoperability framework and a mutual recognition for public and private (on a voluntary basis) solutions

<sup>2</sup> PC can also be used, alone (with or without card readers, those depending also on countries) or in journeys proposing multiple devices use.

fulfilment, must also be addressed to complete the process. Electronic Identity systems could help with some of these challenges, but not all.

There is a commonly held view that electronic identity is an important enabler in achieving the goal of pan-EU access to cross-border financial services, but it's not there yet. Public and Private sector cooperation is necessary for 'federated identities' to work at scale, and alignment is necessary between the policies for identity proofing in eIDAS and those in anti-money laundering (ML) and combatting terrorist financing (TF) laws. Interoperability between State based electronic identity systems and also private sector electronic identities is key to solving the challenges of cross border identification. Doing these things should fuel the Return on Investment necessary for firms in the private sector to invest in using them.

This report, and its annexes, contain a wealth of information and perspectives on varying approaches towards identity verification, the risks associated with these systems, and how they can be mitigated. We expect that this will improve the awareness firms have on what is possible today and inform the EU Commission about the key considerations for developing a more integrated identity verification system in the future.

***In summary, the report has identified several key findings:***

- Firstly, all remote on-boarding solutions come with a certain set of risks and while security and KYC measures can be put into place to mitigate the risks, it is important to ensure that the measures are **proportionate** to the risks presented. Excessive measures, which go beyond what is necessary to protect a valid public interest such as the prevention and detection of money laundering and terrorist financing, may also adversely impact customer user experience. A balance will need to be struck between customer adoption and experience vs. meeting security requirements. In this respect, the Estonian AML regulation is a good example of proportionality. National electronic ID can be sufficient in some cases, but only to a certain extent. Once the account is used beyond a pre-determined level, the identity of the customer is verified more stringently using another identification process, such as video or face to face identification. Portability of identity and KYC/CDD attributes could be a mean for all at once improving and securing on boarding processes. See on this topic the complete analysis in Sub Group 2 report.
- Given the fact that transactions take place remotely that may increase AML/FT risk, especially massive fraud risks, and also given use of new technologies entailing new types of frauds, also potentially evolutive, AML/FT risk should be monitored, in coordination with national security agencies. These risks must be taken into account by countries and Financial Institutions in risk based approach (distribution channels) in particular regarding other factors that might lead to lower risk assessment in not considering them.
- It is recognised that any on-boarding solution can be compromised given the right incentive. The key to establishing a secure process is through the use of several distinct identification measures (e.g. cross referencing of database, mix of human intervention and biometrics) for increased risk situations. **Watertight security is rarely achieved in a single identification method and risks are better managed through a combination of identification measures.**
- All the currently remote on boarding journeys in Europe can be classified under 7 typical on boarding journeys, broadly and in depth presented in this report, ranging from the more basic one, a cross canal journey (partly in face to face), to the more integrated one relying on eIDAS digital identities. Differentiation is based on the way customer identification is made, i.e. how does he prove he is the person he claims to be. On boarding journey 7 more precisely insists on commonly used identification solutions by Payment Services Providers within a typical e-money / e-wallet on-boarding journey.
- Identification methods may include face to face (for cross channel solutions), reliance on identification already made by a preceding bank where customer already has an account through a payment mean of this bank, use of new technologies means like video conference, or digital identification with electronic identities. There can also be a combination of certain of these identification means, or additional external sources requests, such as credit agencies, for applicant provided information and identity data verification.



- Journeys assessment under eID/KYC criteria show a comparable eIDAS Substantial minimum identification level, all journeys reaching this level of confidence, provided that they fulfil AML regulation, or AML authorities guidelines conditions, and provided that all countries apply AML regulations in the same way (see below). For journeys directly using eIDAS electronic identification means, level of assurance High can even be reached.<sup>3</sup> However excepted in case of direct use of eIDAS electronic identification means, due in particular to technical solutions choices, and on effectiveness of what is concretely made, it is important to stress that the statements on each achievable eIDAS LoA is only an estimation of the maximum level achievable under several assumptions. Consequently, this document does not provide a definitive statement of an eIDAS LoA level for such precise all onboarding practice, whose assessment should be effectively done.
- Based on eIDAS rules, followed assessment method considers the two identification steps: ID document verification (composed of ID document authenticity and validity verifications); and verification that the applicant has the claimed identity. Should also be verified (which was not made as outside of the scope of this study being an analysis of what could be observed), that it is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. UK JMLSG guidelines have also been used and presented in this report. They make special considerations in use of electronic sources as independent and reliable for identification purpose. Typical on boarding 7 more precisely describes this approach.
- AML/CFT (“Combating the Financing of Terrorism”) rules can insure a certain harmonization between journeys, to the extent however that it is born by a directive, and a full harmonization could only be insured by a regulation. Some measures as a required payment issued from or to another bank account held by the applicant are observable in Typical on boarding journeys 2 and 7. However as former KYC could have relied on several [practices depending on countries, not all reaching substantial LoA, it should be necessary to carry on risk-based approaches according to countries, or get full harmonization of KYC requirements.](#)
- Regarding certain observed journeys using eIDAS electronic identities (Typical on boarding 6) an AML/CFT risk based approach had been probably done considering *Product, service, transaction or delivery channel risk factors*, or *Customer risk factors* leading to potential higher risks assessment. As a result, enhanced identification proceeding was observed for non-resident despite their use of eIDAS level High digital identities.
- At present, the ability for financial institutions to access and read the chip containing identification data within national electronic ID documents are constrained due to restrictions in the availability of Near Field Communication<sup>4</sup> within some types of mobile devices, and possibly to restrictions pursuant to European regulation regarding electronic **Regulation on strengthening the security of identity cards of Union citizens and of residence documents, limiting access to biometrics data contained in the chip for data protection purpose**<sup>5</sup>. Allowing financial institution

<sup>3</sup> See in particular page 15 on this Level of Assurance Level Substantial assesement conditions.

<sup>4</sup> Regarding NFC see See also on this subject eIDAS Cooperation Network Decision 01/2019 (on the need for open access to NFC interface to support secure mobile use of electronic identity means):

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=100663614>

[Also](#) note new Apple developments at the NFC interface allowing the use of eID with Apple iOS13.

<sup>5</sup> For chip access possible restrictions, see:

French regulation Décret 2005-1726, 30 december 2005 (Art 20 and 21):

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000268015&categorieLien=id>

reading information contained in the electronic chip for limited purpose of Anti Money Laundering, to proceed customers high level identification.

- Asking for developing stronger collaboration between public and private sector to the extent of what is legally feasible in each Member State, in order to allowing financial institutions access to **national ID databases** for authentication and validity checks purposes will greatly enhance the security of the customer journeys and advance interoperability of digital identities among Member states.
- The role of **public and private co-operation** in digital identity management is paramount to advance interoperability and achieve the scale of adoption that is fundamental to any successful digital identity scheme. A **compelling and positive commercial** model will need to be developed to drive adoption across the private sector.
- It should be made mandatory for e-commerce (or other private platforms) to accept at least one EU EIDAS-based e-ID solution. Mandatory acceptance of solutions would ensure a large footprint
- **New Technologies** – AML/CFT regulations should be sufficiently receptive towards the use of future identification technologies that may not be in place at present and to remain technology neutral. In addition, to the extent that being compatible with national regulations and regulators' positions, the creation of a new **pan-European regulatory sandbox** can be a great tool to facilitate, promote and accelerate innovation in the financial sector, stimulate competition and deliver new customer benefits.
- **Data protection** and digital identity management goes hand in hand. Data protection should be at the heart of any trusted digital identity framework and this will need to be reinforced to engender trust among the customers and encourage mass adoption of digital identification processes.
- Identity verification policies vary between Member states, owing largely to different regulations relating to identity verification and National capabilities and convention in how a customer's identity is verified. There is scope to explore the possibility of further **harmonizing the rules and regulations** around identity verification with the objective of advancing interoperability.
- Further harmonization can also be reached by moving towards mutual recognition of different types of identity verification done to the same levels of security, underneath the umbrella of international and national legislation and regulation that allows for this variation in specific approach. This decentralised approach also has the added benefit of enhancing security by reducing reliance on and exposure to attack that would be true if there were one single method regulated. eIDAS framework would permit this mutual recognition.

Lastly, remote on-boarding solutions may satisfy bank's identification and verification (ID&V) requirements, however, it is worthwhile to note that this covers only one aspect of the process required to on-board a customer. Consideration should be given to collate a wider range of data to satisfy KYC requirements, derived from either the ID&V process or other established sources, to generate an end to end, complete and holistic customer profile. Sub Group 2 report makes an in depth exploration for these possibilities.

---

See also European regulation Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (Article 11 § 6):

<https://euroalert.net/oj/80440/regulation-eu-2019-1157-of-the-european-parliament-and-of-the-council-of-20-june-2019-on-strengthening-the-security-of-identity-cards-of-union-citizens-and-of-residence-documents-issued-to-union-citizens-and-their-family-members-exercising-their-right-of-free-movement-text-with-eea-relevance>

## Chapter 1: Introduction

### Background

This remit of this report was defined by the European Commission Expert Group on electronic identification and remote Know-Your-Customer processes (EG)<sup>6</sup>.

The European Commission Expert group was established in December 2017 to provide expertise to the European Commission as it explores issues relating to electronic identity, such as the portability of electronic identification (eID) solutions and remote Know-Your-Customer (KYC) capabilities, to understand the impediments and solutions to easier account opening across Member States. This is in support of the Electronic Identification and Authentication services (“eIDAS”) that seeks to establish a single legal framework for recognising electronic signatures and identities throughout EU and part of the wider framework to create a single digital market.

To achieve the above objective, the EG has created two sub working groups to explore various themes on electronic identification and Know your Customer portability, with the view to expedite and facilitate cross border and cross sectorial use of eID in financial institutions.

The members of the Expert Group agreed on the Terms of Reference for this sub-group, which is to produce:

1. A report that provides an overview and assessment of existing remote on-boarding solutions (and the extent of their use by consumers) in the banking sector, including the identification and assessment of the risks and how these can be mitigated as well as interoperability and overall functionality perspectives.
2. This report should serve as a basis for a follow-up report, including recommendations on best practices for remote on-boarding in the banking sector and how eIDAS and other innovative processes may be used to comply with AML requirements.
3. In parallel, recommendations for conformity assessment principles for remote on-boarding systems and electronic identity management systems.

This report focuses on the first of the deliverables within the ToR, summarising the findings from the more detailed reference materials accumulated by members of the sub-group, and provided to the European Commission by commercial providers of identity verification solutions.

### Purpose / Objectives

This report is the output of one of the working groups and seeks to address the following objectives.

1. Overview of existing remote on-boarding solutions and the extent of their use by customers
2. Risks associated with using those solutions and how those risks can be mitigated
3. Perspectives on the[ir] interoperability and functionality

In order to give context for the use of such identity verification solutions, the sub-group has collated, documented and assessed the main on-boarding journeys in which identity verification solutions are used. There is a wealth of valuable information in this analysis, though it is considered too detailed for the main body of the report and is available for reference purposes within Annex 1.

---

<sup>6</sup> Article 8 Commission Decision C (2017) 8405 final setting up the Commission expert group on electronic identification and remote Know-Your-Customer processes (*eID/KYG EG*), and point 6 of its Rules of Procedure.

## Scope

The scope of the report includes financial institutions, supervisory bodies, national and European regulators in the banking sector.

Dimension	
Products and services	The study is focused on the remote on-boarding solutions employed by the retail banks, and e-commerce payment providers, specifically on customer due diligence and know your customer requirements  In scope: Natural and Legal persons
Supply and demand side	The study is mainly focused on the banks and financial institutions in the EU that can benefit from the use of eID means, or are part of eIDAS schemes.  Remote on-boarding technology solutions in existence at time of research are in scope. Proof of concepts / untested technology are out of scope for purpose of this report.
Time	The report covers pertinent national AML rules and best practices existing at the time of conducting the research (March 18 to April 19) as well as observations of ongoing trends and envisaged changes.  Even though at the time of writing this report, the EU Member states have not transposed the 5 <sup>th</sup> AML Directive into their national laws, this report has been written with the 5AMLD <sup>7</sup> in mind.
Jurisdiction	The geographical scope of this report is the European Union.

This report includes the results of the analysis conducted between the inception meeting of this project that took place in Brussels on 9th April 2018 and the date of submission of this draft report in May 2019.

## Limitations, Constraints and Caveats of the Report

- Limitations

Due to the vast number of remote on-boarding solutions offered in the market and the resource constraint of the team, the overview and assessment of remote on-boarding solutions was based largely on open source desktop research, materials provided to the European Commission Expert Group by commercial solution providers, and knowledge of the EG members. While every effort is made to collate information on the more commonly used types of identity verification solutions, the level of innovation in the marketplace is high, and it is possible that in collating the information from desktop research that additional remote on-boarding solutions may be available but not considered.

---

<sup>7</sup> Non-face-to-face business relationships or transactions, are considered as potentially higher risk, unless certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognized, approved or accepted by the relevant national authorities” are applied.

However, one of the advantages of an 'expert group' is that it can make quick and reliable progress into analysing the subject matter because its members have been selected based on their experience and expertise in the topic. The disadvantage is that the report may lack empirical evidence to further support the key findings/observations.

It is the responsibility of financial institutions using identity verification solutions to ensure they are used in a way which minimises the risk of mis-identifying the customer. Many types of innovative identity verification solutions are configurable to meet the needs and risk profile of a particular Firm, so blanket statements cannot be made as to whether a solution is 'compliant', because that depends on the context of its use and the configuration of such a solution. Therefore, reference is made to the European Supervisory Authorities' 'opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process<sup>8</sup>', which will help Firms achieve compliance.

- Constraints

It is not the intention of this report to provide a technical opinion or provide recommendations on the existing remote on-boarding solutions. It should be noted that at the time of writing this report, Security agencies guidelines regarding eIDAS schemes or innovative solutions have yet to be published (e.g. French National Cybersecurity Agency, German Federal Office for Information Security), which have limited the ability of the Experts to analyze the remote on-boarding solutions. The comments made by the Experts within the sub-group on commercial solutions are intended to help advance from theory to practice, promoting questions, considerations and risks, but without necessarily reaching firm conclusions.

In addition, the sub-group lacked data on the scale of cross-border account opening, and the extent to which eID solutions are currently used between citizens and service providers in different member states. Addressing this through a survey of eID solution providers would help establish if aligning the identity proofing requirements for eID's with the identity proofing requirements in AML Directives will make a meaningful difference in facilitating cross-border account opening and enhancing competition in the marketplace.

- Caveats

Lastly, analysis, opinions and conclusions included in this document represents the collective opinion of the Experts within the European Commission Expert group sub-group and do not represent the official view of the organizations that the individual Experts work in. It is noted that the report has been officially endorsed by the members in December 2019.

### Approach towards researching identity verification solutions

In order to understand the risks, mitigating factors, and functionality of identity verification solutions, the sub-group researched and collated materials from Financial Institutions, Regulators representing the Expert Group Money Laundering Terrorist Financing, Supervisors, and Commercial solution providers. This formed a reference base of information comprised of three parts:

#### A. eID/KYC assessment criteria

In this task, an eID/KYC\_evaluation grid was created to support consideration of any remote on-boarding solutions. The matrix is based on **Commission implementing regulation (EU) 2015/1502 of 8 September 2015** (Annex paragraph 2.1), and **eIDAS Cooperation Network guidelines** (*Guidance for the application of the levels of assurance which support the eidas Regulation*). It is conceived according to on boarding processes, in order to evaluate providers solutions, and is focussed on identities remote

---

<sup>8</sup> **JC 2017 81** OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)

registration, and not on further authentication, nor on other CDD (Customer Due Diligence) and ECDD (Enhanced Customer Due Diligence) attributes collection.

This then drew references from the national private sector initiatives such as the European Banking Authority (EBA<sup>9</sup>) opinions and UK Joint Money Laundering Steering Group (JMLSG<sup>10</sup>) guidelines. This eIDAS assessment criteria was further considered against relevant European AML regulations corresponding to eIDAS prescribed measures (even if AML regulation have not been considered in regard to eIDAS) that may support financial institutions in their assessment of the remote on-boarding solutions. As journeys constitute identification ways of several generations, certain of them are better explained by these other regulations. The assessment criteria are also broadly aligned to the key phases of customer on boarding process<sup>11</sup> (application, verification, collection and management).

### B. A mapping of the different types of customer on-boarding journeys

In this second task, an inventory was created of current customer on-boarding journeys, based on input from EG members and open source desktop research. The resulting inventory was analysed and mapped into seven main types of typical customer on-boarding journeys, and their key features. Additionally, the different types of customer on-boarding journeys are discussed and mapped to the on-boarding phases and existing solutions (where known).

### C. A list of existing remote on-boarding solutions used within the banking sector

In this final task, an inventory list of existing remote on-boarding solutions was compiled by reaching out to the Expert group members, canvassing for their input and feedback based on what their organisation is currently using. The list is further augmented by open source desktop research on the available remote on-boarding solutions in the market and vendor presentations to the Expert group.

All findings which resulted from the study are covered in this report. The resulting findings are validated and presented to the European Commission's eID KYC EG. The sharing of findings are conducted via email, audio meetings and face to face meeting at the European Commission's premises in Brussels.

## Structure

This report analyses the results of the aforementioned tasks in sequential order and is structured as follows:

Chapter 2 introduces the key elements of the eID/KYC criteria, by eIDAS assessment criteria to support financial institutions in their assessment of any remote on-boarding solutions. Then against the key elements, consideration is given towards the European Banking Authority (EBA) opinions, UK Joint Money Laundering Steering Group (JMLSG) guidelines and other relevant European national AML Regulations.

Chapter 3 provides an overview of the different types of on-boarding journeys that a customer may take along with an analysis of the eIDAS and AML regulation (s) relevant to the customer on-boarding journey.

---

<sup>9</sup> **JC 2017 81** OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)

<sup>10</sup> Open source access to JMLSG: <http://www.jmlsg.org.uk/>

<sup>11</sup> Source: 2018 European Commission Report: "Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU." PriceWaterhouseCoopers EU Services EEG undertook the writing of the report at the request of European Commission.



Chapter 4 presents the various types of remote identity verification solutions that are commonly used in EU across the financial sector and the extent of their use by consumers. It will also discuss the impediments/barriers to a portable digital identity across sectors and borders.

Chapter 5 focuses on the risks identified with the use of the identification verification solutions and the associated mitigating controls.

Chapter 6 concludes this report, summarising the key findings and areas of future work.

Annex 1 presents an in depth analysis of the different on boarding journeys (Assessment under eID/KYC criteria, risks related to each solution, and associated controls).

Annex 2 presents European geographic maps for video identification solutions, and electronic identification means.

Annex 3 is an extension of Chapter 2 and provides an in-depth assessment of the eID/KYC assessment criteria, with considerations made against UK Joint Money Laundering Steering Group (JMLSG) guidelines, European Banking Authority (EBA) opinions and other relevant European national AML Regulations.

Annex 4 details the existing EU Member states' AML regulations on remote on-boarding journeys.

Annex 5 presents an end to end breakdown of remote on-boarding journeys in Spain, including attributes collected.

## Chapter 2: eID/KYC\_Assessment criteria

### Context

This chapter seeks to provide a high level overview of the eID/KYC\_assessment criteria to support consideration of any remote on-boarding solutions. The eID/KYC\_assessment criteria will be considered alongside eIDAS, the European Banking Authority (EBA<sup>12</sup>) opinions, National EU AML Regulations and the UK Joint Money Laundering Steering Group (JMLSG<sup>13</sup>) guidelines, whose provisions, to the extent they answer identification question, can be compared to eIDAS. For a more detailed discussion of the eID/KYC\_assessment criteria, please refer to Annex 3, and for eID/KYC reasons and comparison between AML and iDAS see Annex 1.

The key elements of the eID/KYC\_assessment criteria are as follows:-

- i. Documentation**
  - a. Type and content of Documents
  - b. Video & Photo Capture
  - c. Verification – Authenticity and Validity of Documents
- ii. Identity of the individual**
- iii. Additional Considerations**
  - a. Communications
  - b. Liability
  - c. Governance
  - d. Certification

### IA. Type and Content of Documents

When obtaining identify information, consideration must be given to the type and nature of documents or sources used, and the information contained within. eIDAS regulation also accepts identity documents for identification schemes other than those under an electronic form. EBA states that it is important that firms have regard to the validity and authenticity of data, documentation and information obtained in respect of their customers. The European Supervisory Authorities (ESAs) believe that firms should consider, *inter alia*, whether there are controls in place to ensure that identity documents have not been altered, counterfeited or recycled and therefore firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include limiting the type of acceptable identity documents (e.g. documents with high security/biometric features, qualified electronic signature)

In relation to electronic identification means, the 5<sup>th</sup> AML Directive supports the use of electronic identification means or any other secure, remote or electronic identification process that is regulated, recognized, approved or accepted by the relevant national authorities. In addition, a qualified certificate or strong electronic identification device can be accepted on its own in certain countries (e.g. Finland) but not others. For example, in France, the use of such qualified certificates will need to be supplemented by an additional means<sup>14</sup>.

---

<sup>12</sup> **JC 2017 81** OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)

<sup>13</sup> The UK JMLSG is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance. Open source access to JMLSG: <http://www.jmlsg.org.uk/>.

<sup>14</sup> R521-20 of the Monetary and Financial Code

Other forms of electronic verification of documents may take place through the reading of identification details provided by a (prospective) customer on the basis of data read from either an electronic chip embedded in an identification document or from other electronic devices like mobile applications or computer software, subject to the certain conditions being met (e.g. legally recognised document, record retention). Such electronic verification of documents may also take place through privately run systems like **Bank ID**<sup>15</sup>. In Sweden and Norway, for example, the use of Bank ID is widely adopted by customers. Moreover in Germany, applicants can apply for a Deutsche bank account using a Verimi electronic identity issued by an external provider, pursuant to certain conditions<sup>16</sup>.

#### IB. Video and Photo Capture

Under eID/KYC criteria<sup>17</sup>, when capturing photos or videos as part of the identification process, a number of considerations should be given, including that of image quality requirements (e.g. ISO 19794-5, light quality, number of pixels, distance of subject from camera), the potential need for real time video analysis, and how the image is stored/archived. **This is particularly important if the communications channel is via a non-integrated third party (e.g. Skype)**. Furthermore, when using remote onboarding solutions, ways to make use of identity evidences containing a photo (or other physical characteristic) and where possible to make use of biometric algorithms to compare the applicant with the claimed identity should also be considered. Other considerations from the EBA and European regulations are expanded on below.

The ESAs states that firms should consider, *inter alia*, whether there is a risk that a) customer's image visible on the screen is being tampered with during transmission b) an ID document displayed on the screen by a customer during the transmission belongs to another but similar-looking person. These risks must be prevented or mitigated with sufficiently robust controls. Examples of controls may include video conference with trained agent, liveness detection tests, built in security features within the app to detect discrepancies.

In relation to **video conference** (with a human employee in real time) and **video identification** (the human employee does not interact with the applicant), it is worthwhile to note the varying levels of regulations/technical guidelines issued by the Member states. As an example, in Germany, there are precise and technical requirements on how to conduct a video conference while in the UK, the Joint Money Laundering Steering Group is silent on the use of such technology. Germany mandates that the final decision of whether the person matches the ID card presented has to be taken by a natural person (whether in a face to face interaction or via video conference). Within Luxembourg, the CSSF (Commission de surveillance du secteur financier) mandated that the use of video identification as a sole measure is insufficient and will need to be supplemented with additional safeguard measures to mitigate the risks linked to the automated character of this type of identification.

#### IC. Verification of the Validity and Authenticity of Documents

**Validity:** A verification status of the document (whether lost, stolen or expired) is made against an authoritative source (private or public).

ESAs believe that firms should consider whether there are controls in place to ensure that identity documents produced during the (video) transmission have not been altered (i.e. changes made to data

---

<sup>15</sup> <https://www.bankid.com/en/>

<sup>16</sup> Conditions to be met are: (b) Video conference with a trained agent is conducted (b) the underlying ID is still valid (c) eID has been set up with Verimi in the last 24 months (d) the underlying documents (i.e. video files) are distributed as well, and (e) communication is handled via secure channels including a 2FA authentication from the customer.

<sup>17</sup> See: **Commission implementing regulation (EU) 2015/1502 of 8 September 2015 requirement for level Substantial** "steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence", and eIDAS Cooperation network guidances precisising this provision by Comparison of physical characteristics of the applicant against the evidence. Technical details are issued from the used assessment grid. See page 7 eID/KYC assessment criteria.

in a genuine document), counterfeited (i.e. reproduction of an identity document) or recycled (i.e. creation of a fraudulent identity document using materials from legitimate documents)?

**Authenticity:** In order to verify, authenticate and validate documents used in remote on-boarding, there are a number of key considerations and approaches to be followed under eID/KYC. A comparison to existing public sources and databases providing detailed information about identity documents, e.g. the Public Register of Authentic travel and identity Documents Online (PRADO). This would be beneficial in identifying counterfeit documents. Other checks could include ensuring that all features are correct, including syntax, a consistency check (e.g. check-digit<sup>18</sup> validation), whether or not the photo is genuine etc.

The ESAs believe that firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include one or more of the following:

- **Built-in features** which enable them to detect fraudulent documents on the basis of the documents' security features (i.e. watermarks, biographical data, photographs, lamination, UV-sensitive ink lines) and the location of various elements in the document (i.e. optical character recognition);
- Features that compare the security features ingrained in the identity document presented during the transmission **with a template** of the same document held in the firms' internal identity document database; or
- Where the **verification is not based on a government-issued identity document**, to the extent permitted by national law and commensurate with the ML/TF risk, features that allow firms to verify the information received from their customers against a combination of multiple reliable and independent sources (including, but not limited to, government registers and databases), which can be supplemented with data mining and social network analysis, IP address analysis, and location or device analysis.

JMLSG echoes similar principles to ESA and requires that customer due diligence must be carried out on the basis of **documents or information obtained from a reliable source which is independent of the customer**. It is therefore important that the evidence used to verify identity meet this test, both at on-boarding stage and subsequently when due diligence is revised/updated

## II. Identity of the Individual

For remote registration of identities under eID/KYC, identity proofing should be based on the review of more than one piece of identity documentation. In certain instances, the person whose identity is claimed should be informed of the ongoing registration by an alternative channel, **not specified or provided by the applicant**, in order to counter identity spoofing.

In addition, identity proofing can be conducted using information from third parties in accordance with regulatory provisions (e.g. qualified electronic signature), accessing registers/commercial electronic databases. It is recognized that financial institutions may utilize commercial organizations that access many data sources, and provide firms with a composite and comprehensive level of electronic verification through a single interface. Such organizations use databases of both positive<sup>19</sup> and negative<sup>20</sup> information, and many also access high-risk alerts that utilize specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a PEPs or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

---

<sup>18</sup> This is often the last part of a numeric field which is derived from the first part (e.g. modulo '97)

<sup>19</sup> **Positive information** (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others.

<sup>20</sup> **Negative information** includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

Where possible, and when applicable, knowledge based verification processes could also be used to strengthen the validity of the claimed identity.

Importantly, for an electronic/digital check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register), or at a single point in time, is not normally enough on its own to verify identity.

In order to enhance the anti-impersonation controls further, additional verification could be sought that the provided elements (documents, biometric data) have not been previously associated to another identity (as far as is reasonably possible, but at a minimum in the providers system).

## EBA

### *Delivery Channel Risk*

Directive (EU) 2015/849 considers that non-face-to-face business relationships or transactions without sufficient safeguards are **potentially** higher risk than face-to-face business relationships. Therefore, there is an expectation that firms carry out an assessment of ML/TF risks associated with non-face-to-face business relationships and the extent to which the use of innovative solutions can address, or might further exacerbate, those risks.

Consideration should be given to the **risk that potential customers who are on-boarded via the innovative CDD solution are not who they claim to be** as they are impersonating another person or using another person's personal data or identity documents (i.e. identity fraud). Safeguards that could mitigate these risks may include the verification of a customer's identity on the basis of a notified e-ID scheme, as defined in Regulation (EU) No 910/2014, where the scheme's assurance level is classified as high, or a combination of other checks that ensure the information obtained during the transmission can be linked to a particular customer. Examples of checks may include verification of customer's identity based on multiple factors and data sources, qualified electronic signature, sending a mail to the customer's residential address.

### III. Additional Considerations

**Communications** must be secured e.g. through Transport Layer Security (TLS) or cryptographic protocols to guarantee authentication and integrity of transactions, as well as confidentiality. For example, for use of video in Hungary, the AML Act authorises the supervisory authority for financial institutions to determine detailed rules for the minimum requirements of the secure, protected electronic communications equipment and the method of auditing the equipment.

Furthermore, any use of **authoritative and third party sources**/databases to confirm an identity and/or an individual document should also be adequately protected in terms of confidentiality, integrity and availability. **Liability** models also need to be considered when using, and when assessing, a provider. Indeed, the amount of liability may reflect the confidence in the reliability of the system.

It is advised that a provider should have an effective **counter-fraud** policy and monitor false match rates for its product, considering a number of factors including age, gender and nationality. The provider should record and monitor all errors during a remote on-boarding process for the involved identity and deploy additional verifications when the case appears to be suspect (e.g. cumulative scoring mechanisms). Additionally, and where possible, localisation and MNO's (Mobile Network Operators) data should be taken into account. From an internal point of view a provider should implement segregation of duties so that one employee cannot be able to complete an identity registration process alone.

There are also **geographical risks** to consider, as noted in the EBA guidelines. Specifically, it notes that: the key feature of most commonly used innovative CDD solutions is that they enable firms to on-board customers remotely and verify their identity via the internet, regardless of customers' location or distance from the firm. This means that customers are no longer required to live in close proximity to firms to use their services, and do not have to be physically present for the identification purposes. Therefore it's important that firms have the ability to assess geographical risks presented by a business

relationship, including through controls firms may have in place that capture their customers' location (e.g. through device fingerprinting or GPS data on mobile phones) to establish if they are based in a jurisdiction associated with higher ML/TF risks.

This also opens up an idea worth further exploration related to **specific device usage**. **Should all devices be accepted?** Are there specific types, or individual devices, that should be blacklisted? Conversely, should there be a so-called whitelist or certified product list? Would "rooted" devices be allowed? Etc.

Naturally, as per any process, adequate **governance** is required and there should be the ability to conduct relevant and suitable (and timely) audits, both internally and externally. JMLSG guidelines state that a commercial organization should have processes that allow the enquirer to capture and store the information they used to verify an identity.

**Certification** - the Level of Assurance of remote identity registration solution should be assessed by a conformity assessment body (or equivalent) and solutions should be certified (e.g. ISO27001, or other certification to be considered). JMLSG states that before using a commercial organisation for electronic verification of identity, firms should be satisfied that information supplied by the data provider is considered to be **sufficiently extensive, reliable and accurate, and independent** of the customer. This judgement call may be assisted by considering whether the identity provided is recognised through an accredited body, uses a range of multiple positive and negative information sources for identity proofing, published standards which the identity provider has to comply with etc.



## Chapter 3: Typical on-boarding journeys

### Approach

This chapter introduces and sets out the different types of customer remote on-boarding journeys commonly adopted in the European market. For the purpose of research, the project team has collated and studied close to 50 types of customer on-boarding journeys across 10 European countries who support remote on-boarding processes. It is noted that for certain European countries, they do not rely on electronic identification means and hence will be out of scope of the study.

The project team selected customer on-boarding journeys used by a number of financial institutions to illustrate how new technologies are used by financial institution to remotely/digitally on-board new customers. The descriptions are based on the project team's own collection of information and experience of the on-boarding processes. The project team has not, due to a strict timeline to finalise this report, consulted the relevant financial institutions to confirm the accuracy of these on-boarding journey. This report has been anonymised to ensure that the description of on-boarding journeys does not undermine the protection of the commercial interests of the financial institutions mentioned in the report.

The 50 customer journeys were analysed, focusing on how the applicant is identified, i.e. to prove that person is who they say they are. Identification means can be broadly summarised as face to face identification, use of video identification (video conference or selfie), or using electronic identification means. These means are not mutually exclusive and can be combined or supplemented with other KYC/identification means depending on the risk appetite of the financial institution and the governing regulations in play.

Based on the analysis of the different approaches to identification means, the group has mapped the 50 customer journeys into 7 main typical categories. They are as follows:

Journey 1: Cross Channel journey (Remote and Face to Face identification)

Journey 2: Remote on-boarding based on enhanced KYC measures (with or without electronic signature)

Journey 3: Entirely remote on-boarding using video conference and biometric identification (optional)

Journey 4: Entirely remote on-boarding supported by selfie and biometric identification

Journey 5: Entirely remote on-boarding resulting in trust services created

Journey 6: Entirely remote on-boarding using digital identity

Journey 7: Remote on-boarding employed by e-merchants using electronic wallet

### Introduction

The customer on-boarding journeys will provide the context and “set the scene” to allow readers to better understand how the various identity verification solutions are used by financial institutions to support their remote on-boarding process.

This chapter will provide an overview of the customer on-boarding journeys, focusing on key themes and findings. The journeys will also be considered against relevant AML regulations. For a detailed description and analysis of the customer on-boarding journeys, please refer to Annex 1.

To understand a customer on-boarding journey from start to finish, it is important to make the distinction between Identity related data, Know Your Customer (KYC) related data and other on-boarding related data that are collated along the process. These are all data collected from the customer throughout the on-boarding process. They can be broadly distinguished into three categories (refer below table)

Financial Institution Customer On-boarding process (Natural person only)		
Core Identity	KYC	Other processes included as part of on-boarding
Core Identity attributes required to prove an individual's identity. Information requested may include date of birth, name and address.	The scope of KYC includes the core identity attributes required to prove a person's identity. It also includes other information which is collected either for anti-money laundering ("AML") purposes, other Financial crime purposes (for example fraud), or suitability purposes. Examples will include information required on Source of funds and Purpose of account.	This includes data attributes which are not AML or Financial Crime related but are gathered as part of an individual's on-boarding process. This includes information on a customer's communications preferences or information collected for product targeting.

Adapted from Jan 2017 Open Identity Exchange report: "How digital identities which meet government standards could be used as part of UK Bank's Customer On-boarding and KYC Requirements"

For the purpose of this study, this report will focus on the identity proofing aspect (i.e. core identity attributes) of a customer on-boarding journey. KYC and other additional processes that financial institutions may request to satisfy their on-boarding processes are out of scope of this report.

To note, there are other aspects of the eID/KYC\_assessment criteria (i.e. Communications, Authoritative & Third Party sources, Governance, Liability, Mobile devices, Certification) that are discussed in Chapter 2 and are key in considering the merits of any customer on-boarding solutions. However, due to limited public information available, and report anonymisation, the report will refrain from making any analysis of the journeys against these criteria, and will consider that requirements under these criteria are reached. Therefore, it is important to stress that the statements on each achievable eIDAS LoA is only an estimation of the maximum level achievable under several assumptions. Consequently, this document does not provide a definitive statement of an eIDAS LoA level for such precise all onboarding practice, whose assessment should be effectively done.

In addition, at the time of writing this report, there is no empirical study available on the use and customer acceptance of the different solutions used at the journeys either at national or European level.

## Overview of the customer on-boarding journeys

As an overview, it is safe to say that for all of the journeys, they are comprised of a few key identification processes integral to any on-boarding journeys. These are the collation of the applicant's core identity attributes, verification of the document (s) and their validity and in most cases but not all, accompanied by face to face/remote identification methods. However, the exact process/journey and the identity verification solutions employed will vary depending on the financial institution, maturity of the markets and the countries in which they operate in.

From a genesis point of view, the on-boarding journeys have been used by applicants across a period of time and are now co-existing. Journeys 1 and 2 date back to 2004 while Journey 3 (use of video interview) was launched nearly a decade later (2015). This evolution is made possible with the appearance of service providers proposing smartphone identification applications together with video interview. This has since expanded to include automatic video identification solutions like the ones presented in Journey 4, enabled by better liveness detection and fraud controls. This Journey can be considered quicker and easier from a customer viewpoint as opposed to Journey 3 where it involves a live video chat with a trained agent.

***Journey 1 depicts an on-boarding process which typically commences with an applicant applying remotely and subsequently having to go into a branch or a specified location of choice for a face to face identification.***

***Journey 2 presents a more commonly used remote on-boarding journey where the applicant applies online and upload the requisite identity documents. Identification is completed by an enhanced KYC measure, as a payment issued to or from another account the applicant holds in another UE bank. This journey can in addition propose an electronic signature.*** In general, the identification documents and means requested by the financial institution will correspond to their respective KYC needs<sup>21</sup>. The identity documents will be checked by the financial institution or an independent third party solution provider towards an authorized source (e.g. national registry database, credit reference agencies). Once the checks are confirmed, the applicant will be sent a Transaction Authentication Number (TAN) to trigger the electronic signing of the terms and conditions and be supplied with an electronic certificate at the end of the process.

***For Journey 3, one of the identification means adopted is the use of video identification conducted by trained agents. In some instances, the video identification is further supplemented by biometric identification checks.*** The biometric checks are performed by comparing the scanned ID document to the dynamic selfie taken by the applicant with his mobile/computer device. One of the technologies used is the face liveness detection test, e.g. reading of electronic chip within the ID document there by capturing the identity details and electronic facial image of the individual and compared against the selfie taken by the individual. In certain jurisdictions, there are specific regulations governing the use of video identification. For example, the German Federal Financial Supervisory Authority (BAFIN) – Circular 3/2017<sup>22</sup>, is prescriptive of what needs to occur during a video identification process, e.g. mandatory end to end encryption of the communication channel; verification of the security features of the identity documents supplied. The same applies for the Austrian Online Identification Regulation (Federal Law Gazette II No. 5/2017)<sup>23</sup>. It is worthwhile to note that within Europe, despite a general consensus and a recognition of a need to harmonize regulations in the governance of identity verification methods, at present, there are still varying approaches adopted by Member states.

***Journey 4 utilizes automatized identification (selfie) as biometric tool for identification. The applicant will upload the ID document (s) using photos taken with his mobile device.*** The photo ID will be compared to the selfie taken by the applicant, applying biometrics. This journey study (see Annex 1) also permits reference to Journey 3B, when extending journey 4 to journeys involving “a dynamic selfie” i.e. a video, and as such allowing liveness detection, on the contrary to journeys only using a static selfie). It is important to make a distinction between the video identification (“dynamic selfie”) in Journey 4 extension vs. the video identification (video conference) used in Journey 3. In the case of the former, there is no interaction with a natural person and customer interaction is purely with the machine or where the customer simply uploads (a video) identity documents online. The latter form of identification is performed by a trained person and involves real time interaction. In certain EU states, e.g. BAFIN and Luxembourg CSSF (Commission de Surveillance du Secteur financier), this mode of interaction does not constitute video identification and is not sufficiently robust as an identification means. Such identification means if employed will need to be supplemented by additional identification measures to mitigate the risks associated with the automated nature of the selfie method.

***In Journey 5, the applicant applies for the bank account remotely and upon successful application, will simultaneously be issued a trust service recognized by the member state.***<sup>24</sup> The remote on-boarding application process is similar to that undertaken in Journey 3B (i.e.

---

<sup>21</sup> There are various combinations of identification means that the FI may stipulate. They may include a) submission of 2 identity documents and a wire transfer from another bank in the EU b) 1 identity document, a wire transfer from another bank in the EU & a statement of another bank in the EU

<sup>22</sup> BAFIN Circular 3/2017 :

[https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs\\_1703\\_gw\\_videoident.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html)

<sup>23</sup> <https://www.fma.gv.at/en/national/fma-regulations/#58>.

<sup>24</sup> As provided by eIDAS regulation, this journey deals with qualified certificates.

use of video identification and biometric measures). The delivered trust service certificate will then be used in a second phase for on line bank documents signing. Journey 5B deals with direct use of signature certificates provided to the applicant for remote on boarding, embedded as an SDK into the bank application, or used as a standalone application separate from the banking application. One of the certificates is qualified and bears a large number of attributes certifying in this way the applicant identity and attributes.

***Journey 6 focuses on the use of digital identity as the main mode of remote identification.*** The applicant applies for a bank account using his eID document. In the case of Estonia, a country at the forefront of embracing digital identity technology and whose eID scheme's level of assurance is rated High, citizens or residents of Estonia<sup>25</sup> may apply for their bank account using their eID document. The on-boarding process generally begins with the automatic extraction of identity details from the mobile ID or ID card using an ID card reader. The identity information is verified and validated against central database/revocation lists. Once the checks have been performed, the customer can activate the bank account by electronically signing the agreement with his ID card (using a card reader) or mobile ID credentials. This allows the applicant access to bank facilities subject to monthly withdrawal limitations (EUR 15000) – as per Estonian's AML regulation. Face to face or video identification with a third party trained agent and the provision of another identity document will be necessary to lift the monthly withdrawal limits.

As a comparison to Estonia, Belgium's AML regulations are less prescriptive on remote on-boarding channels and instead follow a risk based approach. Annex III of the Belgium AML Regulation indicates that the use of remote on-boarding channel should serve as an indicator of a higher risk customer and that particular attention should be given to the verification of the identity of the customer (e.g. to access the Belgium national registry to carry out additional identity verifications). To further illustrate the varying approaches and level of prescriptive-ness adopted by different EU regulations, France's AML regulation stipulates that for eID schemes with LoA at Substantial, additional identification means will need to be performed. This may, among other measures, be in the form of additional identity document requested or a bank transfer from another account opened to the customer in the EU.

***Journey 7 depicts the typical processes that are used to identify and verify an applicant's identity when opening an e-money/e-wallet account.*** The onboarding flow starts with the applicant completing an online application form which captures all relevant identity information of the person. Verification of the document/data is done predominantly via Credit Reference Agencies (CRA). These sort of identity verification solutions are relevant in countries with mature Credit Referencing capabilities, and within the EU they are particularly strong in UK, and Italy. Full Identity data is available in other EU countries, but in general there is less coverage of all the relevant data fields that need to be verified. In other countries there is a reasonable abundance of data on people's names and addresses, but less data on customer's date of birth.

People with "thin" credit files will generally fail this type of CRA data verification and will be asked to provide identity documents. To this, supplementary measures like Knowledge Based Verification can be adopted. Other data points can help verify the customer in session is the owner of the identity, for example cross-referencing the ownership of the financial instrument attached to the e-wallet, location data linking the session to the address of the real owner of the identity, telephone subscriber checks coupled with proof of possession of the device, checking ownership and access to the customer's email address, and other such processes.

For individuals whose identity could not be verified via data sources or in countries where it is not possible or appropriate to use identity data for verification of customer's identity, the individual will be asked to upload images of documents from a predefined list of types of acceptable proofs of identity

---

<sup>25</sup> Estonian's AML regulation also permits such an on-boarding process from a) E-resident of Estonia b) another state within the European Economic Area (EEA) c) a notified eIDAS member scheme with LoA High or d) where a person is a non EU resident, the identity document is issued by the competent authority of the foreign country. The requirement is for the verifications to be made on the ID document against a credible and independent source.

and address. Technology used, to list a few, can be biometric checks (e.g. face liveness detection) or video identification.

As a final step to confirm the applicant's ownership and control of the funding instrument associated with the e-wallet, the Payment Service Providers (PSPs) typically use micro deposits to prove that the account owner has control over the source of funds. Some CRAs can check if the identity details matches to that of the bank account holder.

Looking forward, Open Banking as mandated by Payment Service Directives 2 (PSD2), to the extent customer has been duly identified at a relevant level by providing bank, will further support the verification of access and ownership of the funding instrument, provided that the account data made available by banks were to include aspects of the customer's identity necessary for AML purposes.

The adoption of any customer journey is heavily predicated on how user friendly and incentivized the customer is. For a customer where there is a strong imperative to obtain the financial service, they may be more motivated/incentivized to complete a more laborious/time consuming identity verification process. A good customer journey should balance the needs of the consumer (i.e. user friendly, secure) while meeting the regulatory and KYC needs of the financial institutions at the same time, and taking into consideration high security standards in financial services industry. From a customer's perspective, the adoption of new identification technologies, like 'selfie' for facial comparison, liveness checks, or video interview may depend on cultural or market maturity factors, but are mostly driven by the need for speed and ease of use. A fully automated and speedy process will almost always be preferred over a video chat. This customer preference will need to be tempered with strong technical measures to ensure the integrity and security of the identification process.

In summary, our analysis of the different types of customer on-boarding journeys reveals that they are heavily influenced by the country's legislation, customer's preference, availability of third party solutions, and technology maturity. These on boarding journeys also appear to be a coexistence of different journey generations. There is no one size fits all approach and it is worthwhile to note that compliance is rarely achieved in a single solution but that risk can be offset with other risk mitigation measures. In addition, identity verification technologies are constantly evolving and the limitations/risks one faced today may be overcome by improvements in technology in the future. Technologies can help to deliver identity services with solutions that should meet both objectives of ensuring secure identity and improving customer experience.

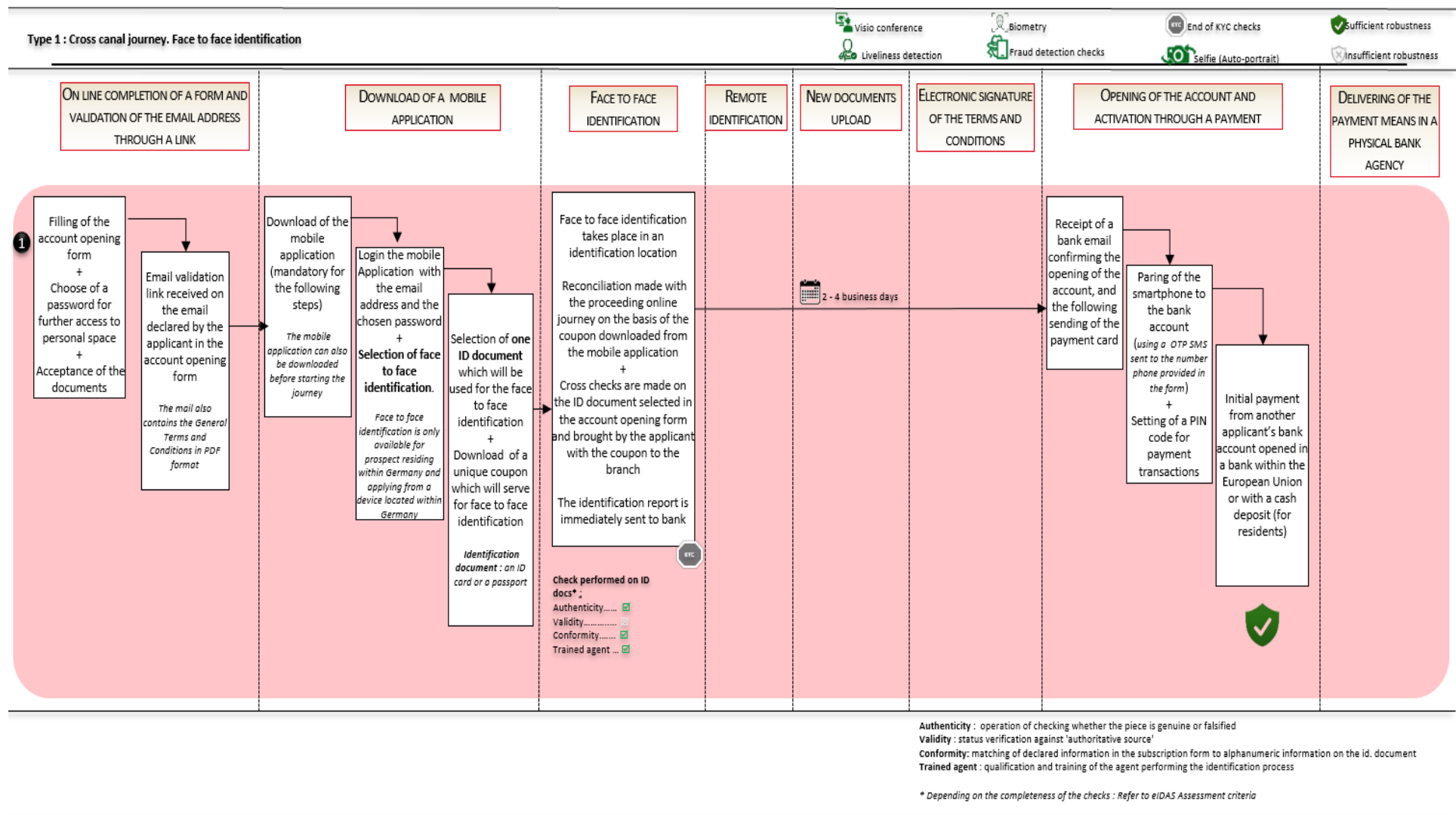
Table 1: Main Typical Onboarding Journeys (Definitions and Legend Keys)

**MAIN TYPICAL ON-BOARDING JOURNEYS  
DEFINITIONS AND LEGEND KEYS**

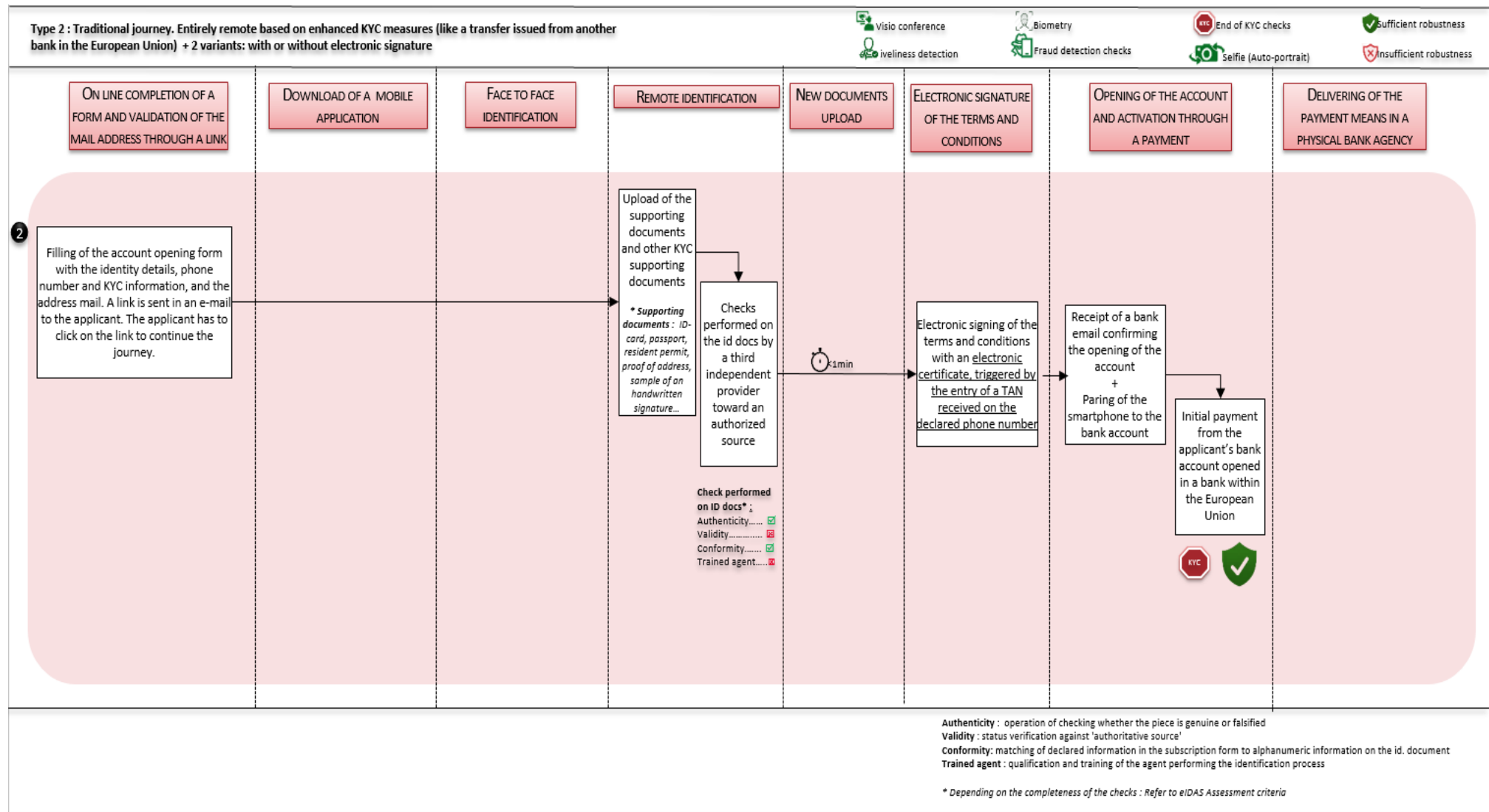
ICONS	SIGNIFICATION	DEFINITIONS	MAIN ONBOARDING JOURNEYS
	Visio conference between the applicant and an identification operator / bank counselor	<b>Authenticity</b> : operation which consists in checking whether the piece is genuine or falsified	• <b>Type 1</b> : Cross canal journey - Face to face identification
	Liveliness detection of the applicant	<b>Digital identification</b> : fast and convenient digital process for a private person to open a bank account in a way that he/she identifies herself/himself electronically in the Internet Bank	• <b>Type 2</b> : Traditional Entirely remote based on enhanced KYC measures ( <i>like a transfer issued from another bank in the European Union</i> ) + 2 variants: with or without electronic signature
	Biometry	<b>Conformity</b> : check which consists in matching of declared information in the subscription form to alphanumeric information on the ID-document	• <b>Type 3</b> : Totally remote journey using Video-chat and if including an additional biometry, and electronic signing
	Fraud detection checks	<b>KYC</b> : process	• <b>Type 4</b> : Totally remote journey with Identification using Biometry only
	Selfie done by the applicant using a built-in camera device	<b>Trained agent</b> : qualification and training of the agent performing the identification process	• <b>Type 5</b> : Totally remote journey resulting in a trust service delivery or with 5B two certificates (including one for KYC purpose)
	End of Know Your Customer measures	<b>Validity</b> : status verification of the ID document against 'authoritative source' (private or public) to check whether the Id doc is lost, stolen or expired.	• <b>Type 6</b> : Totally remote journey starting with or including a recognition of a digital identity ( 6 and 6bis
	Unused feature		• <b>Type 7</b> : On e-merchants websites using electronic money/wallet
	Sufficient robustness of the process regarding the checks performed		
	<u>Overquality</u> of robustness of the process regarding the checks performed		
	Insufficient robustness of the process regarding the checks performed		
	Use of digital identity		
	Use of payment card / bank card		



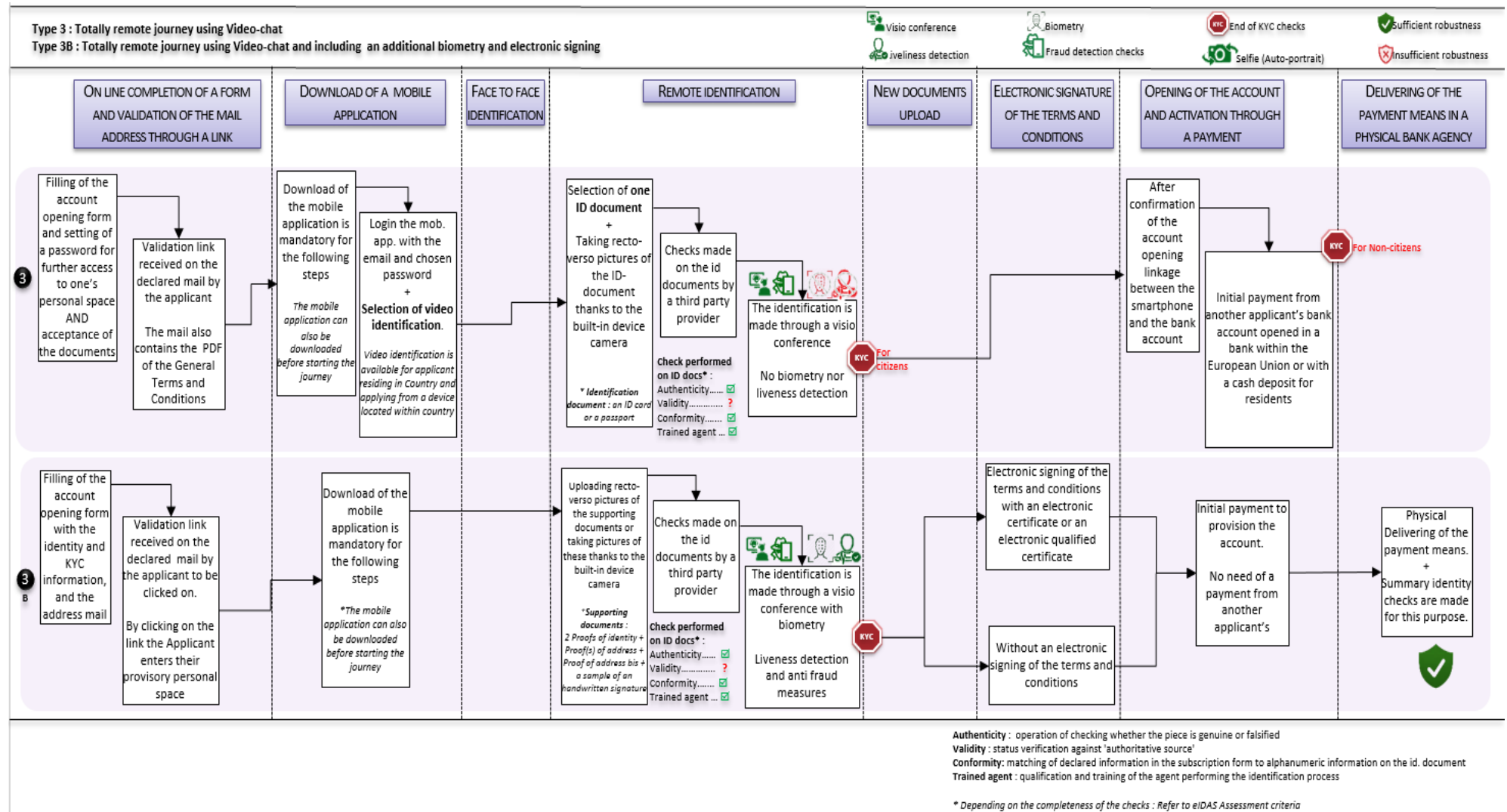
## Journey 1: Cross Channel journey (Remote and Face to Face identification)



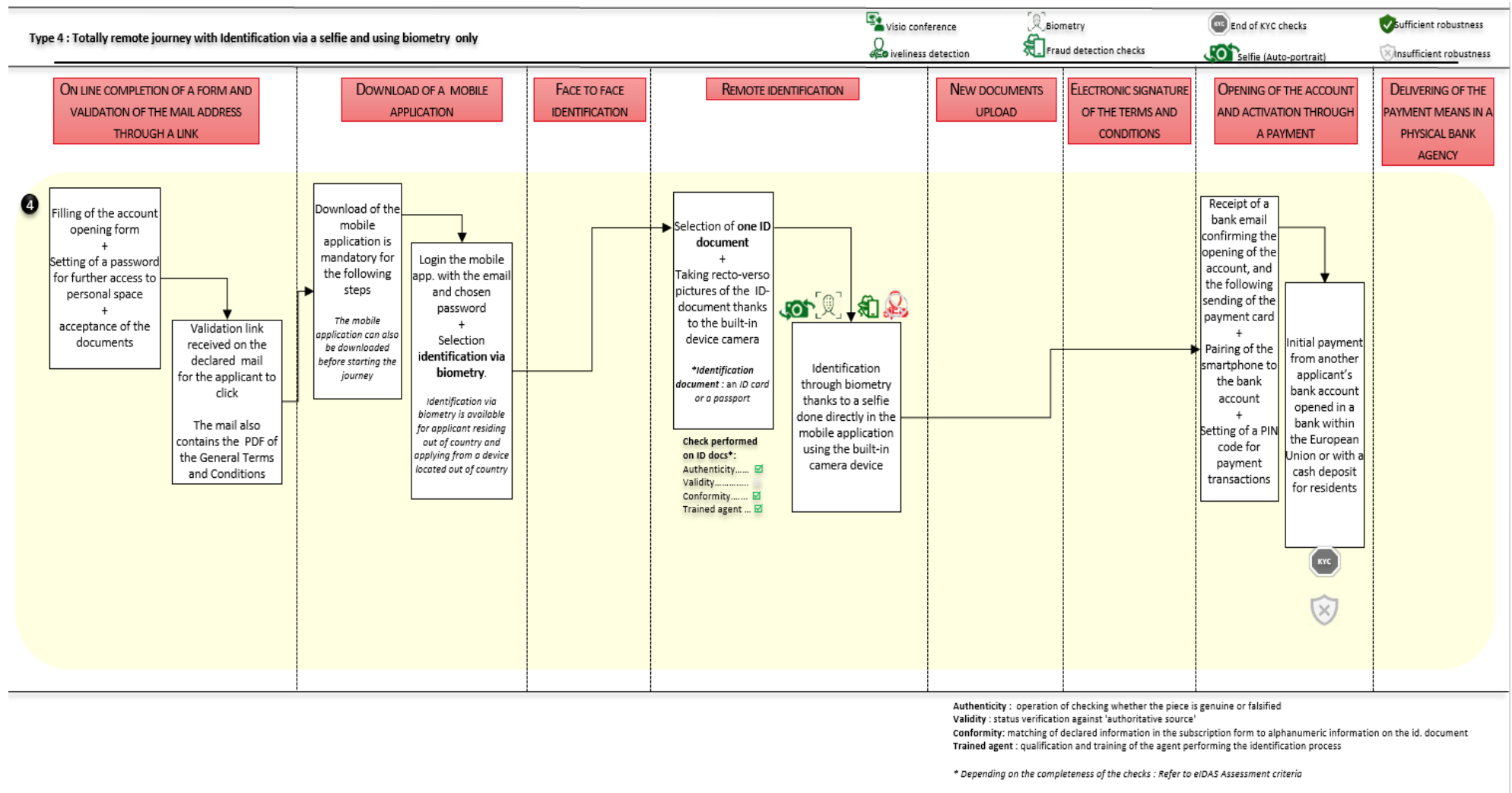
## Journey 2: Remote on-boarding based on enhanced KYC measures (with or without electronicsignature)



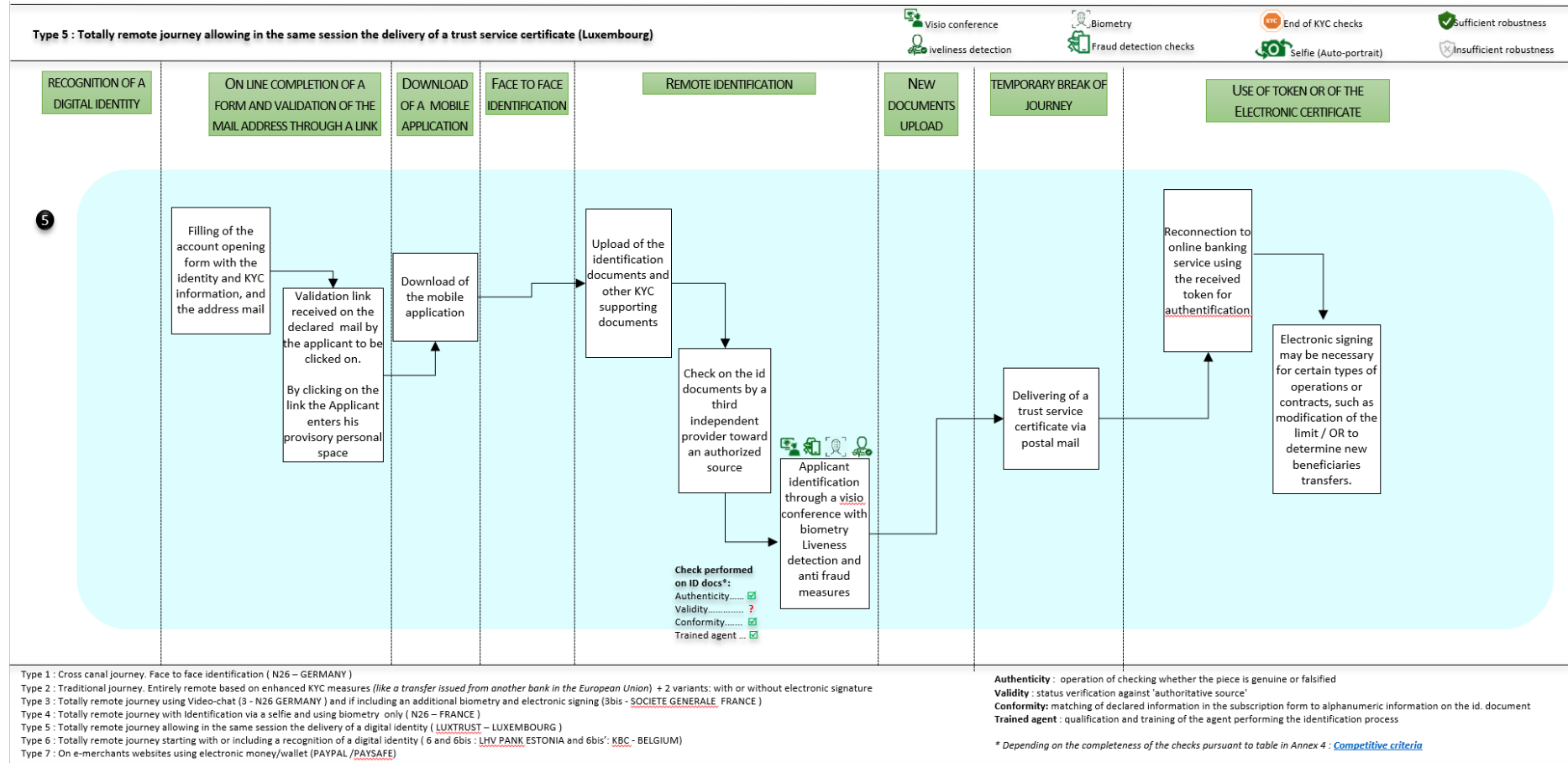
### Journey 3: Entirely remote on-boarding using video conference and biometric identification (optional)



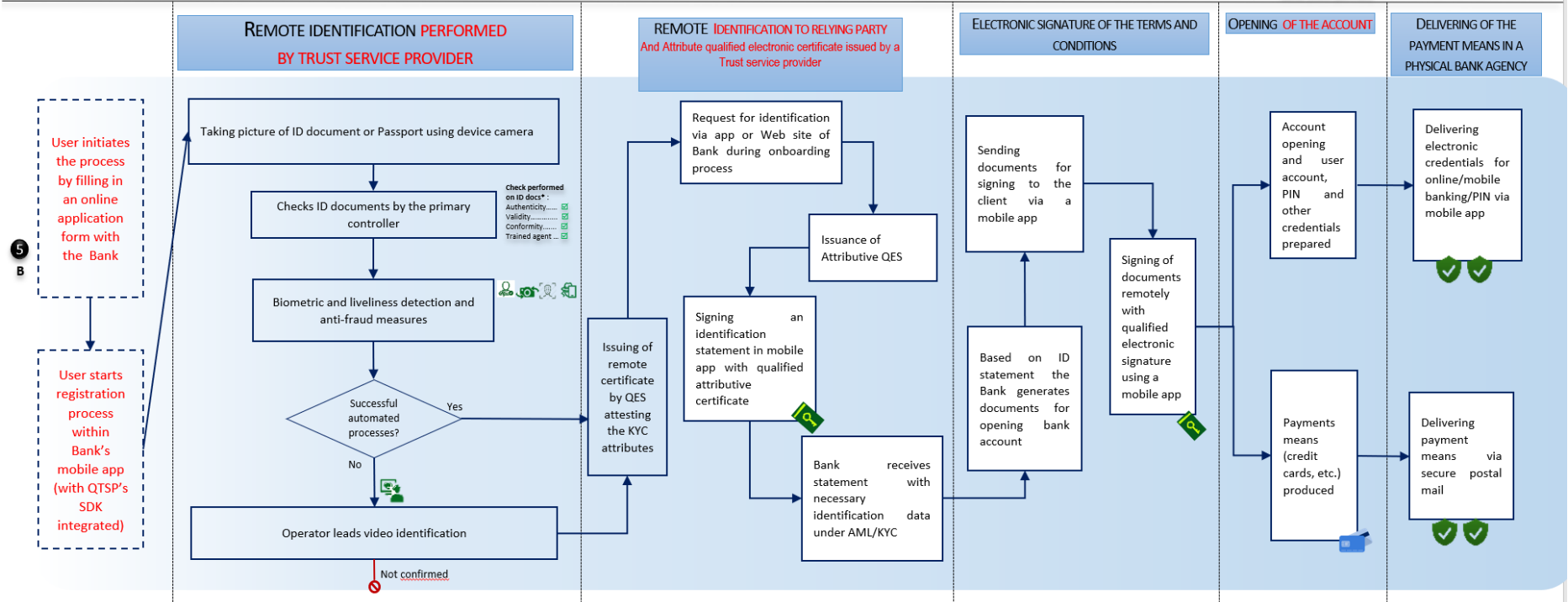
## Journey 4: Entirely remote on-boarding supported by selfie and biometric identification



## Journey 5: Entirely remote on-boarding resulting in a trust service delivery



**Type 5B : Entirely remote on-boarding using a trust service via smart device or on the smartphone for remote electronic signature (Bulgaria)**

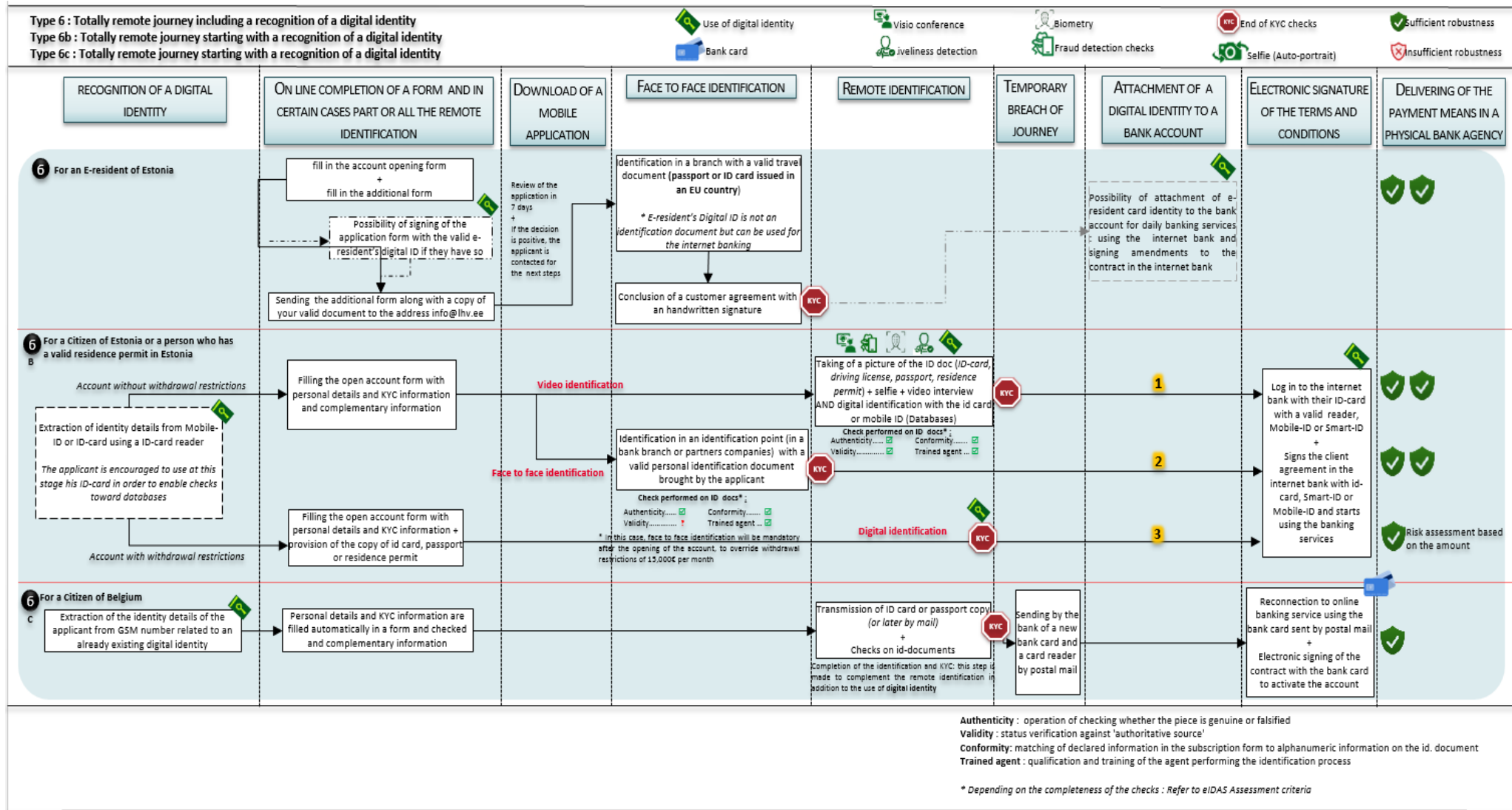


**Authenticity** : operation of checking whether the piece is genuine or falsified  
**Validity** : status verification against authoritative source  
**Conformity**: matching of declared information in the subscription form to alphanumeric information on the id. document  
**Trained agent** : qualification and training of the agent performing the identification process

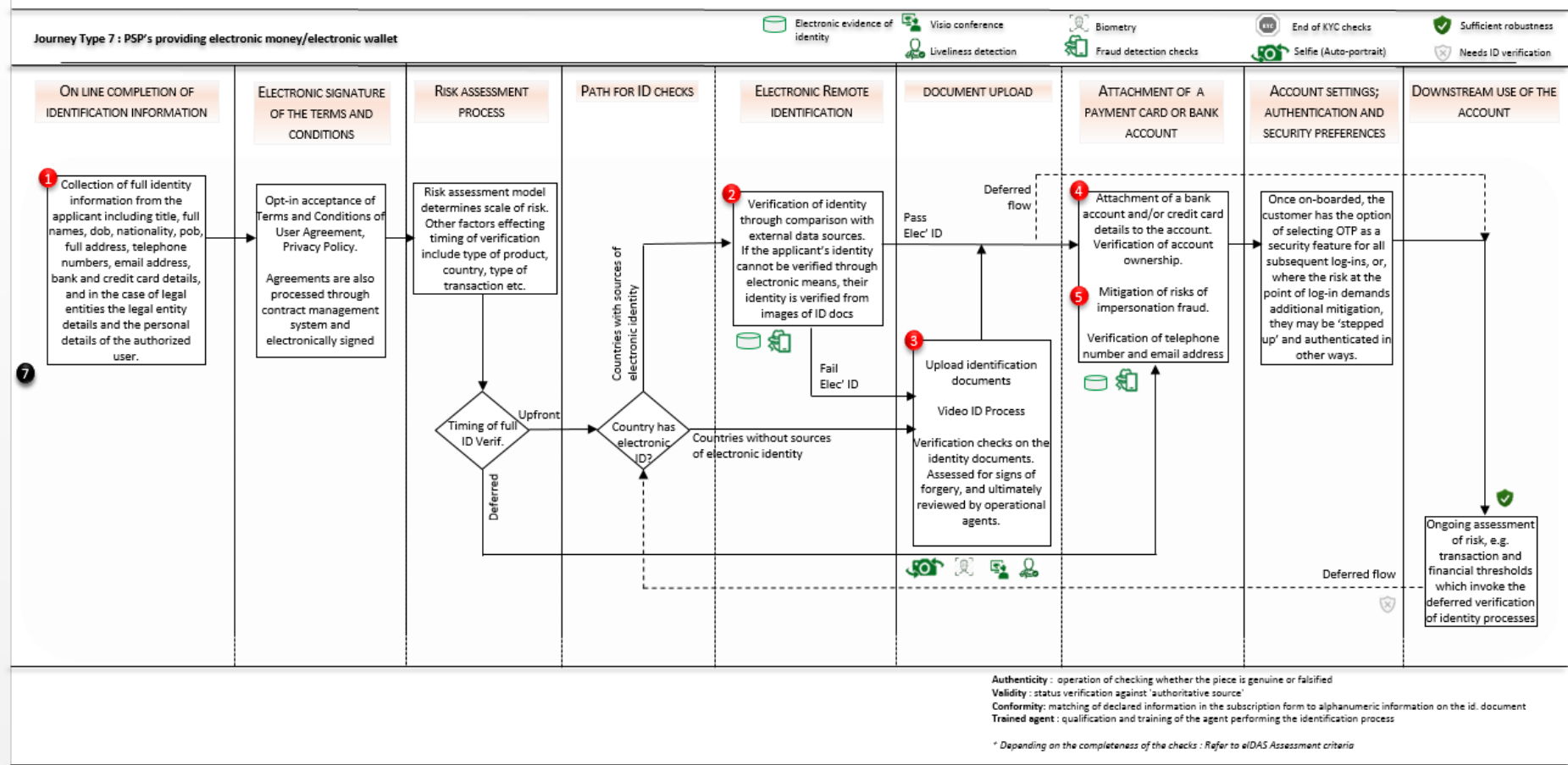
*\* Depending on the completeness of the checks pursuant to table in Annex 4 : Competitive criteria*



## Journey 6: Entirely remote on-boarding using digital identity



## Journey 7: Remote on-boarding journeys employed by e-merchants using electronic wallet



## Chapter 4: Overview of existing remote on-boarding solutions and the extent of their use by consumers

The purpose of this chapter is to provide an overview of the types of remote identity verification solutions that are widely used across the financial services markets in Europe. This reflects solutions that are used by the Companies that the members of this Expert Group work for, and solutions offered by commercial entities that presented their products and services to the EC Expert Group. Therefore, this is not an exhaustive study, but it should cover most of the current methods of identity verification. The risks associated with using the various identity verification solutions, as well as mitigations to those risks, are covered in a separate chapter.

In most cases it is not possible to provide a compliance assessment of the alignment between the various types of identity verification solutions and the AML/CCFT requirements. This is because it is for the responsible provider of the financial services to configure and use the identity verification solution in a manner which is relevant to their product, business model, country or countries of operation, and complementary AML/CFT processes.

Unless otherwise approved by the EC, a decision was taken not to reference commercial solutions by name, but instead to describe their proposition – which should be all that is necessary for delivering the first part of the Terms of Reference ‘ToR’ without introducing the complexity of participation from additional commercial entities.

Chapter 3 records the typical remote on-boarding journeys that are followed by customers opening accounts with providers of financial services. The purpose of these journeys is to provide context for how identity verification solutions are used in practice.

The Sub-Group recognizes the usefulness and relevance of a report prepared for the EC by PWC on digital onboarding<sup>26</sup>. The following sections of this ‘PWC report’ are foundational to the work within this Sub-Group;

- Chapter 2; pp 21-24, which sets out KYC/AML requirements for on-boarding
- Chapter 3; analysis of common and divergent compliance means used for the on-boarding process
- Annex IV; ‘Common and Divergent Compliance Means’ which provides tables mapping the required identity attributes to verification methods

The Sub-Group does not consider it necessary to repeat the analysis presented in the PWC report, but instead aims to complement it by providing expert opinion and perspectives on the main types of identity verification solutions which are in use today, and to a lesser extent on the new and novel identity verification solutions, which will be provided in the second deliverable within the Terms of Reference.

The phrase ‘identity verification solution’ means a technical solution which could be used on a stand-alone basis, or it could be complemented by other solutions and processes that enable the verification of the identity attributes of the customer, i.e. their name, date of birth, nationality etc.

### The evolution of commercial remote identity verification solutions

The identity of a customer must be verified through independent and reliable sources. This has traditionally been achieved by customers evidencing their identity by providing the financial service provider with the stipulated types of Government issued identity document(s). This is a practical and effective approach in face-to-face scenarios where the customer can present themselves physically to the provider of the financial services, or to a service provider that helps verify the identity of the prospective customer, such as a Post Office.

---

<sup>26</sup> <https://publications.europa.eu/en/publication-detail/-/publication/8da08249-49cd-11e8-be1d-01aa75ed71a1>

The emergence of the online channels, and the commercial attraction of using them, has forced the development of policy to legitimize processes for verifying the identity of customers who are physically remote from the provider of financial services, i.e. 'remote on-boarding'. This typically involves customers scanning and uploading digitized images of Government issued identity documents, as well as other documents that help corroborate identity - such as 'proof of address.'

In the case of legal entities applying to open accounts, this is a more complex process which typically involves the identification and verification of the legal entity, the identification and verification of individuals associated with operating the account, documentary proof that those operating the account have the authority to do so, the identification and verification the Directors of the legal entity, and the identification and verification of the ultimate beneficial owners of the legal entity. As there are many different types of legal entities, the subgroup have pragmatically limited their scope to the most common type, which is private companies. This shouldn't narrow the relevance of this report as many of the identity verification solutions that are used to identify private companies will be relevant to other types of legal entities.

Early responders to the opportunities brought by online channels were Credit Reference Agencies, who saw an opportunity to achieve identity verification using the identity elements within their extensive credit files and business information databases, and they developed online identity verification solutions to reduce friction in identity verification processes. These solutions were invariably coupled with the provision of fraud detection solutions that leveraged closed user group data, and in some cases is complemented with knowledge-based authentication products. More recently, the data used in these solutions has expanded to include a wide range of information that collect and analyses the riskiness of the customer's devices, their connection to the channel, their behavioural and physical interaction with the device.

As mobile telephony evolved with integrated cameras and faster network speeds, the opportunity for commercial innovation and improving the customer experience has led to the development of new identity verification solutions. These typically include simple ways of guiding the customer through the process of capturing an image of their identity document, capturing an image of their face, tests to make sure the customer is alive (i.e. not a static image of filmed images), comparing the facial images of the bearer of the document to the facial image on (or in) the identity document, and automated processes for reading and validating the identity documents.

In recent years, driven by the need to remove friction from digital ID validation processes, we have seen emerging solutions that work by collecting data (id attributes) in the background, therefore, not directly impacting the user's digital activities. These include mobile device identification, geo-localization or the provision and checking of digital tokens. Along the same lines, the most powerful development has been the digital IDs that, after an initial registration process, allow the consumer to re-authenticate themselves and register for additional digital services in a really convenient way while maintaining the highest levels of assurance as to their identity.

However, to really have a compelling consumer value proposition and achieve scale, these digital ID schemes must take a federated approach, or based on the collaboration of public and private institutions. This approach has driven the success and rapid adoption in the Nordics (different solutions in the several Nordics, where BankIDs - developed by a number of large banks for use by members of the public, authorities and private sectors) as well as digitally advanced countries such as Estonia (MobilID). Belgian ItsMe relies on a private consortium between Banks and mobile operators, Belgian Mobile ID (BMID).

Improvements in internet bandwidth have made video-based identification sessions technically viable, and when these processes are coupled with capture of a customer's evidence of identity, facial verification between the customer in session and the facial image on the document, liveness tests and systematic document validation and authentication checks, it's possible to viably replace traditional 'face-to-face' interactions. Advances in regulation have authorized the use of these sorts of solutions.

The relentless expansion of functionality within smartphones, notably capabilities in devices to use 'Near Field Communication', has enabled commercial identity verification providers to create

applications designed to read the data within the chip inside electronic identity documents. This has several advantages including removing the vagaries of using Optical Character Recognition to read parts of an identity document which are not designed to be read by machines, but nonetheless must be captured. Reading the identity attributes directly from the chip, including the digitized image<sup>27</sup> of the face of the owner of the document, removes the risk of forgery by means of photo substitution, and increases the accuracy of data capture. However, the ability to use NFC in mobile handsets is not yet comprehensive across all handset manufacturers.<sup>28</sup>

Although nearly all the solutions referenced in this section of the report are intended to be used in remote on-boarding, they could, where necessary, be coupled with physical 'face-to-face' engagement with the prospective customer.

Most Firms will use multiple types of identity verification solutions to match the solution to the customer's ability to identify themselves, and to correlate the strength of the identity verification solution to the type and scale of identity risks they encounter.

#### Categorization of remote identity verification solutions

The Sub-Group have been provided with information about various commercial identity product offerings. This has been augmented with desk research and hands-on experience with using various identity verification solutions.

This revealed that evidence of identity is principally divided between identity documents, identity data, and confirmation of electronic identity through electronic identity schemes. Whereas the underlying sources of evidence of identity are few, there are numerous methods through which the proof of identity is captured and checked.

These are explained in more detail in the reference base of materials collected by Sub-Group 1 and held within the EC online work area. In summary, these solutions can be sorted into the following categories:

1. **Unsupervised capture of identity document:** the customer scans or takes a photograph of their identity document and uploads it to the systems of the financial services provider. Checking the document can be manual, automated or both.
2. **Cross-channel capture of identity document:** the online on-boarding application is complemented with an offline physical identification process, where the customer produces documentary evidence of their identity to the provider of the financial services, or to an approved third-party such as a Post Office
3. **App' Capture of identity document:** the controlled capture of the identity document through an application developed 'in-house', or an application developed by a third-party, which is designed to guide the customer through the process of capturing an image of their identity document, and controlling the settings on the device to improve the image quality necessary to conduct relevant checks. These applications include the capture of the customer's face and a variety of approaches to make sure the facial image is of a live person 'liveness test'.
4. **App' and NFC capture of identity document:** the controlled capture of an electronic identity document coupled with reading information from the chip inside the document, plus facial capture and liveness tests.
5. **Video identification and capture:** a controlled online video identification session, currently involving human operational employees engaging with the customer, capturing evidence of identity, image of their face, and liveness test. There are currently two approaches to the use of video ID, involving either the real time engagement with a live operational agent handling the call, or an unattended self-recorded video session that is later reviewed and validated by a live agent, or

<sup>27</sup> In Germany this is only allowed for federal authorities. See other remarks regarding access to information contained in the electronic chip of biometrics ID documents.

<sup>28</sup> At publication date of this report, NFC on IOS is opening. Next to Android based mobile phones also iOS based phones are available for eID solution in Germany. Apple opened NFC for AusweissApp2 in Germany with iOS13.

through an automated process. The approach involving live agents has delivered very poor user experience, mostly driven by the complexity of managing the queues of incoming calls (like in a traditional contact center) but with the customer not expecting to have to wait in the web/online channel. It also introduces significant costs for the financial institution, which is why the offline approach is gaining ground, but it requires measures to be taken to compensate for the additional risks.

6. **eID:** authenticating the link between the prospective customer and their possession of an electronic identity token (e.g. a physical token, a mobile application, or a chip within an identity document) with the necessary level of assurance for the type of account being opened, thereby re-using evidence of a prior identification session with a trusted identity provider. Please refer to Annex II of the PWC report for further examples. It is notable that the strength of these systems carries a satisfactory level of assurance because they intrinsically couple identity verification with authentication of the owner of the identity.
7. **Personal ID Data:** Verification of the customer's identity from independent and reliable third-party sources, such as Credit Reference Agencies, where the customer's identity is assessed based on the quantity of reliable data held on file, the linkage between the prospective customer and that data, reflected in quantitative form and decisioned through automated rules and/or scores.
8. **Legal Entity Identity Documents and Data:** Verification of the identity of a legal entity can be partly achieved through interrogating formal databases which hold data and digitized images of documents about the formation, structure, ownership, financial performance, and Directors of the business. This is complemented with the provision of images of documents, such as proof of authority to operate the new account, and verifying the identity of individuals associated with the business – such as the authorized user, ultimate beneficial owner.

Just as the method for capturing evidence of identity varies, so does the location of the processing; certain aspects of the identity verification process are executed within the application on the customer's device, other aspects, which require higher processing power, such as facial verification, anti-forgery checks and in some cases Optical Character Recognition, are carried out on the server side.

In nearly all the aforementioned approaches to capturing evidence of the customer's identity, the providers of financial services contract with commercial third-party vendors to provide technical aspects of these services. The risks associated with using third-party solutions are covered in a separate chapter in this report.

The correlation between the evidence of the customer's identity, i.e. documents, data, eID etc., and how it is captured and checked, is addressed within a report written by Sub-Group 2.

In summary, identification evidence is largely the same as it always was – government issued documents suitable to evidence a customer's identity. What has changed, and continues to evolve, is the method by which identity documents are captured, processes to automatically verify that the identity document is associated with the prospective customer bearing it, the automation of anti-fraud and forgery checks, and the use of eID in some Member States.

#### Coverage and extent of use of identity verification solutions

In the absence of authoritative data or recent published surveys on the proportion of applications processed through the different types of identity verification solutions categorized in the above section, the Sub-Group has provided its own perspective on use of these within the sectors of the financial services industry with which the team members are familiar. With the caveat that this may not be truly representative of the industry, we have attempted to summarize our observations on the proportion of customers whose identities are verified using the various categories of solutions.

The extent to which these sorts of solutions are used varies between countries in the EU, the technical abilities of the provider of financial services, the type of product being applied for, and the attitude of providers and their country-based supervisors towards risk.

The dominant method of identifying customers is through the fresh provision of identity document(s) for each newly opened account. There are a few deviations to this general position which arguably facilitate less frictionful approaches:



- There is dominant and widespread use of bank facilitated eID schemes in the Nordic region, Estonia and Luxembourg
- There is a sizeable and increasing penetration of the use of eID in Belgium and Holland
- Countries such as Germany are well placed to use eIDs through the provision of electronic identity cards and policy innovation to streamline identity verification processes for its citizens
- The UK stands out as a country which uses a blend of Government issued documents (typically passport / driving licence, but not identity cards) as well as identity data solutions from Credit Reference Agencies – the latter are explored in more depth in the analysis of identity verification solutions in on-boarding Journey 7
- Video-technology is used effectively in Germany, Spain, France and Estonia (e.g. a presentation by WebID reported >10m successful identifications since launch in 2014)
- Entirely remote on-boarding using trust service provided via smart device is gaining market penetration in Bulgaria as most of financial institutions are using trust services in their digital processes for account opening, loan contract signing, etc.
- The identity of legal entities is invariably a hybrid process drawing on information from centralized public register resources such as Companies House, as well as commercial data providers which draw upon those public registers, and add additional layers of information to it such as financial performance data, risk scores, company ownership analysis, and more. Aspects of the identity verification process which cannot be completed by using these online resources will necessarily involve the provision of documents. Individuals associated with legal entities can be identified in the same way in which they would be identified if they wanted to open an account for themselves.

On the face of it, there are few reasons for thinking that these solutions cannot work on a cross border basis. Clearly where face-to-face identification is required, and there isn't a suitable or convenient alternative which has been integrated into the systems of the provider of financial services (and authorized by their supervisor), then the cross-border customer may be subjected to a more protracted identity verification process than a domestic customer. Customers making cross-border applications may have to produce evidence of their identity and evidence of their address, and it's likely that they would experience some iteration in the account opening flow when providers of financial services invoke non-standard processes to complete their on-boarding checks.

At the time of writing this report, we do not have a clear view on the extent to which the main types of current ID solutions work on a cross border basis, and how realistic it is to suggest that eIDs would solve this issue, or whether they would encounter the same challenges as traditional identity solutions. Indeed, we look forward to AMLD5 providing a clear legal basis for using eIDs to meet the identity verification requirements for account opening.

#### [New and emerging innovative solutions for identity verification](#)

Looking ahead, the following list provides examples of novel or innovative approaches towards the verification of identity.

1. Four types of non-attributed solutions described in Annex V of the PWC report
2. Opportunities described in Annex VII of the PWC report describing innovations in KYC portability, cross-border opportunities and incentives, and KYC attributes
3. The use of blockchain to facilitate retention and access to digitized identity documents and data across multiple Firms, negating the need for re-identification of the user
4. Self-sovereign identity capabilities, where a person controls access and availability of their digital identity information, and does not depend on any centralized authority. An example will be the adoption of a "trusted events" approach where users will share their event histories, i.e. the events that generated the customer data assurances, to relying parties for identification purposes. This approach will resolve some of the inter-operability issues that digital identity schemes face at present, one of which being the agreement of common standards among all parties.
5. Decentralized identity networks which overcome some of the privacy and security challenges with traditional identity data solutions
6. Use of non-standard identity sources which could be relevant for proving identity as well as conducting fraud checks

## 7. New analytical methods of assessing identity data based on techniques such as graph analysis and machine learning

The Sub-Group has not been able to take an in-depth look at these types of solutions as it has been concentrating on the main 'existing' solutions for identity verification. Therefore, at this point in the work of the Expert Group, it is an open question whether the challenges of cross-border account opening will be solved more effectively by any of these new approaches.

### Impediments to progress

The Sub-Group understands that one of the aspects of the European Commission's strategy to encourage competition and improve the choice of financial service providers is to safely remove barriers preventing the provision of cross-border services. It is thought that the use of eIDAS' notified eID schemes and trust services could safely satisfy the identity verification requirements when opening financial services accounts, and this approach is adopted within AMLD5. This increases the importance given to aligning the proofing processes across eIDAS and AML rules, which will create a stable policy platform for future use of eIDs in account opening. Feedback provided to the Sub-Group suggests that the gap is narrow.

It is a moot point as to whether solving for cross-border identification addresses all the challenges Firms encounter when opening accounts for new customers who reside in other countries, such as:

- Assessing the credit risks associated with a new customer whose credit history is held in a database in a different country; can that person's credit file be accessed online via API or a screen-based system, if not then can the data subject make their credit file portable per GDPR to so their creditworthiness can be assessed, can the Firm receiving this data understand and accurately assess the applicants historical creditworthiness, etc.
- Depending on the type of account being opened, establishing evidence of the new customer's income, and affordability of the new service
- Validating documentary 'proof of address', or integrating with data sources which provide such proof
- Potentially verifying employment information

These ancillary issues encountered at the point of account opening are not straight-forward to solve, and they introduce additional technical challenges. The point the Sub-Group are making here is that enabling streamlined cross-border identification through eIDAS services will be helpful, but there are other problems with cross-border account opening which need to be considered too.

The cross-border use of UK credit account performance data which is used to predict credit risk is approved in section 5.6.2 of the UK's Steering Committee on Reciprocity 'SCOR' policy document 'Principles of Reciprocity' (Version 40, dated May 2018<sup>29</sup>). It is assumed that reciprocal arrangements exist with CRA's in other EU countries. The provision of identity data does not carry reciprocity requirements and is made available on an EU wide basis.

Another barrier to the greater use of eIDs is developing compelling business cases to provide a positive Return on Investment 'RoI' for the cost of integrating with an array of eID service providers. This barrier to integration will lower over time as we see increased coverage of eIDs across EU Member States. However, there is competition within financial service providers to assign technical development capabilities, as well as Capex and Opex to projects which vie for those resources. Providers of financial services must decide how to assign those resources within their over-subscribed technical development roadmaps, and unless they plan on entering a market where the use of eID is prevalent, the case for using eIDs may not be as strong as investing in other forms of remote KYC. The collection and publishing of quantitative data points by each member state on the actual numbers of customers issued with eIDs and the scale to which they are used for verifying identity at the point of on-boarding would help make the business cases for integration with eID services.

---

<sup>29</sup> <http://www.scoronline.co.uk/sites/default/files/PoR%20version%2040.pdf>

As eID solutions have been created by different public and private sector entities, it is of vital importance that they are interoperable, meaning that eIDs issued by one system can be recognized by another system, and reusable across different geographies.

A potential solution to these challenges is for providers of financial services to work with FinTech integrators to minimize their own development efforts, and leverage FinTech partners to integrate with various eID services on their behalf. This approach works well when Firms are cash rich but development poor.. It has been voiced that a strong driver for integration with eID schemes is experimentation to help understand the customer perspectives of using such schemes.

Providers of Financial Services are highly focused on creating streamlined user experiences which achieve policy objectives with minimal user interaction. One of the most important metrics reported to shareholders is the number of new active customers acquired during the reporting period. If there is a convincing case that this metric would be strongly fuelled through higher levels of onboarding by customers who have been previously issued with eIDs, and customers would therefore enjoy a streamlined onboarding process, then there are strong grounds for suggesting that Firms will be eager to integrate with eID services. However, the opposite is true for new customers who are yet to be issued with an eID if the Firm is obligated to take them through the eID issuance process.

Furthermore, some eID providers insist that if an eID is used for identity verification in a KYC setting, then it should also be used for ongoing authentication at log-in or at the point of making a transaction. Firms may not want such a contingent obligation placed upon them, as they are likely to have alternate methods for authenticating customers, and the on-cost of such an expense must be factored in to the investment decision.

Turning to more general problems with remote KYC solutions, there are limited databases of lost or stolen identity documents. Providers of identity verification solutions apply detailed checks to mitigate the risk of fraud and forgery, but these could be complemented by an accessible online database of lost or stolen identity documents orchestrated across all member states and would help protect victims of fraud from further abuse. Similarly, it would be helpful if authoritative feedback loops were provided to establish the susceptibility of new identity verification solutions to the risks of fraud and forgery. High error rates e.g. where the evidence of identity is assessed as being genuine but transpires to be fraudulent, would give cause for concern, and it would be helpful to understand how Firms can confidently and safely cooperate to address this.

The use of NFC within mobile devices is an extremely attractive solution, but it is somewhat impaired by the current reluctance of one type of handset provider to enable NFC functionality within their devices.<sup>30</sup>

With regard to verifying the identity of legal entities, these processes are much more convoluted than those for verifying individual identity, where the level of friction is compounded by the number of people who need to be identified, as well as the collection of more documents.

### Initial Conclusions

There are few excuses for thinking that customers cannot be safely identified through remote channels. To this end, Firms implementing innovative identity verification solutions should carefully read the European Supervisory Authorities' opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process<sup>31</sup>. Technical and policy advancements supporting the innovation of new identity verification solutions should enable most customers to identify themselves to local providers of financial services. However, the cross-border position is a more complex problem carrying challenges other than those relating to identity.

---

<sup>30</sup> See above about NFC opening.

<sup>31</sup> [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)

The business case for integrating with eID solutions varies from one country to another. In fact, the case is strongest in countries where the use of eIDs is the dominant and most convenient means of identity verification, or where the investment decision is supported by other factors – such as experimentation and accelerating the learning from real use of such systems to justify expansion into other markets. Technical interoperability across multiple eID systems is essential for regional providers of financial services, as well as enabling domestic providers of financial services to easily identify customers from other countries.

The Sub-Group is not informed by quantitative data points on the scale of adoption of eID solutions, and clear empirical statistics on the scale of use of all types of eID solutions would better inform decisions on the timing for commercial investment to enable integration with these types of solutions.

The Sub-Group recommends that the EC permit solving the problem of enabling NFC across all types of mobile handsets, thereby enabling use of solutions designed to read the identity information accessible within electronic identity documents.<sup>32</sup>

---

<sup>32</sup> See also on this subject eIDAS Cooperation Network Decision 01/2019 (on the need for open access to NFC interface to support secure mobile use of electronic identity means):

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=100663614>

## Chapter 5: Risks associated with using eID and remote KYC identity verification solutions, and how those risks can be mitigated

### Introduction

The purpose of this chapter is to consolidate and summarize the risks associated with Firms using the various types of identity verification solutions referenced in this document. This will primarily focus on the common types of identity fraud, and how a fraudster might successfully conduct such a deception.

It should be noted that although the detection of identity fraud risks is often included within the identity verification solution, they can still be supplemented by other fraud detection systems that operate independently and can mitigate the apparent fallibility of the identity verification solution. This is explained in more detail in the section on supplementary controls.

As this chapter is co-authored by the sub-group, we have drawn on the collective expertise of its members to compile and reflect on the typical types of identity fraud we have encountered. It is likely that there are additional types of identity fraud methodologies outside of the subgroup's combined experience, though we believe we have covered the main themes.

### Identity fraud risks

The table below sets out the more commonly encountered methods of identity fraud conducted at the point of account opening, and how they can be detected. The capability of different types of identity verification solutions to detect these types of fraud remains a moot point and may well vary between different implementations of the same solution, or same type of solution. For this reason, we have not attempted to grade the solutions by their effectiveness, and Firms will need to decide for themselves how effective they are in practice at detecting different types of identity fraud.

#	Category	Description	Key detective control
1	1 <sup>st</sup> party claimed impersonation	The account holder claims to have been impersonated, when in fact they opened the account.	Retaining evidence of the authentication process which compared the physical features of the customer in session with their proof of identity.
2	1 <sup>st</sup> party partial identity fraud	The prospective customer falsifies an element of their identity to open the account which would otherwise be refused, e.g. date of birth or address history	Detecting the falsified field on the ID document. Address history may be misaligned with credit bureau records
3	1 <sup>st</sup> party friendly impersonation	Family member accurately impersonates another family member	Authenticating the physical features of the customer in session with their proof of identity
4	1 <sup>st</sup> party collusion	Applicant opens the account with a view to supplying the log-in credentials and payment instruments to another person who will permissively adopt the identity of the account holder	Application fraud detection systems involving cross-industry data sharing can expose fraud ring activity and links to prior fraud cases. The type of account being opened may be inconsistent with the demographic profile of the applicant, there can be other inconsistencies in the application such as employment information. Constant AML vigilance during lifecycle of the account for consistency with known or declared information available e.g. transactions, location data, device fingerprinting etc. An ongoing process is needed to mitigate the risks.

5	Identity theft	<p>Third party impersonates another person, in many cases the victim resides at the previous address provided on the application form, and the fraudster states they have only lived for a short time at the current address. Or the victim has recently moved out of the address which the fraudster now controls.</p> <p>Forged and altered identity documents to match the identity information and physical features of the fraudster aimed at defeating biometric comparison.</p>	<p>Strong capabilities to detect forged proofs of identity and address.</p> <p>Capturing identity information from the electronic chip inside the identity document.</p> <p>For previous address impersonations, the victim of the fraud could have a live phone subscription at the previous address. In these cases the proof of identity may be forged or misalign with DOB for victim at previous address.</p> <p>For current address impersonations there will probably be forwarding address indicators from the current address on the application to the victim's new address.</p>
6	Deceased impersonation	The fraudster impersonates the identity of a deceased person.	<p>Newly issued proofs of identity and address. Data history may be inconsistent with the age of the applicant.</p> <p>National deceased people register could be checked at the account opening. This is automatically checked by eIDAS nodes, when electronic identification means are used.</p>
7	False identity	Creation of a false persona supported with synthetic proofs of identity	<p>Forgery detection.</p> <p>Where possible, checking issuance of document against national registers.</p> <p>Thin credit file with an absence of historical data.</p> <p>Images of synthetic ID documents may lack evidence of physical use.</p> <p>Authenticating the physical features of the customer with the proof of identity may be a preventative control (i.e. the fraudster must succumb to linking their face to the fraud they are in the process of committing).</p>
8	Legal entity identity theft	Changing information held in public registers of corporate ownership, officers, address, to correlate the whereabouts of the legal entity to false identities and physical locations under the control of fraudsters	Recent change of directors and registered offices. The newly registered office and business premises may not align to the size and history of the legal entity, e.g. use of shared office space, accommodation addresses, etc.

Identity fraud is also conducted against open accounts, for example 'Account Take Over', and although some types of identity verification solutions can help detect this, it occurs downstream from the point of account opening, and is therefore out of scope of this report.

It should also be stressed that due to remote identification situations, massive fraud attacks are liable to occur, and to a lesser extent, systemic risk.



## Detection and mitigation of identity fraud

The processes for detecting these types of identity fraud fall under three main headings; verification, forgery detection, and consistency. The detection of genuine but lost/stolen documents is not included as this could be solved through verifying the applicant to the proof of identity, and in some countries through lists of stolen documents.

- I. **Verification.** The process of checking that the applicant in session is the true owner of the identity. This is typically achieved manually and/or automatically by using biometrics or trained operational agents to compare the facial image of the applicant to the facial image on the identity document or the facial image inside the chip within the identity document, and in a remote setting ensuring that the verification process is not evaded by the absence of an effective liveness check. There is a risk of artificial reproduced video to impersonate someone from thousands of images (“deep fake”), but this can be mitigated through assessment of the images and transmission of a TAN during the live session. German BSI has demonstrated that with usual hardware manipulation of the video stream (live) is pretty hard to discover but in practice no incident has been detected. The risk of fraudsters using 2D or 3D marks is detected by using technical capabilities in identity proofing solutions and biometrics. In general terms, human beings are better at performing liveness detection, and automated identity solutions which use biometrics perform better than humans in comparing an applicant and a picture. The authentication capabilities associated with digital identities including validation against a centralized database and revocation lists, should mitigate the risk of the identity being used by a third party. It is also noted that some national data protection authorities are reluctant to permit the storing of data containing biometric information of individuals, while some other national Data Protection Authorities have provided guidance to allow such storing and processing in the framework of their data protection law. As such, a higher technical solution/controls may need to be sought to mitigate the risk of identity theft.
- II. **Forgery detection.** Automated and/or manual processes confirm that certain types of identity documents are genuine through checking security features, algorithmic checks, and that the documents has not been fraudulently altered. In face to face environments, this can include the use of specialized scanners and trained operational agents. In a remote setting, the capture of the image of the identity document includes processes which detect the correct type of security features are present, and suppliers of identity verification solutions conduct automated checks to validate that the document is genuine. New advanced approaches to the detection of templated forgeries enables the same forged template to be quickly re-detected through unique features on the document. Access to national registers of identity documents is an opportunity to improve upon this process and should be promoted and used. Another security measure will include the reading of the electronic chip embedded within the ID document as opposed to relying on the photograph of the ID document presented.
- III. **Consistency.** Cases of collusion can be exposed through application fraud detection systems involving data sharing across the financial services industry. The demographic of the applicant may be inconsistent with the type of account being applied for. Collusion which amounts to coercion can also be exposed through the applicant being carefully questioned by bank staff. Consistency is also relevant when using electronic identity solutions, and is often supplemented with data sharing processes. Consistency checks are critical to detecting identity fraud of legal entities.

Most of the identity verification solutions reviewed by the sub-group contain similar approaches towards verification of the applicant and detection of forgeries. Solution providers will vie with each other that their solutions are more effective, economic or convenient. This is a matter for each Firm to decide for themselves.

Consistency checks are provided in various forms within electronic identity solutions such as those provided by Credit Reference Agencies and closed-user groups sharing data for prevention purposes.

The types of identity fraud that cannot be clearly detected through identity verification solutions are instances where the real owner of the identity initiates the fraud in their own persona, and the deception concerns the future use and exploitation of the financial facility.

### Supplementary controls

Application data sharing within closed-user groups, which involves sharing data about known fraud cases and victims of fraud, and comparison between application information and the applicant's data history with other institutions, are effective ways of detecting identity fraud. These supplement the identity verification solutions and are particularly effective at detecting fraud ring activity.

Fraud data sharing prevents the persistent use of stolen and false identities and serves to protect victims of identity fraud from further attack and can help pre-empt the use of vulnerable identities from being exploited. Organizations such as CIFAS<sup>33</sup> and National Hunter<sup>34</sup> are two examples of long established and effective data sharing schemes, in addition to those provided by Credit Reference Agencies.

Confirming the identity and control over the funding source, e.g. through a bank transfer into the new account (if the name of the account holder is revealed), or micro-deposit/PIN process, is a way of reducing the risks of identity fraud and is particularly relevant to the use of electronic wallets. Confirming the ownership of the funding source through centralized databases is another type of control that mitigates the risk of fraud. The Account Information Service Provider 'AISP' provisions within PSD2 would be an alternative way of confirming control over and ownership of the source of funds. Normally it is provided by Regulation 2015-847, but applied differently according to countries. DIAMOND SEPA MAIL should also permit to verify the information relating to the account holder for a given account number. The confirmation of the information of ownership by the MNO (telco operator) is also a best practice, even if this identification is weaker than a transfer from a bank (assuming the identification is made by another bank).

Sending the customer payment card to their home address, and other physical correspondence, mitigates risk as a fraudster would require physical access to those premises.

Initiating the first payment from a bank's branch premises deters fraud through the risk the fraudster takes of being physically present in a controlled environment with CCTV coverage.

Using a second channel of engagement, such as sending a TAN to the customer's mobile phone or email address whilst they are in session, can help address spoofing risks.

Data sources can help link the identity of the customer to the subscriber of the customer's phone number, and similarly to their email address, and flag potential fraud risks with the phone and/or email details.

Knowledge Based Authentication 'KBA' can link the customer in session to an established record of that identity, but the strength of this process very much depends on the configuration of the system – such as how many questions have to be answered correctly, what type of questions are asked, how many re-tries are permitted over a given period of time.

The scale of identity fraud in the UK is published in the CIFAS 'Fraudscape' report<sup>35</sup>, and provides objective visibility into the scale of the problem. In 2017 there were 174,523 cases (up 1% on 2016, but down 8% in the banking sector). The report reflects on other dimensions of identity fraud including the demographics of victims, and year-on-year variances in levels of different types of fraud.

### Other risks associated with using identity verification solutions

1. Risks that similar technical solutions produce varying levels of identification assurances.

From the outset, some of the remote on-boarding solutions, may appear to have similar functionalities but in reality, may work very differently and lead to varying levels of identification assurance.

To mitigate this risk, EU regulations that talk to the use of new technologies such as video conference can help Firms better assess the technical solutions. In certain cases, these regulations may also refer

---

<sup>33</sup> <https://www.cifas.org.uk/>

<sup>34</sup> <https://www.nhunter.co.uk/>

<sup>35</sup> <https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Fraudscape%202018-Final.pdf>

to complementary technical provisions that can be issued by other authorities such as the Finance Ministry. This also implies that regulations permit these new identification means, provided that solutions could be assessed under objective criteria, like eIDAS schemes or other acceptable industry standard norms (e.g. ISO Certification<sup>36</sup>). This will also entail regulators to have employees with technical background.

To better understand the technical solutions employed, banks will also need to self-assess and document any new processes they propose to deploy. A legal and IT study can be undertaken, which should include a Privacy Impact Assessment focussing on IT risks and risks linked to solutions. In particular, IT analysis can perform intrusion tests to assess the technical strength of the solution.

## 2. Risks of false declarations by the person

These could be prevented through automated processes cross checking declarations with supporting evidence. In addition, interactive questionnaires can help further detect contradictions. The use of data, data cross-checking and artificial intelligence can largely mitigate this risk.

## 3. Risks to confidentiality of customer data

These risks could be assessed by conducting a prior Privacy Impact Assessment (PIA) as provided under GDPR. In particular data exchange with third party suppliers should be made through protocols that ensure data confidentiality.

It should be noted that solutions which record video recordings of identity verification sessions may be viewed differently between Data Protection authorities and Banking supervisors. What is perhaps best practice for one entity creates heightened risk for the other.

## 4. Cybersecurity risks

Aside from the risks of data being intercepted in transit, it is also at risk of loss, unauthorized access, or other damage whilst it is held within the domain of a third party supplier

## 5. Vendor Management and Subcontracting risks

It is somewhat inevitable that identity verification solutions are sourced from external vendors who have developed technical expertise in their domain, which would be less likely to be developed through in-house development teams. This brings the opportunity to compare the efficacy of similar competitive solution providers and select the most effective and relevant solutions for a particular use case, product type and customer journey.

Firms must ensure that the tuning of identity verification solutions correctly balances the demand for high pass rates which help deliver the business case for investing in them, with very low error rates. This is very important where the identity verification process assesses the identity of the applicant as being genuine when in fact the applicant is not the owner of that identity. Automated systems will also yield false alarms, often associated with mis-reading text on identity documents which differs to the particulars provided by the applicant. Such false alarms create disruption in the customer experience and usually incur operational costs, but they do not expose the Firm to the risk of fraud.

In addition to opportunities of using vendor solutions, the use of third-party suppliers also brings risks for the Firm using them, and effective and structured testing of third party solutions is important to make sure they are configured correctly, and that control over the solution configuration is maintained through the lifecycle of their use. In this regard, the ESA report 'Opinion on the use of innovative solutions in the customer due diligence process' is an important reference document.

Furthermore, there is a risk of financial institutions being dependent on a few major players for remote solutions, e.g. IOS and android for client identification or smartphone bots/apps. The lack of market

---

<sup>36</sup> Multiple ISO technical standards can apply for identification. For instance ISO 19794-5, ISO 27 001.

Reference to standards also permits consideration of future technologies even not existing for the time being for identification purposes.

players or in certain cases an effective duopoly, may restrict a bank's ability to challenge, negotiate or adopt alternative solutions.

There is a raft of other risks associated with the use of third parties that need to be considered, assessed and managed, including; information security, sub-processor risks, physical security, privacy, confidentiality, procurement, performance effectiveness and availability, financial viability, PR, corporate social responsibility, resiliency, records and information governance, sub-contractor risk. These risks must be recorded, assessed, monitored and managed through the duration of the relationship.

With regard to the risk of resiliency, this can also present an opportunity for optimization. Depending on the nature of the solution, it would be risky to have just one supplier for a critical service, and by selecting and implementing two competitors it is possible to measure their comparative performance, switching the whole flow in the event of service disruption ('fail-over') or selected traffic ('waterfall') between suppliers according to their performance. Banks could also offer two different kinds of journeys in order to be able to reorient clients in case one of the process is compromised.

#### 6. Risk of over-simplifying journeys to achieve customer convenience

There should be a healthy tension between security and convenience. New identity verification technologies make it possible to achieve both aims, though there will always be pressures to improve convenience as well as close security loopholes. On balance, when it comes to identity verification, we should not make the perfect the enemy of the good.

As an overall observation, Firms must ensure that the tuning of identity verification solutions correctly balances the demand for high pass rates which help deliver the business case for investing in them, with very low false positive rates.

#### How else can these risks arising in the use of identity verification solutions be mitigated?

The expert group has heard repeated calls for the following issues to be addressed:

- I. An EU wide consolidated source of lost or stolen identity documents
- II. An EU wide solution to verify that an identity document is current and valid. An example of this is the Australian Document Verification Service<sup>37</sup>.
- III. Application data sharing and identity fraud data sharing schemes (these may necessarily be country based rather than EU wide)
- IV. As far as NFC in mobile is one technical possible solution among others, influence mobile handset manufacturer to enable NFC reading of electronic identity documents, as relying on the data inside the chip of such a document, and the process for accessing it, is less risky than relying on an image of the physical document
- V. The promotion of digital identity schemes and effective means of interoperability to enable cross-border use of digital ID's, will over time encourage more Firms to use these stronger forms of identity verification solutions, remembering that convenience is a stronger commercial driver than security. The use of these schemes would appear to be more attractive when reliance can be placed upon them to compliantly establish a new customer's identity without the need for additional identity verification measures.
- VI. New identification technologies for on boarding should be promoted in national AML regulation (refer Risk 1 above).
- VII. New technologies like Artificial intelligence, data use like digital data fingerprint, should be promoted in fraud detection. Fraudsters profiles could be drawn and permit the avoidance of frauds.

---

<sup>37</sup> <https://www.dvs.gov.au/Pages/default.aspx>

## Chapter 6: Conclusion

In today's world, where interactions are increasingly becoming borderless and digital, having a trusted and re-usable digital identity recognised across a wide ecosystem of players is a key enabler to any economic and social development. The OECD<sup>38</sup> has written about the rapid rise in the need for robust digital identity management solutions and envisaged a dramatic increase in consumer demand for privacy and protection from identity fraud.

With this in mind, we have drawn from this report several concluding points and areas of future works:-

### 1. Proportionality of security measures

***Excessive measures will adversely impact customer user experience. A balance needs to be struck between customer adoptions and security requirements, considering different levels of security, and also AML/CFT risks.*** Security and KYC measures must therefore be **proportionate** to the risks present in the application, whilst ensuring compliance with the risk based approach as set out in the AML Directives. While it is positive in principle to increase security, it needs to be considered against the customer's risk profile and the risks associated with the type of facility applied for. Security is key, but if it is not convenient, people will not use the proposed solution.

For illustration, sophisticated technical video identification equipment can be defrauded by some kind of 3D masks. However, at present, the risks of these masks being used for account opening are very low as they are very difficult and costly to make. This **proportionality principle** aligns with the fourth AML directive which is based on risk assessment. In this respect, Estonian AML regulation is a good example of proportionality. Relying on national electronic ID to open bank accounts are sufficient in some cases, but only to a certain extent. Beyond certain statutory account limit, another means of identification (video identification or face to face) will have to be used to complete the electronic identification.

### 2. Cross referencing processes

***Almost all means of identification can be compromised given the right incentive. However, the identification methods can be strengthened through the adoption of a mix of security measures using different sources of information, rather relying on a single solution, in the situation of increased risk.*** For instance, the information provided by customer has to be cross checked against an authoritative source, or several data bases, and a transfer from a bank account relies on the identification made by another source (normally with a good liability rate). A balanced security profile consists of a **proportionate combination** of several reference sources.

Furthermore, processes blending the strengths of humans and machines can be very efficient. They combine machine capabilities such as real time biometric comparison with human sensibility and appreciation using interactivity. This also avoids the systemic risk from purely relying on technical solutions. However, this needs to be balanced against the fact that human intervention can hinder innovation leading to the use of automated solutions (e.g. Artificial intelligence) and therefore is more appropriately used in handling exceptions rather than mainstream identity verification processes within digital on boarding flows.

### 3. Electronic ID documents

Financial Institutions should be authorized to read chips within electronic national ID documents - subject to addressing any relevant security and data protection concerns. Limited access to the Near Field Communication (NFC) interface prevents financial institutions from developing new solutions that

---

<sup>38</sup> OECD 2015: [https://one.oecd.org/document/DSTI/ICCP/REG\(2015\)12/en/pdf](https://one.oecd.org/document/DSTI/ICCP/REG(2015)12/en/pdf)

improves user experience during onboarding processes, as well as increasing the robustness of identity verification processes.

The ability for mobile handsets to fully use their NFC reading capabilities for the purposes of proving customer identity by reading the chip within electronic identity documents should be enabled for both Public Sector and Private Sector purposes.

#### **4. The role of public and private co-operation in digital identity management**

For digital identity to truly take off and be adopted widely by consumers, it is important for the public and private sectors to work collaboratively to advance **interoperability** and achieve the **scale of adoption** that is fundamental to any successful digital identity scheme.

We need the European Commission to actively encourage the respective governments/regulators to foster a climate of interoperability of e-government digital identities with private sector identity solutions. Mandatory acceptance in private sector could accelerate and foster eIDA based e-ID solutions.

#### **5. Commercial viability of Digital identity schemes**

Any good and **sustainable** digital identity solution will need to make commercial sense for all parties involved (e.g. Identity providers, Relying Parties, Government and Consumers). Consumers will need to be incentivised to adopt innovative digital identification solutions if the process is relatively **frictionless** and **secure**, and results in a digital identity that can be trusted and re-used across public and private sectors and even across geographical borders.

It is also worthwhile to consider the opportunity costs to governments and private sectors of not developing an effective digital identity ecosystem. There are vast economic benefits to be gained from working collaboratively to create a safe, secure and privacy respecting ecosystem for managing digital identities. Maintaining a status quo and not advancing digital identity solutions will ultimately be detrimental to any country's economic growth.

#### **6. Customer acceptance**

The imperative and motivation for the customer to open a particular type of financial account defines their acceptance or reluctance to progress through the necessary security layers. Customer acceptance is dependent on several factors that are measured at each step of the on-boarding process (e.g. at the point of completion of on line forms; selfie; video interview; electronic signature etc.). If the process is too time consuming or complicated, the majority of applicants will abandon the process. The upload of identity documents and other supporting documents can also be an obstacle to completion of the journey. However, there are automated ways of reducing the burden of document handling. In addition, the acceptance of new identification technologies, like selfie or automatic data extraction, may depend on cultural or market maturity factors, but mostly depends on the easiness and quickness of use. Consequently, the use of fully automated processes will require highly technical security standards.

The customer abandonment rate is also dependent on other factors such as whether it is possible to sign contracts with an electronic signature. Conformity with European Court decision regarding provision of documentation under a durable support, leads to avoidance of the use of links. This means a more complicated and time consuming process as opposed to the use of links.

#### **7. Convenience of a Pan-European regulatory sandbox**

Innovation requires continuous, rapid experimentation in order to rigorously prove consumer acceptance, technical viability and compliance. However, the ability for private institutions to experiment and test new technologies/proofs of concepts at pace are limited by lengthy internal approval and implementation processes and the potential compliance risks.

To the extent that being compatible with national regulations and regulators' positions, A **pan-European regulatory sandbox** can be a great tool to promote and accelerate innovation in the financial sector, stimulate competition and deliver new customer benefits.



If properly set up, it can allow stakeholders to collect important insights and lessons learned, helping reduce the uncertainty around new technologies (or products, or services) before drafting a new regulation.

## 8. Data Protection

Data protection and digital identity management goes hand in hand. In today's digital environment, it is increasingly difficult for an individual to fully appreciate and understand who is gathering information about them. **If consumers do not feel that their data are protected, they will not transact online**<sup>39</sup>. Within Europe, the Global Data Protection Regulation (GDPR) seeks to manage that risk through enacting laws that reinforce the idea of an individual control over one's data, for example within the new range of Data Subject Rights. Invariably, as part of the digital identification process, data will be collected and checked for authenticity and KYC purposes. It is crucial that the data collection and processing are **relevant and proportionate** to the risks/profile of the customer and the services that they are applying for.

It is essential that the European Commission recognise the importance of putting data protection at the core of any trusted digital identity framework, and have strong laws to govern the collection, storage and sharing of personal data collected during the identity management process. A special protection is needed around biometric identity data that are more and more used for identification and authentication. Both the handling and storage of these type of data require additional security measures.

eIDAS is fully compliant with GDPR's minimization principle, and there is a separate European Commission work-stream group that will look into the e-eIDAS attributes necessary to achieve KYC.

## 9. Harmonization of rules and regulations of EU Member states

Despite the over-arching European AML directive that attempts to harmonize the different regulations relating to identity verification, there still exist significant differences across the Member states. This can hinder interoperability, raise additional costs/complexity and create an uneven playing field between financial institutions located across different states.

We should explore the possibility of further harmonizing the rules and regulations around identity verification with the objective of advancing interoperability and avoiding regulatory arbitrage.

However, it is acknowledged that ML/TF risk is particular to member states. Different Member States face different ML/TF risks, which should be set out in National Risk Assessment, and as such be in a position to adopt measures appropriate to their circumstances. Taking a "one size fits all" approach would be inconsistent with the risk based approach enshrined in EU law through the AML Directives and internationally through the FATF Recommendations and Guidelines. eID should focus primarily on achieving consistency and portability in the verification/authentication of customer identity, through interoperability and harmonization. In case of low risk, a true EU standard should be possible without country-specific exceptions.

## 10. New Technologies

AML Regulations should be sufficiently receptive towards the use of future identification technologies that may not be in place at present and remain technology neutral. eIDAS regulations or technical standards (ISO etc.) might be an appropriate venue for setting standards that facilitate interoperability and standardization. In this regard, we note that there is a separate European Commission workstream addressing eID interoperability.

## 11. Lack of standardization and interoperability

At present, the identity management framework in EU is fragmented with limited success in cross border or sectorial consumption of digital identities. This is partly due to lack of common standards, differing regulations within EU states and lack of trust. To further the objective of interoperability, there is a

---

<sup>39</sup> BBVA: Digital Identity: The current state of affairs /18-01

separate European Commission work stream that is looking into the eID interoperability framework with additional sets of attributes to enhance the portability of digital identity. The group's findings will be crucial in establishing an interoperable digital identity framework.

## **12. Technical Guidance**

The assessment of any remote identification solutions lies beyond AML regulations. It is reliant on the understanding of the technical as well as security aspects. For example, one has to understand the technological controls that the remote identification solutions employ to protect the integrity of the data and the data transfer. We recommend that **authorities developed guidelines or technical standards** to help support the implementation of technology solutions and also reduce the uncertainty that may arise when firms are trying new remote solutions. This will likely involve **technicians to support the authorities in drafting guidelines in this field.**

Looking ahead, additional questions will need to be addressed beyond this report. Creating a trusted and portable digital identity will require, among others, creation of common standards and an agreed digital identity management framework. This is the focus of another European Commission sub working group and their findings will contribute towards advancing eID interoperability among Member states.

## Annex 1: Typical on-boarding journeys

This Schedule presents an in-depth approach of the different types of remote onboarding journeys first introduced in Chapter 3. The below methodology is followed to support the detailed assessment:

Each typical on boarding journey will be described through a use case for the different on boarding steps. An assessment of such on boarding journey will then be made. Two identity checks will be considered: a) Authenticity and validity checks on the documents b) Identity verification, i.e. how the applicant proves to be who he claims. Both steps will take into consideration eIDAS criteria and the AML rules. Through the assessment, risks and associated mitigations will be identified and proposed. Methodology and assessment grid as described above in Chapters 1 and 2 eID/KYC\_Assessment criteria is detailed hereafter and shall be applied to each on boarding journey.

For the record **Commission implementing regulation (EU) 2015/1502 of 8 September 2015** (Annex paragraph 2.1), and **eIDAS Cooperation Network guidelines** (*Guidance for the application of the levels of assurance which support the eIDAS Regulation*) will be used.

For clarifying, it is precised that all of the following on boarding journeys do not use eIDAS electronic identification means. eIDAS rules are used only regarding the Enrolment phase of a scheme, as presented in § 2.1 of sub mentioned Commission implementing regulation. Next phases necessary for a complete scheme evaluation in view of a notification towards the European Commission will not be used (Electronic identification mean management, Authentication, Management and organisation). The purpose of the study consists in assessing the way the applicant is identified while a bank onboarding, which corresponds to the enrolment phase. eIDAS rules will be used to this end only.

## General identification rules under eIDAS and AML regulation

### **eIDAS REGULATION:**

**Assurance levels of electronic identification schemes are defined in Article 8 of the eIDAS regulation.**

The assurance levels low, substantial and high shall meet respectively the following criteria:

- (a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
- (b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
- (c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

How is defined E-idas Substantial level<sup>40</sup>?

Level Low:

The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

*The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.*

It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

Level Substantial, level Low plus:

The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and

The evidence is checked to determine that it is genuine; *or, according to an authoritative source*, it is known to exist and relates to a real person and

Steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;

## **AML REGULATION:**

4<sup>th</sup> AML directive Article 13-1 provides that Customer Due Diligence 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;

(c) Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

And 13-2, that obliged entities may determine the extent of such measures on a risk-sensitive basis.

eIDAS regulation (Commission implementing regulation (EU) 2015/1502 of 8 September 2015) defines an authoritative source as any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity).

As a result of a comparison between these two regulations, AML and eIDAS, in both of them identification is based on two main phases: verification of the customer identity and identification of the customer. Verification of customer identity consists in verification identity information. This information, whatever its support (paper or electronic data) has to be obtained from an authoritative source. An authoritative source as defined under eIDAS constitutes a reliable and independent source. Then identification consists in insuring that the claimer of an identity is that person having this identity. At a certain level of confidence the claimer must be compared to the photo of the claimed identity provided by the authoritative source.

These two idea identification and claimer identification are not more precised in FATF recommendation 10, however they are described in FATF recommendation guidance on digital identity (still in draft when this report is written). In this guidance, Step 1 is Collection and resolution: collect core attributes and attributes evidence and resolve to a unique identity within a population or a context. Step 2 Validation.

---

<sup>40</sup> Commission implementing regulation (EU) 2015/1502 of 8 September 2015) Implementing Act

Authenticity and accuracy of identity evidence/information is determined and related to a living individual. Step 3 Verification, Confirm ID relates to the applicant.

At eIDAS level of assurance Substantial, verifications are made regarding the identity attributes and the claimer of that identity, both steps towards an authoritative source.

Consequently, the two regulations AML and eIDAS are aligned regarding identification requirements. An eIDAS Level Substantial identification could meet AML identification and ID documents verification requirements for AML standard risk. eID/KYC assessment grid as described in detail hereunder will then be followed for each typical onboarding journey, in order to approach an assessment under eIDAS of the onboarding journeys.

## Authenticity and validity check of documents eID/KYC\_grid

### 1- Authenticity checks:

#### 1-1 Following criteria have to be complied with, for the authenticity verification of the identity document:

- Comparison against reference databases (e.g. PRADO) or other sources providing detailed information about identity documents [e.g. <https://www.consilium.europa.eu/prado/en/prado-start-page.html#>]. This could help to identify a counterfeit document.
- All features (MRZ or not) correct
- Syntax
- Laminate- Physical security features in the documents, for e.g. ripples/backgrounds, holograms, OVID (type of hologram)
- Consistency (e.g. check-digit). Some attributes on an identity documents might include a 'check-digit'. This is often the last part of a numeric field which is derived from the first part (e.g. modulo '97)
- Is the photo the genuine
- If not checked against an authoritative source how is this check for remote onboarding?
  - At High level, the photo has to be checked against an authorized source. That could be directly possible with the use of the chip containing the photo, or towards a national database.
  - Staff checking the physical documents must: have received an appropriate training and have a good knowledge of the documents design and their security features; be able to identify forged documents, by inspecting them; be able to use the equipment in an appropriated way (for example ultra violet lights).

### 2- Validity checks:

Under eIDAS regulation, the following criteria have to be met: status verification lost, stolen, expired against 'authoritative source' (private or public). Identity check of the applicant

For remote registration of identities, the identity proofing should be based on more than one identity evidence. The claimed identity should be informed of the ongoing registration by an alternative channel (i.e. not specified by the applicant) in order to counter identity spoofing.

Pertinent rules for face to face situations are following:

- Knowledge based verification processes could be used when applicable/possible as additional proof of evidence.
- The provider should verify that the provided elements (documents, biometric data) have not been previously associated to another identity in its system.
- For an identification level High, an identity document bearing a photography of the applicant must be presented. This photography must be checked under an authorized source. There are two reliable means to do that: either check against a register containing the photographs, or check using the electronic chip of the electronic identity document to access the photography contained in the chip.
- Then in a second step the applicant must be compared to the photography with a high level of confidence; that means reaching few negative false. Either this check is made by use of biometry, with performing algorithms or by an agent. The agent must be experienced and have received specialized training. He must also have a practical experience of documents authenticity and their security features, and be able to identify false or forged documents, by examining them.

Regarding documents/ -capture -video/photo:

Capture evidences (videos, selfies) must be archived for future investigation. Real time (video) analysis is needed, with image quality requirements (e.g. ISO 19794-5) (light, pixels, distance camera toward object/subject). Remote onboarding solutions should always make use of identity evidences containing a photo (or other physical characteristic) and should make use of biometric algorithms to compare the applicant with the claimed identity. Special attention should be paid if the communications channel isn't part of / monitored by the provider's application (e.g. Video chat via Skype).

*See also examples of the ways identification is contemplated under other JMLSG, EBA guidelines and European regulation.: Annex 3: Detailed analysis of eID/KYC Assessment criteria.*

## Attributes Collection:

*Please refer to the relevant figures of the on-boarding journey for the attributes collected. Annex 5: Digital On-boarding for Bank Accounts in Spain*



# Journey 1: Cross Channel journey (Remote & Face to face Identification)

Figure 1: Overview of on-boarding process

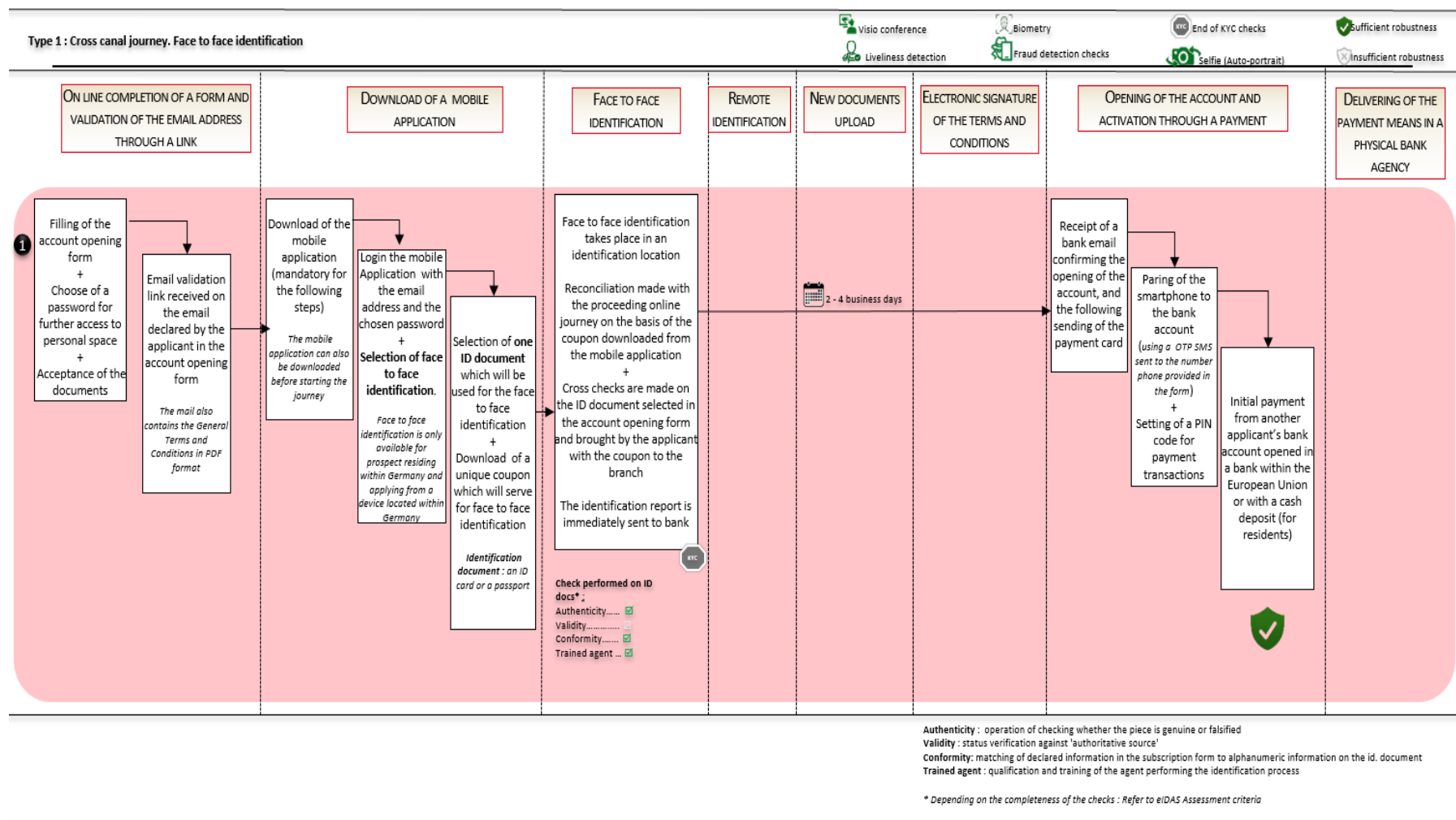


Figure 1 portrays a type of on-boarding process which typically commences with a remote online application supplemented with face to face identification.

The journey starts with the bank applicant filling in an online form from their internet website or via their mobile application. The applicant will have to register their email address, define a password and to subsequently confirm the validity of that address supplied by clicking on the email link sent by the bank. A welcome email initiated by the bank will also instruct the applicant to download the specified mobile application into their phone. All future steps will be actioned exclusively via the mobile application.

Through the mobile application, the applicant will select the location of their choice to conduct the face to face identification check. For some banks, they may choose to partner with external parties (e.g. Post office) to conduct the face to face identification checks on their behalf. The applicant will download a unique coupon which will need to be presented for the face to face identification at the location of the customer's choice. The face to face identification will involve the applicant providing the trained staff a government issued document (national identity card or passport) for identification.

Document authentication will be performed by the trained staff who will perform a physical inspection of the document. This may involve scanning the document with a specialized scanner which can access and cross check across multiple countries the authenticity of the document presented. The verification software will determine whether the ID document or passport presented is genuine. The trained agent will also conduct a face to face verification by comparing the individual to the photograph on the government issued document.

Once the face to face identification and verification of documents are completed, the results (Pass/Fail) will be transmitted to bank by the provider. Successful applicants will be notified by an email from the bank, confirming the opening of the account and the sending of the payment card to the applicant's residential address (within 2-4 days). The applicant will also need to pair his mobile phone to the bank account and set a PIN code for payment transactions. To activate the bank account, the applicant will need to initiate a bank payment from another bank in the EU or for a resident through a cash deposit.

#### Analysis of the journey against eID/KYC assessment criteria

##### i. Document Verification: Authenticity check

As far as a face to face identification is conducted, only one ID document is required. The identification document is verified by trained staff who scans them using a specialized scanner which is able to determine that the document presented is genuine by checking for irregularities, for instance, optical and security features. Depending on the provider or local regulation, smart card chips can be read. Based on the above checks and depending on the technology used, we can assume that the checks can reach eIDAS LoA High.

##### ii. Document Verification: Validity check

Under eID/KYC, the following criteria have to be met: Status verification lost, stolen, expired against 'authoritative source' (private or public). If one were to assume that the third party provider is able to access national registry or other authoritative databases, they could confirm the validity of the identification documents and thus reach eIDAS LoA High.

##### iii. Identity check of the applicant

The verification of the person is done in a face to face manner by the trained Staff. The eIDAS rules for face to face situations are as follows (Implementation of the eIDAS Regulation Execution Act EU 2015/1502 of the European Commission September 8<sup>th</sup> 2015):

- i. Knowledge based verification processes could be used when applicable/possible as additional proof of evidence.
- ii. The provider should verify that the provided elements (documents, biometric data) have not been previously associated to another identity in its system.
- iii. For high level identification, an identity document bearing a photography of the applicant must be presented. This photography must be checked under an authoritative source. There are two reliable means to do that: either check against a register containing the photographs or check using the electronic chip of the electronic identity document to access the photography contained in the chip. However, in certain cases, one can only rely on the photograph on the card as there is neither a register nor a chip available for the cross check to take place.
- iv. Then in a second step the applicant must be compared to the photography with a high level of confidence; that means reaching few negative false. Either this check is made by use of biometry, with performing algorithms or it can be made by an agent. The agent must be experienced and have received a training for that purpose. He must also have a practical experience of documents conception and their security features, and be able to identify false or forged documents, by examining them.

With regards to Journey 1, 1 identity document bearing a photograph of the applicant is required and compared against the applicant in person by the trained staff. We have made the assumption that the staff will have received the requisite training and skills to perform the identity checks.

Knowledge based verifications may be utilized by accessing national databases. As an example, In Germany, in addition to the national identity documents databases, the positive credit base called SCHUFA is also searchable. SCHUFA searches are made in other German banks to support their on-boarding processes.<sup>41</sup>

Assuming that the above mentioned conditions are met, and considering that the identification is made face to face, the eIDAS LoA can be High.

iv. Anti-Fraud Detection

The below anti-fraud measures are made by the bank to mitigate the risk of a false identity and the risk of impersonation.

<b>Verification of central identification elements</b>	<p><b>Physical Address</b> The payment card is mailed to the applicant's residential address. This ensures that the residential address given belongs to the applicant</p> <p><b>Mobile Device pairing</b> The applicant's smart phone is paired to the customer account with the pairing code sent via SMS. The confirmation of the information of ownership by the Mobile network owner can be considered, even if this form of identification is not the most robust as other controls (e.g. transfer from a bank)</p>
--	---

<sup>41</sup> This deals with "Knowledge based verification processes could be used when applicable/possible as additional proof of evidence." Criteria of the grid at the step "Identity check of the applicant". eIDAS Cooperation network guidance page 9 specifies that "Other Member States may go further in augmenting identity proof with multi-level security measures in matching several authorities's data (e.g. a tax records, which further gets matched with the population register sending activation codes).

	<b>Email</b> Validation email is sent to the applicant to confirm that the email provided belongs to the applicant.
--	--

#### Identification of risks and any mitigating controls

##### 1. Risk of a Fake or Forged Identity Document

The document verification measures undertaken to achieve an eIDAS LoA High should mitigate the risk of forged/fake documents to a large extent. Physical inspection of the documents (including detecting tampered photographs) by a trained staff can help mitigate the risks. The electronic nature of the ID document (e.g. reading of MRZ, chip) will facilitate the checking of the validity of the document.

##### 2. Risk of a non-valid ID Document

Risk can be minimized through accessing a national database (s) to confirm the validity of the identity document. This may differ between countries where access to national register databases are not made available to the private sector or that there is restricted access.

##### 3. Risk that the identity document is presented by an imposter

This risk is minimized to a certain extent by the risk management controls adopted in Point 2. It is worthwhile to note that while face to face identification reaches an eIDAS LoA High, there are certain technology solutions (e.g. use of biometrics) that can be equally effective if not more. Refer Journey 3 and 6 for examples.

##### 4. Applicant supplies false information during the on-boarding process

This risk exists in all customer on-boarding process, whether it be face to face or remote on-boarding. Trained personnel, as well as supporting documents, and database/register checks (e.g. negative or positive credit file checks) can mitigate the risks. In addition, KYC checks can help banks identify anomalies in their data provision.

Journey 2: Remote On-boarding based on enhanced KYC measures (with or without electronic signature)

Figure 2: Overview of on-boarding process

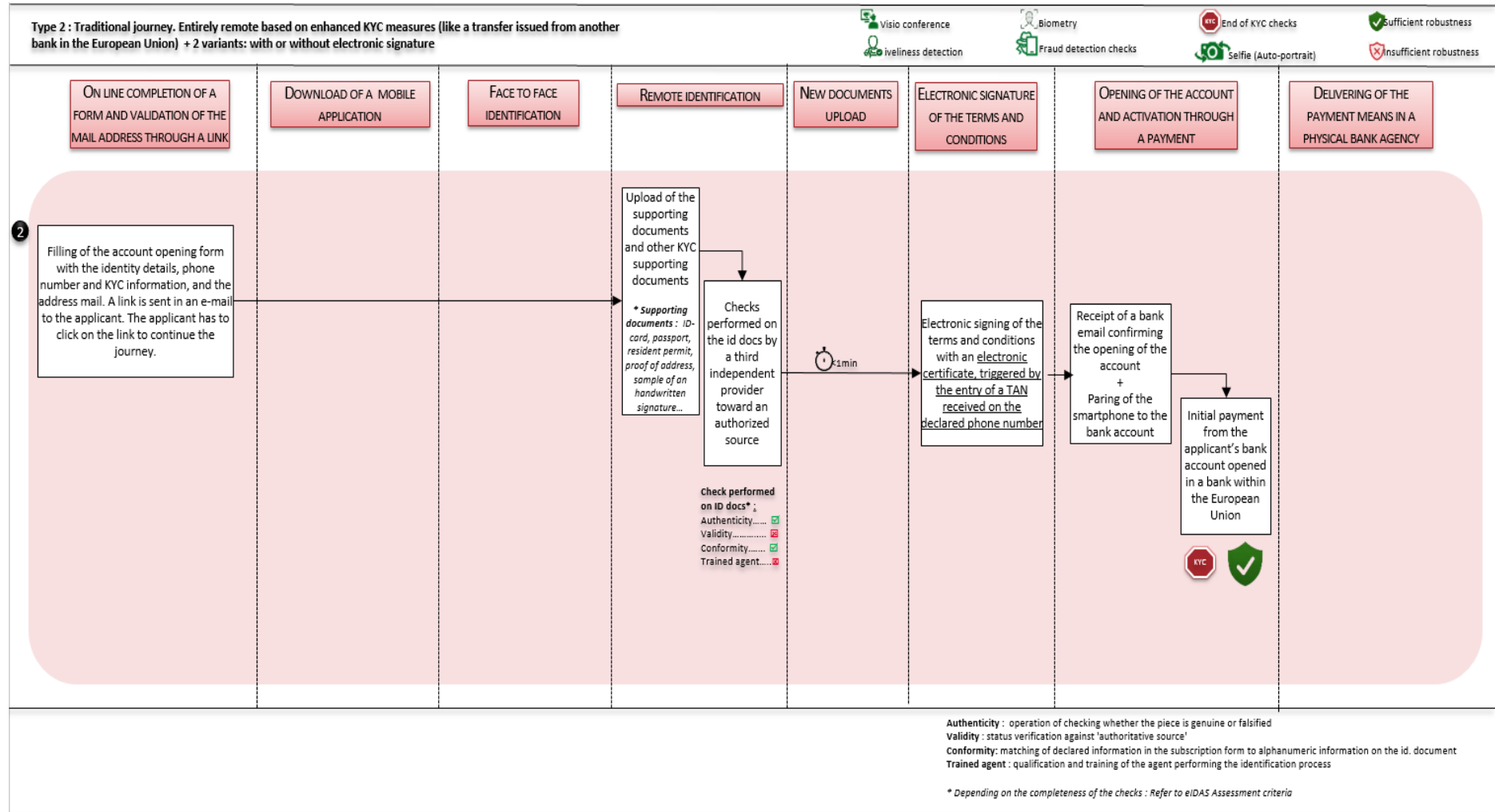


Figure 2 depicts a more conventional form of remote on-boarding process typically employed by financial institutions over the past decade. The process usually commences with the applicant applying online and filling in the account opening form with his/her identity details and KYC information, together with phone number, email and residential address. Email address is tested through a link sent to the applicant he has to click on, to continue the journey. The applicant will then proceed to upload the required identity and KYC documents. Documents may include national ID card, passport, proof of address etc. In general, the identification documents and means requested by the financial institution will correspond to their respective KYC needs<sup>42</sup>. The identity documents will be checked by the financial institution or an independent third party solution provider towards an authoritative source (that means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity; e.g. national registry database). Once the checks are completed, successful applicant will be sent a TAN to trigger the electronic signature process. The electronic signing of the terms and conditions can be accompanied by an electronic certificate. This signature can be considered as an advanced electronic signature provided it fulfils the eIDAS criteria for an advanced signature (Article 26<sup>43</sup>). Upon receipt, the financial institution will send an email to the applicant confirming the opening of the bank account and the pairing of the mobile phone to the bank account. In certain instances, there will be a need for the applicant to effect a bank transfer from another bank account opened in the EU to complete the account opening process.

#### Analysis of the journey against eID/KYC assessment criteria

##### i. Document Verification: Authenticity check

The authenticity checks on the ID documents may be conducted either by the financial institution itself or an appointed third party solution provider. Minimum checks may include Machine Readable zone (MRZ) verification and coherence controls on the ID documents, together with the information supplied by the applicant.

##### ii. Document Verification: Validity check

Depending on the providers and whether access to national registry or authoritative databases are accessible, validity and authenticity checks can reach at least eIDAS “Substantial”. A level of eIDAS “High” is likely not attainable as the ID documents are not used in their electronic form (i.e. no reading of the electronic chip within ID document).

##### iii. Identity check of the applicant

The identity check of the applicant is conducted via the supplement of additional identification means. For instance, the FI may require two forms of identification means a) an official ID document b) transfer from another bank account in the name of the applicant in the EU. Knowledge based verification (“KBV”) can be used when applicable/possible as additional proof of evidence. This allows verification of information given or declared by an applicant against a trusted source or data provider. For example, in France, KBV verifications towards national registers are limited. Due to data protection rules, the negative indebtedness register (registering only people in debt) can only be accessed for credit checking purposes (e.g. loan application, or credit card delivering). Knowledge based verification can be used when applicable/possible as additional proof of evidence. Knowledge Based Verification consists in verifying the applicant declarations against trusted data bases, or an authoritative source.

---

<sup>42</sup> There are various combinations of identification means that the FI may stipulate. They may for instance include a) submission of 2 identity documents and a wire transfer from another bank in the EU b) 1 identity document, a wire transfer from another bank in the EU & a statement of another bank in the EU

<sup>43</sup> eIDAS Article 26: Criteria for an advanced electronic signature:-(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.



For example in France, KBV verifications towards national registers are limited. Due to data protection issues, the negative indebtedness register (registering only people in debt) can only be accessed for credit checking purposes (e.g. loan application). A TAN can also be sent as an additional security measure. Given that there is a lack of comparison of a physical characteristic (s) of the person with an authoritative source, the process can reach “Substantial” level.

#### iv. Anti-Fraud detection

All contact details (i.e. address, telephone number and email) are supplied by the applicant. Where applicable, the contact details are verified (e.g. validation email, pairing of smartphone to bank account). These checks ensure that the contact details supplied by the applicant are accessible to the applicant and thus are presumed to be his.

#### Identification of risks and any mitigating controls

##### 1. Risk of a Fake or Forged Identity Document

The document verification and validity checks can largely mitigate the risks. This is largely dependent on the technology (deepness depending on the algorithms used) employed by the provider to detect fraudulent documents and this risk is exacerbated given the fact that the documents are not presented in a face to face situation. Physical checks have to be made on the documents: electronic chain of the electronic part of the document and consistency.

##### 2. Risk of a non-valid ID Document

Risk can be minimized through accessing a national database (s) to confirm the validity of the identity document. This may differ between countries where access to national register databases are not made available to the private sector or that there is restricted access.

##### 3. Risk that the applicant is not the person he claims to be

In this journey, the identification is predicated and reliant on prior processes that have identified the applicant. Supplementary measures (e.g. the use of Knowledge based verification (KBV) and a bank transfer from another bank account) can be used but it comes with its own set of risks.

For example, a bank account can be opened by the imposter in a country/bank with less stringent onboarding practices or the bank account access is being hacked. Focus on the different risks is as follow:

- A- Either the transfer account is issued from or is made to the applicant account, but that does not correspond to the identity documents.
- B- Or the applicant uses another person account. Two cases may be: the account owner is accomplice, or the account is used without the consent and knowledge of his owner.

Case A the transfer account is the applicant account, but that does not correspond to the identity documents.

Two cases may exist:

- A1: The account has duly been opened to the real person by the first bank, and that means the identity documents are false. See above authenticity and validity risk regarding the ID documents.
- A2: The account has been fraudulently opened. That is a general risk treated in this study, the purpose of which is to propose mitigations. The responsibility relies on the initial bank. What is unknown is the number of times that way of identification has been used for the same person by different banks. The risk could exist if the first account had been opened in a country or a bank applying lower identification ways. Fraudulent practices consist in disseminating money

as fast as possible. The acceptance of some banks or some countries could constitute a risk based approach.

Case B the applicant uses another person account. Two cases may be: the account owner is accomplice, or the account is used without the consent and knowledge of his owner.

- B1: the account owner is accomplice. To a certain extent AML watch on the accounts could permit to detect this fraud. It is unsure that the identity of the account owner (at least Name and Surname) is carried with the transfer.
- B2: the account is used without the consent and knowledge of his owner. For instance a BIC/IBAN has been found or stolen, or could have been formed. In this case a difference has to be made depending on a transfer is made from or to the first account in the other bank. For a transfer from this account, the applicant must be in capacity to operate the account. That could also be the case for transfers to such account, with a system used by PayPal, where a code is transmitted by the new bank inside the transfer, and the applicant has to reuse it for the activation of the new account. But it would not be the case for transfers to the first account without this security. In such case it is probable the account owner could not have reaction to such operation on its account. The name of the transfer issuer could also be confirmed by the issuing bank, carried as transfer metadata.

The risk can be mitigated if the name of the account holder is revealed when the bank transfer is done as confirmation of the metadata by the issuing bank. Normally it is provided by Regulation 2015-847, but differently applied according to countries. DIAMOND SEPA mail should also allow the verification of information relating to the account holder for a given account number.

Confirmation of the ownership information by MNO (telco operators) is also dependent on a previous identification, even if this identification is weaker as a transfer from a bank (due to AML regulation bank identifications are deemed to be trustful). This information can be qualified by MNO, giving for instance the age of the phone line.

On KBV, how secure are the databases that is being used to generate KBV questions and can fraudsters access that information and pose as the applicant will largely influence the extent to which the fraud risk can be mitigated. The person can thus be asked for his mother's name or his car registration number. This method leads to a scoring.

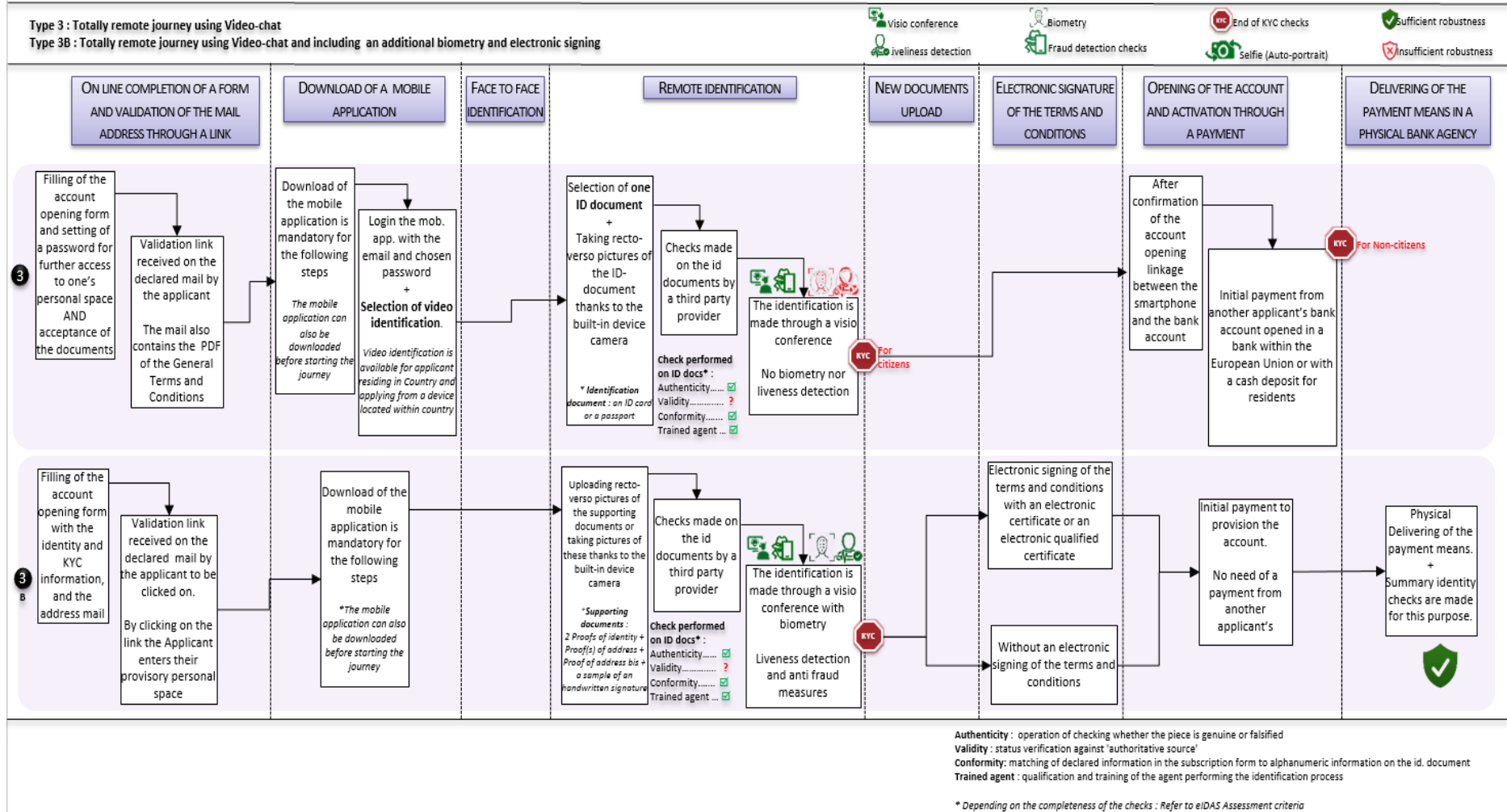
#### 4. Applicant supplies false information during the on-boarding process

This risk exists in all customer on-boarding process, whether it be face to face or remote on-boarding. Trained personnel, as well as supporting documents, and database/register checks (e.g. negative or positive credit file checks) can mitigate the risks. In addition, KYC checks can help banks identify anomalies in their data provision.

<p>As far as the first account (basis of the identity confirmation) has been opened in a secured way and that above mitigations measures are followed, this solution could reach an equivalent to at least Level Substantial. Note that a real assessment under eIDAS criteria of this identification process would require an assessment of the underlying identification process (i.e. general bank identification to reach substantial level, which indeed depends on different on boarding processes). Consequently eIDAS is not directly applicable to such processes relying on a previous identification.</p>
--

Journey 3: Entirely remote on-boarding journey supported by video conference and biometric identification (optional)

Figure 3: Overview of on-boarding process



For Journey 3, the remote on-boarding process is carried out using video conference identification and supplemented by biometric checks (optional). A video conference identification will consist of the following:

- Applicant to present the identity document to the camera which allows processing checks to be performed on the identity document and towards national data bases (in a possible variant the identity document is uploaded), AND
- Identifying the applicant through the video conference and a selfie extract of this video conference, against the picture bore by his identity document (with possible use of biometrics), AND
- Permitting to obtain complementary information relating to KYC, CDD and customer needs, and also permitting fraud detection.

This type of on-boarding journey using video identification permits the applicant to reach a one time on boarding without waiting for a transfer. It is also appropriate for young people who do not have a pre-existing banking relationship.

The applicant will start the process by applying online and filling/uploading the requisite information/document. The application can be done either using a mobile phone (via a specific mobile application) or in certain cases, via the bank's online application portal. In most instances, a validation link will be sent to the applicant's email address, the applicant has to click on to continue the journey. The applicant will then proceed to select the video conference as identification. A unique processing number may be issued to the applicant advising of the secure video connection. During the video conference, the trained agent will perform a facial recognition by comparing the applicant to the photo on the ID document and the applicant's selfie. In addition, an OTP SMS may be sent to the customer which the customer will have to verify at the same session. The video conference will also enable the completion of KYC/CDD measures and further anti-fraud detection measures. The entire video conference session will be recorded and retained according to the country's data retention policy.

The results of the application will be confirmed to the applicant (can be immediate in certain cases) and be followed up with the sending of the payment card to the applicant's address. The applicant can also proceed with pairing of his mobile phone to his bank account. In certain instances (to be compliant for cross border customers whose national AML regulation does not allow video identification), additional identification method will entail the applicant in making a bank transfer from another bank account that he owns in the EU. In other cases of a resident, a simple cash deposit is required to activate the payment card.

Journey 3B is similar to Journey 3A with the exception of additional biometric checks. The biometric checks as a supplement which increase the identification performance. The video conference relies on the biometric facial recognition by comparing the identity document picture (with a dynamic selfie of the applicant during the video session. Security measures like liveness detection come in addition to the biometric checks. In such journeys using video conference, liveness detection is made by the bank or provider human agent. Several means are used: questions to the applicant, sending of a code on the applicant smartphone.

#### Analysis of the journey against eID/KYCAssessment criteria

##### i. Document Verification: Authenticity check

The authentication checks on the documents utilizes both technological controls and the expertise of specialist third party providers. Depending on the provider, some of the authenticity checks will involve the provider accessing the applicant's terminal camera, and takes photos of the front and back of the ID document during the video chat session. The applicant will have to present the ID document to the camera in different angles to verify the optical security features of the ID document (e.g. hologram checks). Some country's legislation recognize video identification processes. For example, in Germany, BAFIN is prescriptive on the types of ID document that are permitted during a video identification process. Under BAFIN circular the identity documents permitted for Identification of natural

persons present via video identification procedures are only identity documents with security features that are sufficiently forgery-proof, clearly identifiable and therefore verifiable both visually in white light and using the available image transmission technology as well as which have a machine-readable zone which may be used during the video identification process as proof of identity pursuant to anti-money laundering regulations. The checks have to be made by a trained employee of the obliged entity or of a third party to which the obliged entity outsourced the customer identification requirement. For a full list of the requirements, please refer to BAFIN Circular 3/2017.

A live video conference session vs. uploading of documents allows certain controls to be applied to detect fraudulent ID documents. Use of an upload copy does not permit so easily the reproduction of holograms, and even the holograms may lose their dynamic dimension. With video, the applicant may be asked to tilt his document horizontally or vertically to allow the trained agent to conduct conformity checks in white light. Another control measure consists of asking the applicant to place a finger over security zone of the document. In this instance, in putting the finger over the identity document, holograms will appear on the fingers of the applicant, hence alerting the trained agent of the presence of a video projection that is attempting to obscure parts of the document. However new demonstrations conducted by the Federal Office for Information Security (BSI) found that in certain cases, putting a finger (s) over the ID document does not expose such attacks. This happens when the fraudster uses a color copy of the identity mean, in addition to an emulation of the secured features of the identification mean.

It is noted that in instances where a genuine identity document has been falsified (e.g. change of photo), a check against authoritative sources may not be sufficient to prevent such frauds, especially if the stolen ID cards are not reported. In such cases, a check may need to be made against the electronic chip of the ID document but such verification methods may imply that banks are legally authorized to read the electronic chip of the ID documents which in jurisdictions, is not possible (e.g. France), and raises issues regarding the future European regulation on electronic ID documents.

#### ii. Document Verification: Validity check

The ID documents presented will be checked against an authoritative source, barring no legal restrictions. A level of eIDAS “High” is likely not attainable as the ID documents are not used in their electronic form (i.e. unable to access and read the electronic chip within ID document).

#### iii. Identity Checks

The identity check of the applicant is conducted via a live video session with the bank personnel or a trained agent. Depending on the legal requirements, certain prescriptive conditions will need to be met at the video conference for it to be compliant (e.g. BAFIN Circular). According to eIDAS regulation, any remote registration of identities will need to be based on more than one identity evidence. To counter identity spoofing, the claimed identity should be informed by more than one channel not specified by the applicant, in order if it is the case to confirm the real claimed identity of the use of his identity. In the case of video conference, the applicant will undergo a series of psychological questioning and observations by trained personnel to ascertain that the identity is as per claimed and that the applicant is present of his own volition (i.e. not under duress). In addition, a TAN will be transmitted either via SMS or email during the live session and the applicant will be asked to enter the TAN (alternative channel).

As iterated throughout the report, it is noted that within Europe, despite a general consensus and a recognition of a need to harmonize regulations in the governance of identity verification methods, at present, there are still varying approaches adopted by Member states. For instance, as a contrast to BAFIN, Estonia’s AML regulations mandates the types of CDD questions that will need to be asked during the live session (e.g. activity profile, purpose and nature of establishment)

The identification stage can reach at least eIDAS Substantial.
--

iv. Anti-Fraud detection

<p><b>Verification of central identification elements</b></p>	<p><b>Physical Address</b> The payment card is mailed to the applicant’s residential address. This ensures that the residential address given belongs to the applicant</p> <p><b>Mobile Device pairing</b> The applicant’s smart phone is paired to the customer account with the pairing code sent via SMS. The confirmation of the information of ownership by the Mobile network owner can be considered, even if this form of identification is not the most robust as other controls (e.g. transfer from a bank)</p> <p><b>Email</b> Validation email is sent to the applicant to confirm that the email provided belongs to the applicant.</p>
---	--

In addition, there are 2 possible fraud risks associated with video conference sessions. One being use of an artificial reproduced video – i.e. spoofing of that person, using thousands of images gathered of that person. Image treatment, algorithms, secured video transmission application, plus the transmission of a TAN during the live session, will largely mitigate the risk. The use of a desktop browser with a secured service network (SSN) to the server for on boarding, rather than via a smartphone application can be a more safe way of on-boarding.

Identification of risks and any mitigating controls

There are risks inherent to any journeys and to a large extent, the BAFIN circular seeks to mitigate some of the risks identified (e.g. customer’s image projected on screen is not real, ID document displayed on the screen by the customer belongs to another similar looking person, ID documents are counterfeited, tampered with).

To a large extent, the risks can be mitigated by technological controls adopted by the providers (e.g. liveness detection) and also trained agents who are able to identify possible suspicious behavior or image inconsistencies. In addition, it is noted that a live video chat session represents a stronger identification mean versus a fully automated video identification (selfie). In the live process, trained personnel can observe the procedure, ask additional questions and data to verify the identity of the customer. They can make a decision during the session as to whether additional measures are needed to identify the customer. While automated processes are usually less expensive to implement and reduce customer’s onboarding time significantly (thus improving the user experience), there are security issues to address. Live solutions offer more control and flexibility to the bank but usually comes with a higher price tag. Another solution could be the use of an automatic process until a certain risk scoring limit/trigger is reached. When that happens, the bank could then propose the applicant to switch to a video interview with a human person.

There is a risk of identity spoofing if the picture on the ID has been tampered with and it could not be detected in the absence of a physical inspection. For Journeys like 3, 3B, 5 and 7 when biometric elements (photo) are not verified against an authoritative source (other than the documents presented through a video/selfie), an additional security measure will probably need to be in place to mitigate such risks. This risk of spoofed picture can be mitigated, by accessing the photograph in the chip (provided it is accessible to banks).



**IDENTIFIED RISK 1: A FAKE OR FALSIFIED DOCUMENT IS USED**

Fake identity document: this risk is decreased with video conference (vs uploaded documents), permitting random controls by turning the document. See also measures contemplated under eID/KYC (sample of id documents, etc.) in methodology part.

A check toward the authoritative source (having issued the ID document) is also required in order to ensure that the document has been issued, and is not lost or stolen, or delivered to a wrong person.

**IDENTIFIED RISK 2: THE IDENTITY DOCUMENT IS PARTLY COVERED WITH A VIDEO PROJECTING CERTAINS PARTS OF THE DOCUMENT**

The measure consisting in asking the applicant to place a finger over security zone of the document, aims to detect this kind of fraud. In this case, in putting the finger over the identity document, the holograms projected by the video will appear on the fingers of the applicant. However according to German BSI, depending on the way the identity document is forged, not all types of fraud can be detected by this mean.

**IDENTIFIED RISK 3: IDENTITY SPOOFING WITH A FALSIFIED IDENTITY DOCUMENT BEARING ON THE PICTURE OR USE OF A COPY OF THE IDENTITY DOCUMENT**

There is a risk of identity spoofing if a picture on an identity evidence (consistent for the other elements) has been modified and that it could not be detected in the absence of physical inspection. Either a real identity document has been falsified, or a copy of a real identity (supposing that the real ID document has not been declared as stolen or lost) is used. Depending on the controls, and the sophistication of the fraud, such frauds could nevertheless exist.

The check against the authoritative source might not prevent from these frauds, supposing that the photo is available. Or a check in an electronic way of an electronic ID document could prevent from this risk (chip request to access the photo inside the chip). Such a verification implies that banks are legally authorized to access the electronic chip of the identity documents (but that risks not to be possible under the future European regulation on electronic ID documents).<sup>44</sup> Note that there could remain residual risks even with this secured process in case of hacking after the chip reading. For Journeys 3 and 3B, 5 and 7 when biometric elements are not verified against an authoritative source (other than the documents shown through a video/selfie) an additional security measure could take place to avoid identity spoofing.

---

<sup>44</sup> For chip access authorization, See:

French regulation Décret 2005-1726, 30 december 2005 (Art 20 and 21):

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000268015&categorieLien=id>

See also European regulation Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (Article 11 § 6):

<https://euroalert.net/oj/80440/regulation-eu-2019-1157-of-the-european-parliament-and-of-the-council-of-20-june-2019-on-strengthening-the-security-of-identity-cards-of-union-citizens-and-of-residence-documents-issued-to-union-citizens-and-their-family-members-exercising-their-right-of-free-movement-text-with-eea-relevance>

**IDENTIFIED RISK 4: THE ID DOCUMENT DISPLAYED ON THE SCREEN BELONGS TO ANOTHER SIMILAR-LOOKING PERSON**

That could also exist in face to face identification with a trained employee, or biometrics could permit to avoid this risk, provided that the two persons do not share similar anthropometric traits.

**IDENTIFIED RISK 5: THE APPEARING PERSON ON THE VIDEO IS NOT THE REAL OWNER OF THE IDENTITY DOCUMENT.**

There are two possible attacks.

1) Either with use of an artificial reproduced video or a video morphing (deep fake). In this case another person is presented than the one who is in face to face. That consists in another presentation of the person, using thousands of images of that person.

Appropriated technical measures must be taken like image treatments and algorithms permitting the detection of this kind of fraud. Use of secured application in order to avoid risks occurring on smartphones is also required (a security default of the application could for instance entail that a virus bore by the smartphone could intercept the video stream coming out the application and send another video stream). Maximum security would be reached when the application is installed on a secure element like a chip (that can be necessary when the application is aimed to be reused for authentication purposes with a high level of confidence). The risk of attack on an application is higher than one of attack on a server when the identification process is determined towards the applicant, by the server. Consequently an identification process could be more secured when a desktop using a browser is used for the on boarding rather than a smartphone. A TLS (or SSL) (Transport Layer Security or Secure Sockets Layer, i.e. a cryptographic protocol (f.i. implemented https) should be used to guarantee authentication and integrity of transactions). Consequently, the analysis and computation need to be made remotely on server based; the smartphone is not considered a trusted device.

The TAN transmitted to the applicant in real time permits the verification of the person's existence. The interaction with a human being also permits the liveness detection by the human person.

2) Or "attacks of physical representation" by made up persons presentations which are more difficult to detect. Real persons are made up to seem similar as the photo of the ID document. The only mean to counter this kind of attacks consists in the use of biometry identification. For the time being biometry allows to counter made up people, 2D masks. Rigid 3D mask cannot be countered. Human is also able to detect this kind of fraud.

**IDENTIFIED RISK 6: USE OF A ROOTED SMARTPHONE**

Rooting is the process of allowing users of smartphones to attain privileged control (known as root access) over various Android subsystems. Rooting is often performed with the goal of overcoming limitations that carriers and hardware manufacturers put on some devices. This might in some cases lead to security breaches. For Android smartphone, safetynet can be used, or any other root detection solution to mitigate the risk.

**Other risks:**

**IDENTIFIED RISK 7: The applicant is duly identified with valid identity document but makes false declarations during the on boarding proceeding**

This risk is not proper to remote on boarding process but could be accrued when the applicant is not seen. This risk is natively limited with an on line video identification ruled by a real person. The person can assess the applicant behavior, and counter-question. The risk could be accrued when the video identification would be ruled by an automatized system, and not a real person for the account of the bank. Another way of mitigation consists in checks of the applicant declarations towards data bases (knowledge basis checks).

### **IDENTIFIED RISK8: ACCRUED RISKS IN CASE OF USE OF “VIDEO IDENTIFICATION” INSTEAD OF “VIDEO CONFERENCE”**

Video conference is a video session between two real persons, an applicant and an operator. Live-online verification and legitimation process includes a banks representative controlling the procedure from the bank’s side and instructing the person to follow guidelines. Technology wise the data is collected much the same way as in automated procedures, but in live process the Banks representative will observe the procedure, ask additional questions and data to verify the identity of the customer. Banks representative will make a decision during the session if any additional verification methods have to be used to identify this client.

Video identification is a video between an applicant and a machine Automated process is where a person receives instructions to follow certain procedure of verification in front of his/her webcam. This process is recorded and collected information will be analyzed and if everything seems to be ok, then the process is approved. No human interaction from the bank side is made during this automated process. The machine has capacities in fraud detection, like liveliness, false. However machine does not have the same capacities as the human being, especially in ruling the interview. Anyway, video identification should be controlled afterwards by a human being.

Luxembourg’s CSSF supervisory guidances <sup>45</sup> makes a difference between the two means. Video conference is preferable. According to Luxembourg CSSF, this kind of online/digital or robo-video-identification, without intervention of a natural person on behalf of the professional, requires the application by the professional of supplementary safeguards in order to mitigate those particular risks linked to the automated character of this kind of identification process. However, a video identification depending on the provider, and using biometrics could reach satisfactory levels.

### **IDENTIFIED RISK 9: MASSIVE FRAUD ATTACKS AND SYSTEMIC RISK**

As far as it is a remote process, massive fraud attacks can occur, with several accounts being opened in the same time by a criminal organization.

Also systemic risk could be considered. This risk occurs can from automatized processes. In such case the reliability of all the transactions realized under such a process could be suspected. There can be:

**Either an integrity issue of automated identity verification:** for example when one of the identifications is found invalid then it raises a major integrity failure with all identifications done via the same process. All the customers identified in such a way, will have to be re-contacted in order to proceed to a new KYC. Beyond that there could be an opportunity attack, for instance in an attorney having found a breach in a process and exploiting this vulnerability to repudiate identification and contracts. That could lead to reputational risks. The question is: how many people does it take to trouble the bank?

### **IDENTIFIED RISK 10: GDPR AND SECURITY RISKS ON PERSONAL DATA**

Photo and video recording, cross verifications in particular toward different data bases decrease the KYC and CDD risks, and permit to ensure the liability of applicant identification and personal situation.

However the more personal data are collected and processed, different sources are consulted the more data breaches risks increase, and in case of not legitimate or not proportionate use, GDPR compliance would not be observed.

At first GDPR, provides with a principle of data minimization. Data processing must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data security is also priority.

---

<sup>45</sup> FAQ AML/CFT and customer on-boarding/KYC methods, CSSF  
Commission de Surveillance du Secteur Financier Version of March the 8th 2018

According to GDPR article 32, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Especially in assessing the appropriate level of security account, in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, non authorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

The choice of KYC process must be closely linked to prior real AML risk assessment pursuant to AML4 directive, and increased use of data must be proportioned, and limited to higher risk factors, or be linked to customer profiles.

#### GENERAL MITIGATION MEASURES TO DECREASE THE RISK ON IDENTIFICATION:

All the mitigation measures must also take into consideration GDPR rules, and in particular principle of minimization of the collected data, being given that electronic identification mean respect GDPR. Risk on data in demanding several identification means and data bases checks.

- Use of a real time video conference in a non-automated way, combined with an automated process in order to assist a human to make a decision.
- A best practice relies on registering of the video. That allows further controls, and proof. Despite not provided by eIDAS, it can be compulsory according some national AML regulations. Nevertheless it will not directly avoid frauds, and have to be proportioned under GDPR.
- Use of a secure application. For high level of reliability, examples will be like ANSSI, CSPN “Certification Security Level One delivered by the French Security Agency.
- The confirmation of the information of ownership by the MNO (telco operator) is also a best practice, even if this identification is weaker as a transfer from a bank (supposing the identification made by another bank).
- Use a desktop using a browser with a secured SSN (TLS) to the server for the on boarding, rather than a smartphone.
- The video identification process can be enhanced with other measures like the invoice and reuse of a TAN.
- Risk detection measures can be applied or additional measures (see under II) in consideration of a risk assessment (like internet traces: IP, mail, to be checked against negative data bases, time logout sessions, multiple attempts, etc.).

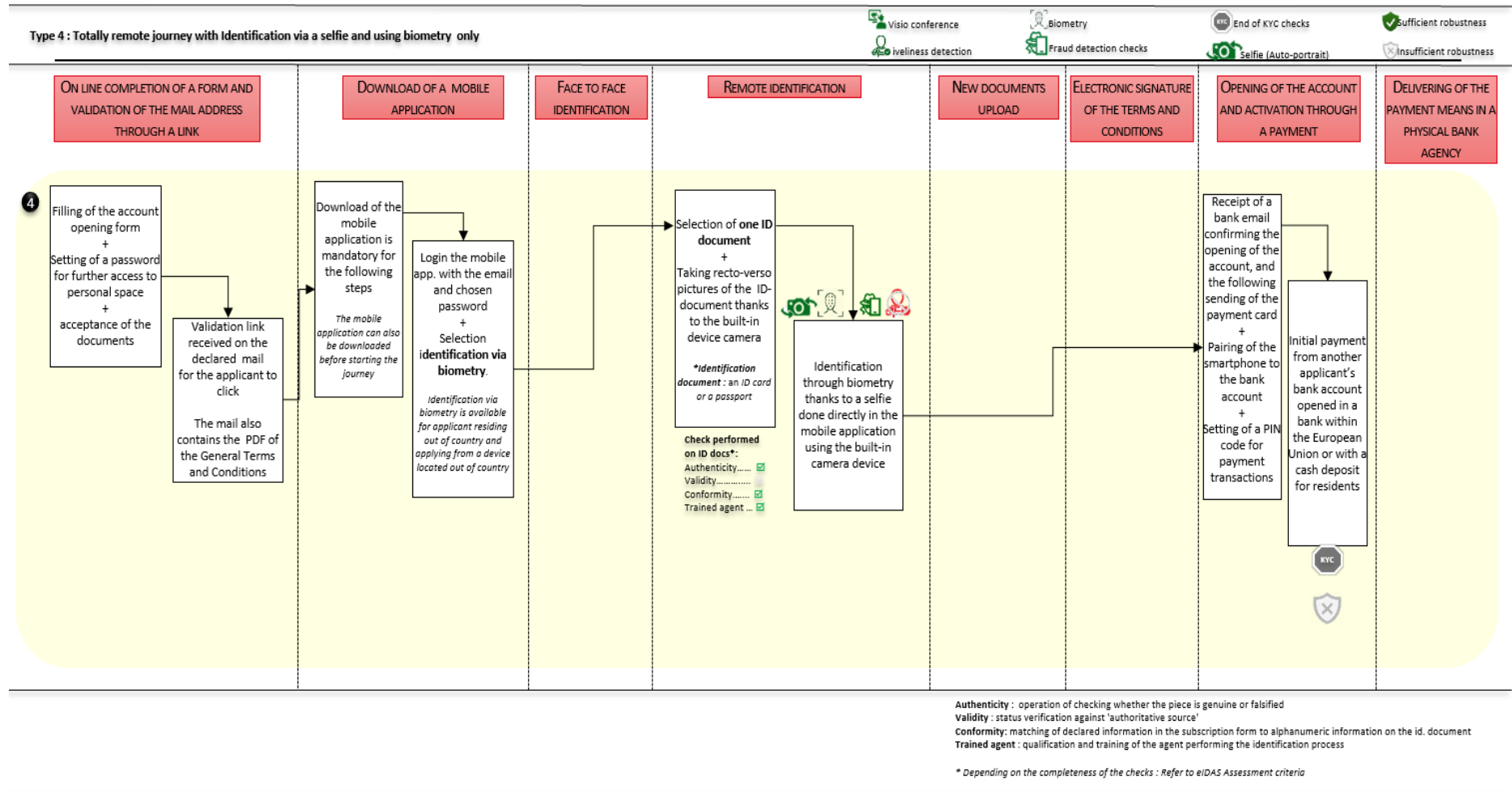
GDPR regulation considers that risk detection enters into the legitimate interest of the data controller (See Recital 6 (“The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.”). 4<sup>th</sup> AML regulation promotes the use of new technologies (Recital (19) “New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.” However all GDPR provisions have to be respected.). As far as other GDPR provisions do not require a customer consent (for instance for sensitive or sophisticated profiling), anti-fraud measures could rely on legitimate interest basis.

- The identification process can be crossed with other data, towards electronic data providers.

- Knowledge based verification processes can be used when applicable/possible as additional proof of evidence. It requires data bases accesses.
- **Counter verification of the identity using an alternative channel (not specified by the applicant) in order to counter identity spoofing:**
  - Contact the physical person (identity owner) by sending a confirmation to that person's residential address or equivalent and credible information of address,
- Check the pivot points given by the customer (welcome letter). Account transfer (through a code invoice like PayPal) required for account activation.

Journey 4: Entirely remote on-boarding journey supported by selfie and biometric identification

Figure 4: Overview of on-boarding process



Journey 4 is broadly similar to that undertaken by Journey 3 with the exception that instead of a video conference with a person, it is replaced by a selfie taken by applicant and augmented with biometric checks (fully automated checks). This type of journey may be offered by some financial institutions to applicants who are residing outside the FI's country of operation.

The main differences between Journey 4 (selfie) and 3 (video conference) are as follows:

- The ID documents are photographed and uploaded, and not presented to a camera under different angles; 2°)
- Applicant has to make a selfie of himself, framing his face. There is only one picture (and not a video). The picture is taken from a single angle: full-facing (i.e. no side profile, no eyes shut or opened, neutral expression)
- The process is automated (no real time with a human person).

#### i. Document Verification: Authentication check

The ID documents are uploaded by the applicant where checks will be applied. The confidence level to be reached via this method is heavily reliant on the technology used to detect fraudulent documents. There have been some reliability issues encountered by this process relating to ID documents checks. Accounts could be opened with false ID documents.

In the event that the authenticity checks on the document did not detect the use of falsified identity document (where the photo has been tampered with), two kinds of controls could be required. The check against authoritative sources may ascertain the photo (subject to the registering of identity photos in a central data base) or the FI can access the electronic chip within the ID document. Such verifications imply that banks are either legally authorized to access the electronic chip of the ID documents (see above on this subject Annex 1 Journey 3) or certain government databases containing photos. Both can be restricted. The case can also be that national database of photos does not exist.

As discussed in Journey 3, the authenticity checks on ID documents during a live video conference with a trained agent permits random controls to be applied and makes it harder for fraudulent documents to be used. However, depending on the verification technologies used, the authenticity evaluation using this journey could reach the authenticity evaluation could reach eIDAS Substantial (High level could not be reached without use of the ID document in its electronic form (reading of the electronic chip).

#### ii. Document Verification: Validity check

If the documents are checked against an authoritative source, the eIDAS level can reach at least Substantial. Depending on the provider used, where the applicant is a non-resident, the checks against national databases will not be applicable, which will lower the level of assurance towards the validity of the documents received. However, there are some third party wide providers (e.g. ARIADNEXT) that are able to access different European registers and provide a greater level of assurance towards the validity of the documents supplied.

#### iii. Identity Checks

A biometric identification (e.g. liveness detection) is made, comparing the applicant's selfie to the ID document photo. In some instances, human intervention or additional checks are imposed for higher risk customers. Depending on the FI, a manual review process of the automated checks may be undertaken by a separate team to mitigate against computer, systemic errors. In certain EU states, e.g. BAFIN and Luxembourg CSSF (Commission de Surveillance du Secteur Financier), this mode of interaction does not constitute video identification and is not sufficiently robust as an identification



means<sup>46</sup>. Furthermore, as the selfie is not dynamic (there is only one selfie and not a video), liveness detection measures which can be ruled with an automated video, do not seem to be possible with a simple selfie (with the only smartphone back camera, without infra-red light, on a static image). Such identification means if employed will need to be supplemented by additional identification measures to mitigate the risks associated with the automated nature of the selfie method.

The eIDAS level could be low level. Depending on the choice of the provider, the use of dynamic selfies<sup>47</sup> (through an automated video, and not a single selfie) should be required permitting the reach of Substantial level (see Journey 3 for Automated processes).

iv. Anti-Fraud detection

<p><b>Verification of central identification elements</b></p>	<p><b>Physical Address</b> The payment card is mailed to the applicant's residential address. This ensures that the residential address given belongs to the applicant</p> <p><b>Mobile Device pairing</b> The applicant's smart phone is paired to the customer account with the pairing code sent via SMS. The confirmation of the information of ownership by the Mobile network owner can be considered, even if this form of identification is not the most robust as other controls (e.g. transfer from a bank)</p> <p><b>Email</b> Validation email is sent to the applicant to confirm that the email provided belongs to the applicant.</p>
---	--

Identification of risks and any mitigating controls

A risk associated with video identification (i.e. "dynamic selfie" and not a unique selfie) vs. video conference is the lack of human intervention and the fully automated process. As noted in Journey 3, video conference with a trained agent allow more random checks to be conducted and human judgment can play an important role in detecting suspicious behavior (although it is acknowledged that humans can be biased and unreliable in performing such tasks as compared to machines). In addition, the fully automated process will carry a greater risk of a systemic failure. For example, should one of the identifications be found invalid, it will call into question the integrity of the entire process that has followed the same identification means. To avoid such systemic failures, banks should have a process/contingency planning in place to handle and reduce such failures when they occur (e.g. "recall"

---

46 Use of selfie does not allow the following checks to be made as opposed to a real time video identification:

- **ID Authenticity checks:** a photo ID uploaded may not bear all the features and holograms. In real time interview, the applicant is asked to flip his identification document (vertically and horizontally) to the camera, to help read the data and holograms, check more easily that the picture is not glued onto the aforesaid document or that the document has not been altered;

- **Identity Check:** a) real time video conference permits to verify that the customer is the same person as the person on the identification document (e.g. consistency check: match the age of the customer with the customer's physical appearance, etc.). b) To listen to the customer reading aloud the identification number on the identification document, or observe the customer using the transmitted TAN. c) Make behavioral & psychological observations d) Conduct an interview permitting to collect information (including CDD information) and to raise complementary questions under a script to make cross verifications regarding the customer declarations.

47 Applicant has to photography himself under different angles, e.g. in profile, face on, eyes opened, eyes shut. This possible liveness detection measure, should permit the avoidance of manipulations on image capture machines or communication networks.

of customers who are verified under the flawed process, using of telephone number for electronic signing of contract).

It is noted that the systemic risk will be exacerbated if the identity verification service is performed by a third party. The integrity issue will be even more widespread if there is a failure on their identification processes that impacts the wider ecosystem and where identities of customers are relied upon previously.

The main cause of concern from a security perspective is the potential loss of system integrity during a failure. For example, looking at the recent high profile cyber breaches, the largest cost arising from the security breaches are the loss in the integrity of data, meaning that all data has to be recollected and verified. This is the biggest risk to any system where the data can no longer be guaranteed authenticity and accuracy<sup>48</sup>.

#### Identification of risks and any mitigating controls

##### **IDENTIFIED RISK 1: THE PERSON ON THE SELFIE IS NOT A LIVING BEING**

The case consists in using a picture of the person to lure the comparison of a person to the photography of the identity document.

There exist providers proposing liveness detection. For this purpose, a “dynamic selfie” is required: a video is used where the applicant has to present under different angles (in profile, face on, eyes opened, eyes shut), or other liveness technics can be used. Biometry should also be used. A secured application is required. In a solution such as the one presented using a static single selfie, liveness detection cannot be made.

##### **IDENTIFIED RISK 2: FALSIFIED IDENTITY DOCUMENT BEARING ON THE PICTURE**

Main risk on such a process would consist in the use of a document forged regarding the identity picture.

A real identity document has been falsified, changing the identity picture into the fraudster’s picture. But fraudsters could be reluctant to give their photos, and could favor other frauds (bearing on identity or using other on boarding means that do not require photos). This fraud could, depending on the controls, and the sophistication of the fraud, such frauds could nevertheless exist.

Authenticity checks on the document itself could permit the detection of a change in the picture. The check against the authoritative source might not prevent from these frauds. It permits to detect whether the document has been issued, and is still currently valid (not lost, stolen or delivered to a wrong person). Only a check of the photo itself against a national register, or in an electronic way of an electronic ID document could totally prevent from the risk consisting in change of picture on the ID document (through a chip request). Such a verification implies that banks are legally authorized to access the electronic chip of the identity documents (not possible in France for the time being, and possibly problematic with the future European regulation).

There is a risk of identity spoofing if a picture on an identity evidence (consistent for the other elements) has been modified and that it could not be detected in the absence of physical inspection. An additional security measure could take place to avoid identity spoofing.

- e.g. payment from a bank account in EU in the name of the applicant

---

<sup>48</sup> Joseph Carson (CISSP, CSPO, ITIL), Cybersecurity Expert in <http://netcorp.ee/blog/2016/03/06/online-identity-verification-in-banking-security-risks-in-automated-and-live-processes/>

- to inform the claimed identity about the current bank account opening. This should take place using an alternative communication method or channel that do not use attributes provided by the applicant: letter to an official address, notification to a previously registered email, phone call. Difficult if the applicant is a non-resident foreigner.

### **IDENTIFIED RISK 3: A FAKE OR FALSIFIED DOCUMENT IS USED**

Fake identity document: That can be made more easily with the simple upload of a copy of the document, than with the exhibition of the document through a video conference. The use of a photocopy of an identity document permits less easily the reproduction of holograms on the transmitted copy, and even the holograms lose their dynamic dimension. On the contrary, a video conference permits random controls by turning the document. Nevertheless and depending on the used algorithms, the ID document checks on the basis of a copy can be reliable.

A check toward the authoritative source (having issued the ID document) is also required in order to ensure that the document has been issued, and is not lost or stolen, or delivered to a wrong person.

### **IDENTIFIED RISK 4: USE OF A COPY OF THE IDENTITY DOCUMENT**

The only detection way to detect the use of a copy of an identity document (the real identity document belonging to another person than the applicant), consists in the use of an electronic identity document in an electronic way.

### **IDENTIFIED RISK 5: THE APPEARING PERSON ON THE PHOTO IS NOT THE REAL OWNER OF THE IDENTITY DOCUMENT.**

There are two possible attacks.

1) Either with use of an artificial reproduced photo (See above RISK 1). 2) Or “attacks of physical representation” of made up persons presentations which are more difficult to detect. The only mean to counter this kind of attacks is the use of biometry identification, Biometry could also permit to fight against the risk of a similar looking person.

The use of a single selfie as identification mean does not require so sophisticated frauds. Liveness detection cannot be made.

### **IDENTIFIED RISK 6: USE OF A ROOTED SMARTPHONE**

Rooting is the process of allowing users of smartphones to attain privileged control (known as root access) over various Android subsystems. Rooting is often performed with the goal of overcoming limitations that carriers and hardware manufacturers put on some devices. This might in some cases lead to security breaches.

### **IDENTIFIED RISK 7: SYSTEMIC RISK**

See above

### **IDENTIFIED RISK 8: GDPR COMPLIANCE**

The requirement to be GDPR compliance (biometry, selfie collected, photo identity document collected). Transmitted data. Further KYC measures.

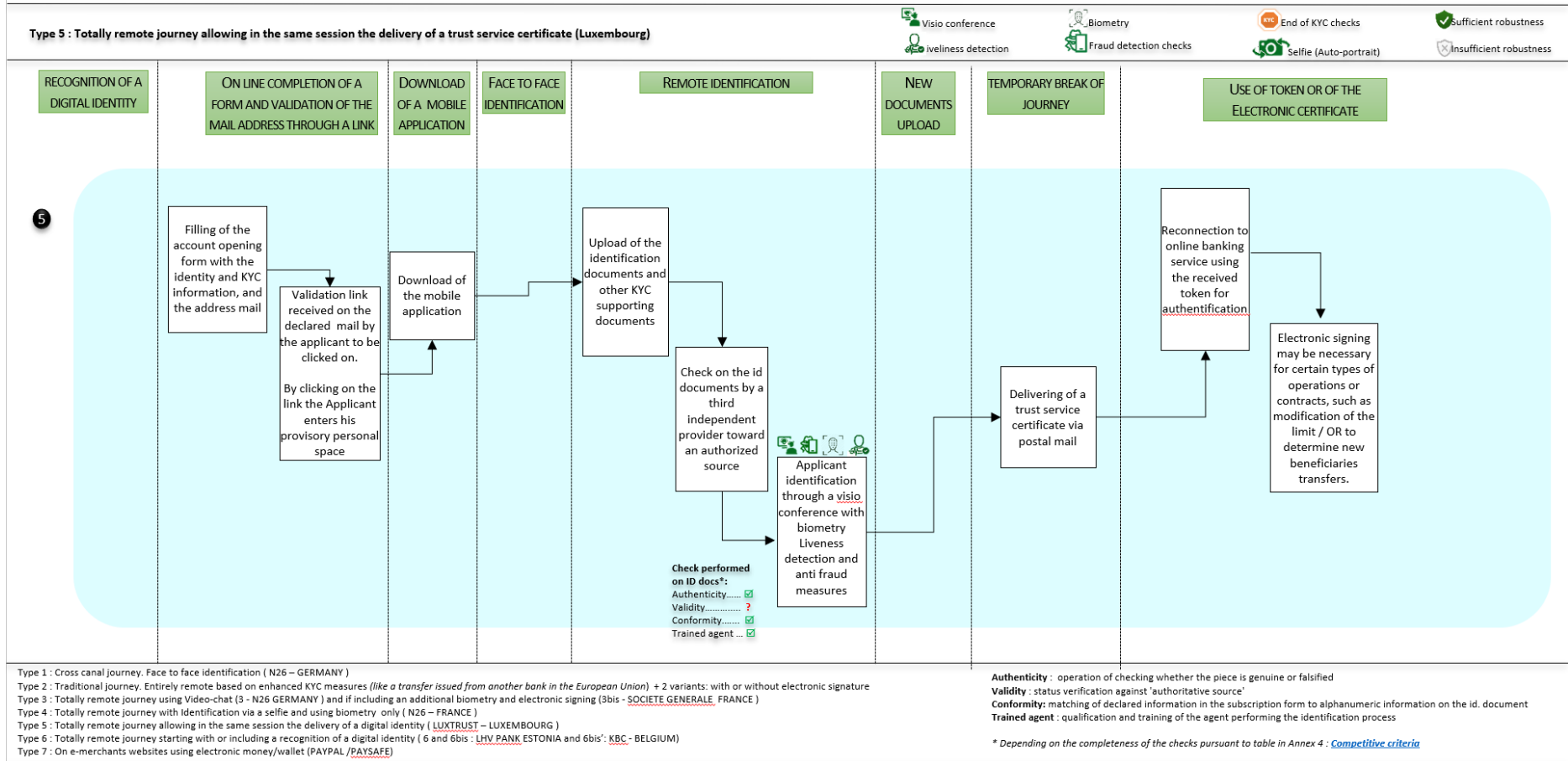
## GENERAL MITIGATION MEASURES TO DECREASE THE RISK ON IDENTIFICATION:

Mitigation measures seem necessary to this solution.


- Use of enhanced KYC measures. Other identification mean must be added to this process.
- Use of a higher technical solution with dynamic selfies (video), and not just a selfie. Ensure high level of liveness detection together with biometry. The liability of the solution also depends on the choice of the provider. The provider must be able to monitor frauds and new kinds of frauds, and to adapt his solution.
- Use of a secured application.
- A best practice relies on registering of the video. That allows further controls, and proof, it can be compulsory according some national AML regulations.
- The identification process can be crossed with other data, towards electronic data providers.
- Knowledge based verification processes can be used when applicable/possible as additional proof of evidence. Thus, the person can for example be asked for his mother's name or his car registration number. This method leads to a scoring. It requires data bases accesses.
- Counter verification of the identity using an alternative channel (not specified by the applicant) in order to counter identity spoofing.

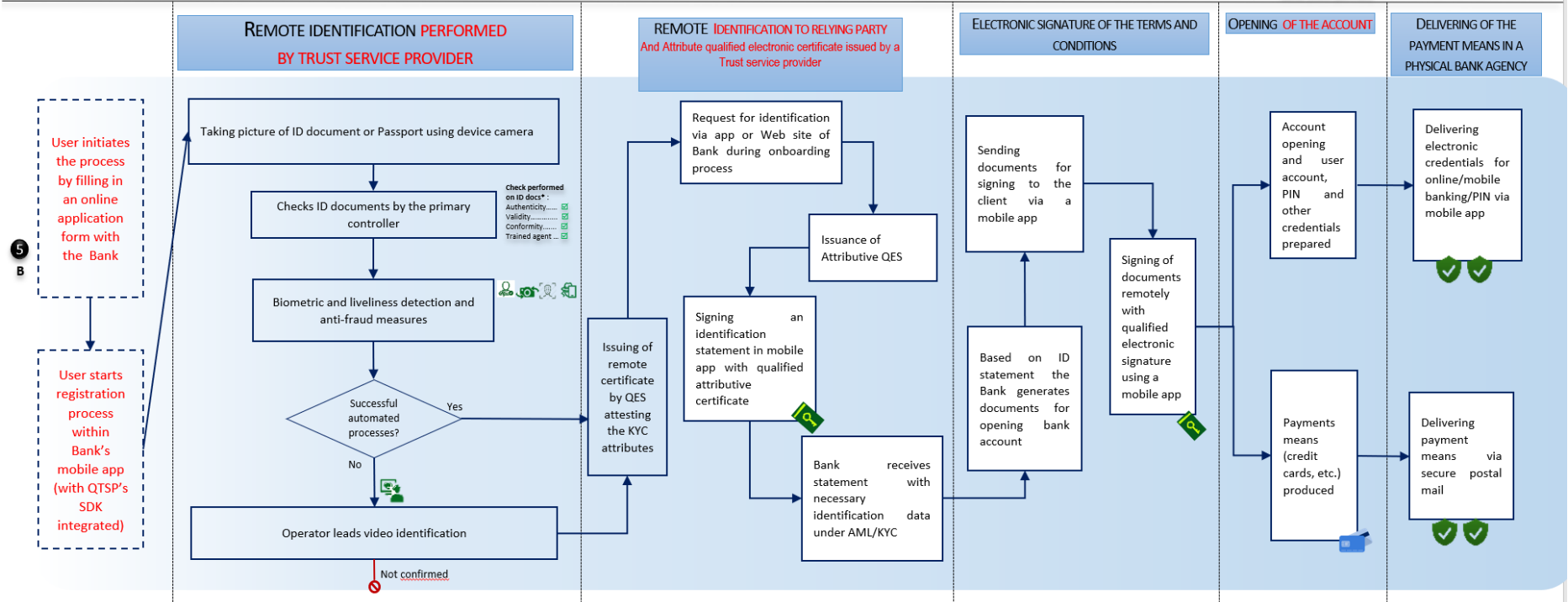
Journey 5: Entirely remote on-boarding journey resulting in a trust service certificate created.

Figure 5: Overview of on-boarding process



Type 5B : Entirely remote on-boarding using a trust service via smart device or on the smartphone for remote electronic signature (Bulgaria)

-  Visio conference  
 livelihood detection
-  Biometry  
 Fraud detection checks
-  End of KYC checks  
 Selfie (Auto-portrait)
-  Sufficient robustness  
 Insufficient robustness



**Authenticity** : operation of checking whether the piece is genuine or falsified  
**Validity** : status verification against authoritative source  
**Conformity**: matching of declared information in the subscription form to alphanumeric information on the id. document  
**Trained agent** : qualification and training of the agent performing the identification process

\* Depending on the completeness of the checks pursuant to table in Annex 4 : *Competitive criteria*

For Journey 5, open source desktop research and feedback from EG members have revealed fewer specific details on the processes as compared to other Journeys where information are more readily available and forthcoming for analysis. This may be due to competition issues, information not disseminated by the providers, or just general limited public information. This type of Journey is also broadly referenced in the PwC report titled “Study on e-ID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU<sup>49</sup>”. This type of journey can be found in one of the major bank based in Luxembourg.

At a high level, the Journey will typically commence with the applicant registering with a valid email which is verified and confirmed with a one-time password. The applicant will upload the requisite ID documents and other relevant KYC supporting documents. In order to capture other applicant identity information, such as the residential address, a commodity bill is considered<sup>50</sup>. For remote identification, the applicant will go through a similar identification process as per Journey 3 (video identification). Once the identification process is completed, successful applicants will be notified and be issued a certificate trust service. The certificate may be mailed to the applicant’s residential address. Once the certificate is established, the applicant will log into the bank’s website and electronically sign the contract with his digital identity credentials.

On boarding journey 5B presents situation in Bulgaria, where two types of certificates are provided by a qualified trust services provider, and used for banking remote on-boarding.

The first one is a certificate issued in the name of the applicant by the qualified trust service provider. This “attribute qualified certificate” bearing a certain number of user personal attributes, is issued remotely “on-the-fly” in real time, and it is used just once by the user to sign his statement for provision of personal data, for identification purpose. At this present moment (when the user signs), the Qualified Trust Service Provider (QTSP) can check real-time that the user is alive, and his attributes are valid. Thus, attributes are declared by the user in a special statement for provision of personal data compliant with GDPR through a qualified e-signature supported by a QTSP qualified attribute certificate. This certificate itself (and not only the signed statement) holds more personal attributes as a normal certificate, i.e. those required for KYC.

Regarding the attributes, the scope of the KYC checks normally depends on the type of client and level of risks, subject to the financial institution’s policy. Part of the information is provided in the course of the e-identification. The current scope may encompass names, date of birth, citizenship, address, number of ID document, date of issue and date of expiry, country of issue, type of the document, and national ID number where available. However, the QTSP service goes beyond attestation of physical identity of the natural person: it is designed in a way that may provide further data covering basic and also advanced identity attributes, like profession (i.e. lawyer), education (i.e. MBA degree), health status (i.e. blood type), geolocation, whether the user is listed as a terrorist, whether he/she is a good taxpayer, criminal record, credit history, etc. The system makes possible e-identification not only of natural persons, but also of legal persons (QTSP is integrated with more than 80 commercial registers worldwide). Some of the data cannot be automatically collected from primary registers or sources and are subject to user declaration (for example source of funds, PeP status, etc.). These data are only self-declared by the user by electronically signed documents (statements for self-declaring circumstances), and are not attested by the qualified certificate. All this is possible with one-click straight from the mobile device.

The qualified trust service provided by the QTSP in Bulgaria is linked to primary databases - national ID document register and the national citizenship register, while the remote video identification is considered to be equal to a face to face identification. Where integration with national ID documents

---

49 PriceWaterHouseCooopers report “Study on e-ID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU”, Page 112, Annex V SAMPLE OF EMERGING DIGITAL SOLUTIONS, SP2

<sup>50</sup> In Luxembourg, on the contrary to Belgium ID card, the address is carried in the electronic ID card chip, but is not available to the private sector.



register is not available, the ID document data is retrieved through NFC from the mobile phone. Since the qualified certificate is issued upon real-time checking of the status of the person and the personal attributes, the declared identity is considered highly reliable, reaching level of assurance “high”. In a similar manner to solution 5, the issuing of the attribute qualified certificate is made through remote video-identification. But QTSP solution is automated and is certified as having the same level of assurance as to a physical presence under eIDAS Art. 24 (1) (d). Thus, the identification for issuing the qualified attribute certificate and the identity attestation and done for less than a minute in a completely automated regime.

The considered method for identification is completely new, and from a legal point of view it does not rely on the technologies used (video identification, 3D liveness, etc.), but on an eIDAS trust service provided by a qualified trust service provider through the issuing of a qualified certificate, relying on the consultation of national registers, and a remote biometric identification. The certificate bears more identification attributes as normal certificates. This method for e-identification is explicitly regulated as meeting the AML requirements under Art. 13 (1) of the 5th AMLD. It seems that no other such solution is provided in Europe.

As an advantage, eIDAS rules regarding responsibilities and mutual recognition apply to such an identification through a qualified certificate.

This method is more favorable to banks, than direct use of video identification apart from a trust service. If a bank only uses video identification (with 3D liveness, etc.), it relies on the technology, and the risk of wrong identification remains on the bank. The legality and the AML/KYC compliance in using this method also depends on the national AML/banking authorities. On the other side, if the bank identifies the client through a trust service (qualified certificates with more attributes), the bank relies on a regulated trust service, ruled by eIDAS. The risk of wrong identification rests with the trust service provider by law. The method explained is thus equally legal in all EU member states.

The two scenarios for on-boarding might seem to be similar, but the methods employed would completely differ from each other in their legal consequences.

As explained above, for on-boarding purposes are issued two qualified certificates. The first one is used for identification, when the second one is used by the applicant for signing of e-documents (bank contracts, GTC, PeP declarations, etc.). It is a normal qualified certificate with two years validity, but also issued and used remotely. Thus, for electronic signing of bank documentation, the applicant uses his qualified signature from his mobile, while his certificate and the qualified signature are created remotely in an HSM (certified for remote signing). Normally the solution for signing and e-identification is embedded as an SDK into the bank application, but it can be used as a standalone application separate from the banking application.

This solution is used by most Bulgarian banks.

## Document Verification: Authenticity and Validity check

Depending on the document checks involved, e.g. accessing national databases, the eIDAS level of assurance regarding ID documents checks can reach at least Substantial.

### i. Identity Checks

The identity checks will be conducted via video conference with a trained agent. This may be conducted by the financial institution or via a trained third party. Depending on how the video conference is being conducted and the local regulations governing how the video conference should be conducted (e.g. Luxembourg Bank Authority (CSSF) published strict guidelines on how video identification should be conducted), we can assume that the checks can reach an eIDAS LoA of at least Substantial.

## Identification of risks and any mitigating controls

Refer to risks identified for Journeys 3 and 3B.

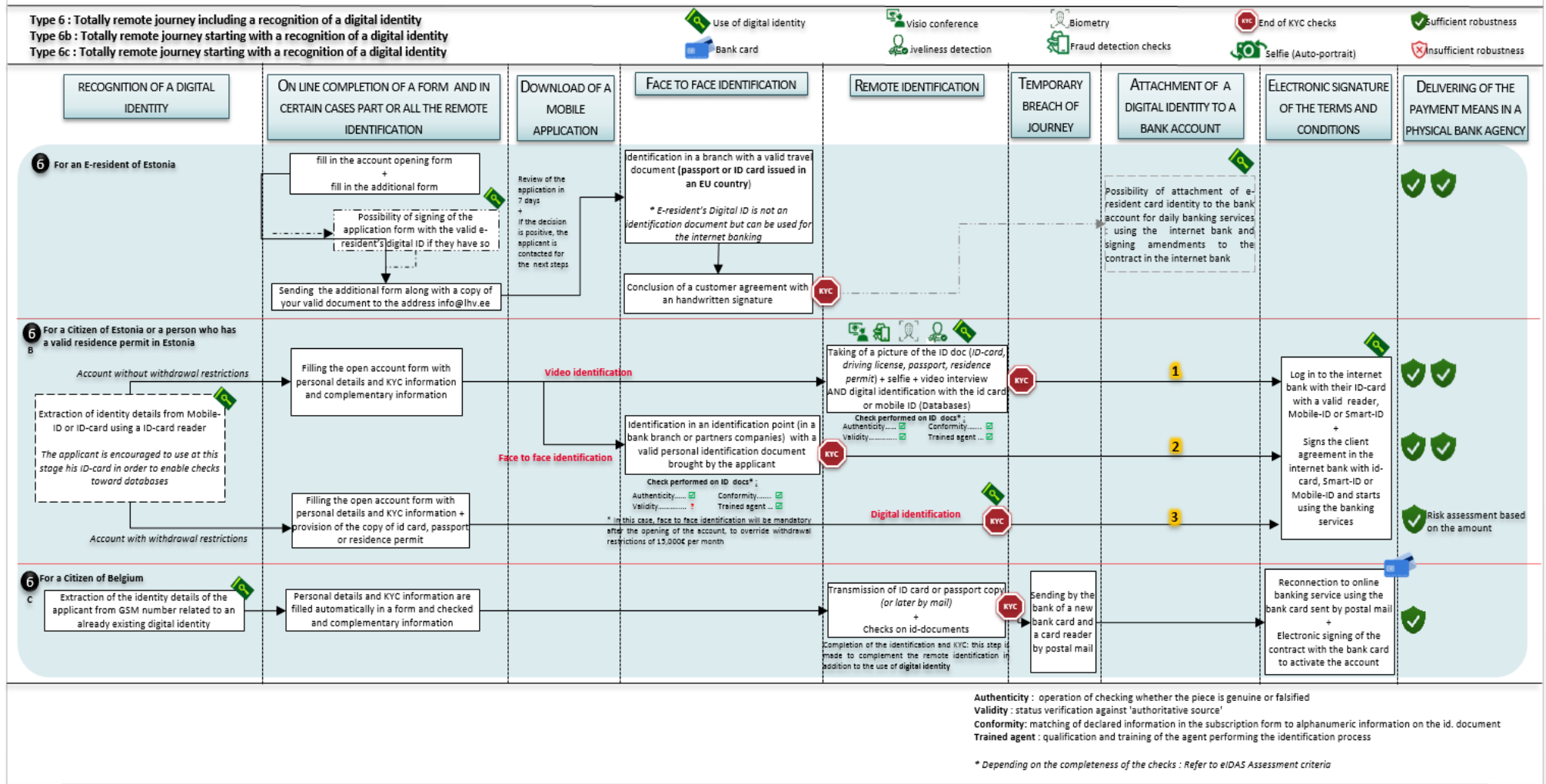
Specificities of on-boarding Journey 5 rely on:

The way the national ID is used: the Luxembourg eID bears one chip. Functionalities of this chip include identification, authentication and electronic signature. Authentication and electronic signatures are a common opt-in choice of the citizen, while the first functionality is mandatory. Hence, the identification level could be different, according to the way the ID card is used.

Regarding trust services or electronic identification means that could be delivered and sent to the applicant after the journey, leveraging on the identification made during the onboarding, reliability for further use of these means also rely on the trust in their delivering to the right person .Hence, if delivering is made by postal way, postal address should have been verified.

Journey 6: Entirely remote journey using digital identity

Figure 6: Overview of on-boarding process



Journeys 6 focus on the use of digital identity as the main mode of remote identification. For our analysis, we have benchmarked the bank journeys undertaken in Estonia and Belgium. Estonia has “Notified” eID status with the European Commission and using digital identity for remote on-boarding is common practice among the financial institutions. Belgium banks uses an electronic identification mean which can be derived from the national ID card, and is currently being notified level High.

In the case of Bank A in Estonia, the journeys are offered to citizens with ID card or residents physically based in Estonia. A separate journey is available for e-residents of Estonia. Additional verification would be made on the national identity document (including the data) and against the information originating from a credible and independent source.

In Journey 6B, regarding Citizens of Estonia or persons having a valid residence permit in Estonia, the on-boarding process generally begins with the automatic extraction of identity details from the mobile ID or ID card using an ID card reader, means the applicants are encouraged to use for automatic checks. They also permit an automatic filling of the application form which is completed manually with other necessary information. The identity information is verified and validated against central database/revocation lists. Once the checks have been performed, KYC can be considered to be performed. The customer can then activate the bank account by electronically signing the agreement with his ID card (using a card reader) or mobile ID credentials.

For Journey 6B (citizens and resident permit owners), an account can be opened remotely on the basis of the digital identity and supporting documents submitted without any remote/face to face identification taking place but the account will be subject to restrictions per Estonian AML regulation. Regulation dictates that the total sum of outgoing payments relating to a transaction or a service contract does not exceed 15 000 euros per calendar month. In this case, either a face to face identification will be mandatory after the opening of the account, to override withdrawal restrictions of €15,000 per month , or a video identification complete with identifications checks must be made during the on boarding journey in addition to the digital identification with the electronic identification mean (Journey 6B). In such a process the electronic identification mean is used at several stages: 1) the electronic identification mean may be used for electronically filling in the requisite data. The applicant is recommended to use it at this stage, so that checks towards data bases can be made. 2) It is used by the applicant for the digital identification towards the provider proceeding to the video identification. 3) It is used for digital signing of the acceptance and declaration regarding the remote identification process using video, on the provider platform or this approval is made with the general terms and conditions and finally 4) it is used on the internet bank platform to sign the general terms and conditions.

The additional identification to electronic ID can also take place in face to face (bank agency or partners), on the basis of a valid personal identification document brought by the applicant. This last solution (6B) constitutes another type of cross channel journey (refer on boarding Journey 1 for other cross channel journeys). Cross channel journey is compulsory in case of E-resident (Journey 6), who do not have access to the entire remote on line journey. After beginning the journey on line, they are required to go to a bank agency for a face to face identification. At the beginning of the journey, they can sign an application form with valid e-resident’s digital ID. There is also a possible attachment of the e-resident card identity to the bank account for daily banking services using the internet bank and signing amendments to the contract in the internet bank. Consequently, use of E-resident electronic identity is restricted despite its level High under eIDAS.

In the case of Journey 6B, there are strong parallels to be drawn to Journeys 3 and 3B.

For Bank B in Belgium (Journey 6C), an account can be opened remotely with the applicant’s digital identity I. Additional documents (e.g. transmitted ID card or passport) will need to be provided by mail whereupon authentication and verification checks will be conducted on the documents. Successful applicants will be posted their bank card to their residential address for activation. The applicant will

electronically sign the bank's terms and conditions using the bank card that he receives over the post, and in doing so, confirming the physical address.

As a comparison to Estonia, Belgium's AML regulations are less prescriptive on remote on-boarding channels and instead follow a risk-based approach. Annex III of the Belgium AML Regulation indicates that the use of remote on-boarding channel should serve as an indicator of a higher risk customer and that particular attention should be given to the verification of the identity of the customer (e.g. to access the Belgium national registry to carry out additional identity verifications). To further illustrate the varying approaches and level of prescriptiveness adopted by different EU regulations, France's AML regulation stipulates that for eID schemes with LoA at Substantial, additional identification means will need to be performed. This may, among other measures, be in the form of additional identity document requested or a bank transfer from another account opened to the customer in the EU.

- i. Document Verification: Authenticity and Validity checks
- ii. Identity check of the applicant

As far as electronic identities are used, several key phases are conducted concurrently, i.e. authenticity and validity check of documents, identity check of the applicant. These steps are borne by the electronic identification mean and have already been made as precondition or condition to the delivery of the electronic identification mean. The bank shall only verify the validity of the id mean (as for acceptance of electronic certificates; that the certificate has not been revoked)).

As the banks rely predominantly on the pre-approved digital identities submitted by the applicants, the authentication and validity checks on the requisite ID documents and to a certain extent, identity checks of the applicant is assumed to have been conducted to a level of assurance that is acceptable. The level of identification is defined in 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.

Recital (15) of the eIDAS regulation stipulates that the obligation to recognize electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognize electronic identification means having lower identity assurance levels. However, it should be noted that for eIDAS Low level of assurance, it is deemed not robust and reliable enough for FI's on-boarding purposes. The use of electronic identities lower than High is possible if it is supplemented with additional identification measures. A risk analysis has to be determined by the FI whether to accept the electronic identity as the only means of identification or whether it needs to be supplemented with additional checks (e.g. supply of another ID document, Knowledge based verification).

In certain jurisdictions, the law is prescriptive on such matters. For example, in France, AML regulations dictates that the use of a notified substantial electronic identification mean has to be completed with another KYC measure among which include 1) an identity document and a further document proving the identity; 2) a verification and certification of the copy of the identity document or register from a third independent from the person who is to be identified; 3) a credit or debit wire transfer from or to an account opened to the customer in the European Union; 4) an identity certification issued from another bank; 5) a substantial level eIDAS electronic identity; 6) a qualified eIDAS signature or an advanced signature relying on a qualified eIDAS certificate.

For the case of Estonia, the eIDAS level of assurance of such digital identities are at a High level. For the case of Belgium, the particular digital identity scheme that Bank B is using has yet to be notified to the EU but based on its identification checks, it can reach Substantial/High. At present, Bank B requires a further identification step in addition to the digital identity, a copy of an identity document (i.e. identity card/passport) for authentication and verification.

On the other hand, it is interesting to note that in the case of Journey 6, as a pre-condition, e-residents

will apply with their electronic identity that is assured at a level High. They will also need to present a copy of their identity document in order to compare the applicant to his ID document photo during the face to face identification. This may appear excessive and onerous on the applicant as in order to be granted an e-resident card, applicants will already need to be identified face to face in their consulate.

The identification level for the described Estonian journeys reach Level High. From a general point of view, the identification level corresponds to the level of the electronic identification mean. A process consisting in the combination of electronic identification Level Substantial with other measures can also reach Level High.

### iii. Anti-Fraud detection

As one of the anti-fraud measures, electronic identification providers can monitor (as far as it is permissible under local laws), the relevance of certain data, e.g. the beneficiary's website, the localization of the electronic identification mean. This process will imply that an approval from the electronic identification mean owner, also a partnership between the TELCO operator and the provider of the electronic identification mean. In particular, this will be relevant to electronic identities delivered by, or in involving TELCO operators. The use of SIM chip as a secure element can facilitate the monitoring of such data. However, it is noted that this can be subject to cyber-attacks (e.g. rootage of the device<sup>51</sup>).

As an illustration of an IT security flaw, in Estonia, in October 2017, a cryptographic flaw was uncovered in the smartcard technology that affected 760,000 Estonian national ID cards. The security flaw will enable criminals to exploit the flaw and allow them to clone the cards and commit identity fraud<sup>52</sup>. As a precautionary measure, the Estonian Prime Minister announced the temporary disablement of the certificates of affected IDs until the security fix is done. Even though no confirmed fraud was reported, this incident demonstrates that no system is foolproof and there is always a risk of technological failure and it is important to have additional measures to mitigate risks.

#### Identification of risks and any mitigating controls

#### **RISK 1: The electronic identification mean is transferred and used by another people as the owner**

The case may be: the applicant has given his electronic identification mean together with the pin code to another person. Frauds are committed under the responsibility of the applicant. That is quite comparable to the next,

This fraud is similar to other ones:

- the applicant launders money for the account of another people. That also exist in physical word without use of digital identities, or
- the applicant is forced in the use of its electronic identification means. That is quite improbable due to this length of an onboarding journey, availability of the account, and the fact that the account should also be first provisioned.

These risks are inherent to remote situations, as far as the person is not seen. But risks have also existed in face to face on boarding. And even a cross channel journey, requiring a face to face

---

<sup>51</sup> Rooting is the process of allowing users of smartphones to attain privileged control (known as root access) over various Android subsystems. Rooting is often performed with the goal of overcoming limitations that carriers and hardware manufacturers put on some devices. This might in some cases lead to security breaches.

<sup>52</sup> <https://www.v3.co.uk/v3-uk/news/3020479/estonian-authorities-block-national-id-cards-due-to-flaw>

identification does not prevent against money laundering for the benefit of another one (it would just prevent from the risk of use by another user than the owner of the digital identification mean).

### MITIGATION MEASURES TO RISK 1

All the mitigation measures must also take into consideration GDPR rules in particular principle of minimization of the collected data, being given that electronic identification mean fulfills GDPR minimization principle. Risk on data increases in demanding several identification means and resorting to multiple data bases checks. This risk also exists in requiring copies of the ID documents (during the transmission to the bank, the storage by the bank, and on the applicant desktop or device where the ID document copy will remain). See works Sub Group 2 relating to eIDAS attributes for KYC, in regard to this minimization principle.

Without prejudice to GDPR rules, several mitigating controls can be considered:

- Risk detection measures can be applied or additional measures (see under II) in consideration of a risk assessment.

GDPR regulation considers that risk detection enters into the legitimate interest of the data controller (See Recital 6 (“The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.”). 4<sup>th</sup> AML regulation promotes the use of new technologies (Recital (19) “New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.”).

- The authentication process can be crossed checked with other data.

The electronic identification means providers can also monitor (as far as permitted by the national nodes), the relevance of a certain number of data, such as the beneficiary website, the localization of the electronic identification mean.

Note that this process could require, under GDPR rules, an approval of the electronic identification mean owner, and also a partnership between the TELCO operator and the provider of electronic identification mean.

That could in particular be made for electronic identities delivered by, or involving TELCO operators. Thus, the use of SIM cheap as secure element, on the mobile bearing the digital identity could permit to monitor such data.

Case of Estonia: A mobile ID is proposed. This mobile ID is derived from the ID card and uses the TELCO SIM. Using a mobile ID permits collection of Telco data in real time. SIM is also a secure element (i.e. a security zone like a cheap, which is not reproducible). The TELCO also uses its own network, and ensures that the applicant is located in Estonia. **However, this security can be attacked by a rootage of the device. That will imply anti rootage measures.**

- Knowledge based verification can be used when applicable/possible as additional proof of evidence.

Thus the person can for example be asked for his mother’s name or his car registration number. This method leads to a scoring. It requires that such data bases exist and are accessible. That is made for example by the UK Government solution UK verify, comparing the declaration to governmental data basis (considered as reliable sources). The applicant’s declarations are so checked.

The identity is reached by scoring with a very high confidence rate. In this solution the English government has opened all his data bases to a certain number of Identity providers. These checks leading to a score consist of establishes the candidate’s identity by cross referencing personal information against a variety of sources. Electoral Roll, Telephone directory, Credit accounts (eg. bank



accounts, credit cards, loan accounts etc.), Court and insolvency records, CIFAS fraud database, Deceased register).

**RISK 2 Another person uses the electronic identity unbeknownst to the owner. The electronic identification mean is used outside the owner control (whatever the level of the electronic identification mean). The Electronic identification mean is not sufficient by itself or its level is not sufficient**

This case occurred in Estonia regarding the electronic ID cards (in theory Level High) which encountered ROCA security problem. Even if no confirmed fraud occurred, the electronic identification means were suspended until the security breach correction<sup>53</sup>.

**MITIGATION MEASURES TO RISK 2**

A risk analysis has to be made upstream in order to determine whether a digital identity is or is not sufficient, and for which level. Normally an electronic identity level High should be sufficient. Further due diligences may also be required to collect further attributes that those driven by the electronic identification mean. For instance Estonian AML regulation considers that an electronic identification level High is not sufficient for non-citizens, and in some cases (regarding the amount of the account).

Then where needed, mitigation measures can consist in the following:

- **An enhanced level can be demanded;**
- **Complementary measures can be foreseen.** That can consist in the collection of further documents and information, or in proceeding to further verification.

For instance, French AML regulation lists the different possible complementary measures (one is needed **in addition to a notified electronic mean level substantial**): 1°) an identity document and a further document proving the identity; 2°) a verification and certification of the copy of the identity document or register from a third independent from the person who is to be identified; these checks are made by a quality technical third party verifying the identity documents as foreseen for other typical on boarding journeys (See typical on boarding journeys from 1 to 5 that do not use electronic identification means). 3°) a credit or debit wire transfer from or to an account opened to the customer in the European Union; that is a way to verify the identity on relying on another bank having already identified the applicant. 4°) an identity certification issued from another bank; 5°) a qualified eIDAS signature or an advanced signature relying on a qualified eIDAS certificate;

- **Additional information technology means can be used.**
- **The use of video identification** which can be regulated by the national AML, Finance or Supervisory authorities, under technical as well as process criteria.

See Typical On boarding journey 3 regarding the technical conditions for use of video identification, under **BAFIN** circular and **Estonian Finance Ministry regulation**. See also the aforesaid **Luxembourg's CSSF<sup>54</sup> supervisory guidances regarding video conference and video identification**.

What has to be pointed out is the fact that in Estonian AML regulation the use of information technology means apply to E-resident or person from a country outside the European Economic Area, or for finance risked operation in consideration to the involved amounts. In these cases, the identification based on the national identity document has to be made in addition to an electronic identification with an electronic identification Level High. That means that the applicants actually have to use their electronic

<sup>53</sup> Refer to ZDNET: <https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/> (Accessed on 26 April 2019)

<sup>54</sup> CSSF : Commission de Surveillance du Secteur Financier (Luxembourg)

identification mean Level High as precondition. The technical regulation provides that the applicant has to sign the acceptance on the use of the information technology mean, with his digital signature. The copy of the national identity document is also used in order to compare the applicant to his ID document picture. That could be considered as over-quality if it was not supported by a prior and relevant risk assessment.

- **The verification of the identity documents:** the more secured way (reaching High level) to ensure the comparison between the applicant and his identity document, is to use an electronic way to ensure the comparison is made with the picture included in the cheap of the ID document, or to compare it to a national register containing the picture. Furthermore, the use of an identity document in an electronic way insures that the applicant is using the original of the identity document and not a copy. This electronic way of checking the authenticity of the identification document, depends on the identity documents, and the authorized persons to use them in an electronic way. Banks may be not allowed to it. It raises issues regarding the future European regulation on electronic ID documents.

- **Additional information collect and checks.**

- Knowledge based verification processes can be used when applicable/possible as additional proof of evidence with comparison towards data bases.
- Information is checked against several registers, or Commercial Electronic Databases
- **Further verification can be made using an alternative channel to test the information provided by the applicant.**

Thus in the Belgian KBC journey, signature of the general conditions is not fulfilled with the electronic identification mean, despite the fact it bears a signature certificate and has been used for the digital identification of the applicant. The credit card that has been sent to the Applicant is used for the purpose of the signature. That allows to test the physical address. That signature is a precedent condition to the account activation.

- **Counter verification of the identity using an alternative channel (not specified by the applicant) in order to counter identity spoofing:**

Contact the physical person by sending a confirmation to that person´s residential address or equivalent and credible information of address, or make sure that the person sends a certified copy of identification, or by other equivalent means. (Sweden).

**IDENTIFY THE PERSON DIGITALLY AND CASES WHERE AN ADDITIONAL VERIFY DATA WITH THE HELP OF INFORMATION TECHNOLOGY MEANS UNDER ESTONIAN REGULATION**

Considered people and applicable regulation	Conditions leading to the use of information technology means	Identification mean (electronic and other identification means required)	Use of the identification mean	Conditions (including technical) applicable to the provider for the video interview)  <i>(Minister of Finance regulation on Requirements and procedure for identification of persons and verification of persons' identity with information technology means)</i>
<p><b>CASE 1:</b></p> <p>Person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country (<u>eIDAS regulation</u>)</p> <p>[PROVIDED THAT</p> <p>Total sum of outgoing payments relating to a transaction or a service contract does not exceed 15 000 euros per calendar month nor, in the case of a customer who is a legal person, 25 000</p>		<p>A document issued by the Republic of Estonia for digital identification of a person</p> <p>OR</p> <p>another electronic identification system with assurance level 'high' which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC</p>	<p>DIGITAL IDENTIFICATION WITH THE ELECTRONIC IDENTIFICATION MEAN</p> <p>AND</p> <p>COPY OF THE NATIONAL IDENTIFICATION DOCUMENT for foreign national.</p> <p><u>(Estonian Identity Act and coherence reading with AML regulation regarding the other cases where identification of the person and verify data with the help of the information technology means is required)</u> Nevertheless, Estonian Identity Act stipulates that the photography</p>	<p>NOT APPLICABLE</p>

<p>euros per calendar month.</p> <p><u>(A contrario reading of the AML regulation)]</u></p>		<p><u>(eIDAS regulation and Estonian Identity Act.</u></p> <p><u>Estonian AML regulation does not foresee this general case nor any identification level regarding this, on the contrary to France where substantial level can be used if completed with other identification means)</u></p>	<p>enables unequivocal verification of the identity of the holder of the document and copy of national ID card are demanded in journeys regarding citizens.</p>	
<p><b>CASE 2:</b></p> <p>Person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country</p>	<p>Due diligence measures are not applied while being physically in the same place as the person or their representative.</p> <p>AND</p> <p>Total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month.</p> <p><u>(AML regulation)</u></p> <p><u>(AML regulation)</u></p>	<p>A) A document issued by the Republic of Estonia for digital identification of a person</p> <p>OR</p> <p>another electronic identification system with assurance level 'high' which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114) is used for identification of a person and verification of data with the help of</p>	<p>DIGITAL IDENTIFICATION WITH THE ELECTRONIC MEAN</p> <p>AND</p> <p>COPY OF THE NATIONAL IDENTIFICATION DOCUMENT for foreign national.</p> <p>Additionally, information originating from a credible and independent source is used for identifying a person and verifying data. To identify an e-resident and verify data, a credit institution and a financial institution has the right to use personal identification data entered in the database of identity documents.</p>	<p>1) DIGITAL IDENTIFICATION:</p> <p><u>The information system of the service must allow for digital identification of a person and digital signing.</u></p> <p>The applicant must use a document prescribed for the digital identification of a person issued pursuant to the Identity Documents Act (NB: this provision is in contradiction with the AML regulation authorizing the use of European notified identification means. Identity Documents Act does has not been modified to take into consideration the eIDAS regulation).</p> <p>Pursuant to Identity Document Act, a document prescribed for digital identification of a person is a document prescribed for identification of a person and verification of identity in an electronic environment. It bears information which</p>

		<p>information technology means.</p> <p>AND IN ADDITION TO A)</p> <p>B) Where a person is a foreign national, the identity document issued by the competent authority of the foreign country.</p> <p><u>(AML regulation)</u></p>	<p><u>(AML regulation)</u></p>	<p>enables identification of a person digitally, including a cryptographic key enabling digital identification and the respective certificate, and information which enables digital signing, including a cryptographic key enabling digital signing and the respective certificate, and other digital data may be entered in a document.</p> <p>Upon the above identification of a person and verification of person's identity the service provider may use information technology means that have the hardware and software required for the digital identification of biometric data.</p> <p><u>The applicant identifies himself when entering the information system specified by the service provider.</u></p> <p>The applicant confirms <b><u>with his or her digital signature</u></b> upon the establishment of a business relationship his agreement to the use of the video identification and makes declarations on the truth of the data provided by him.</p> <p><b><u>In addition an applicant who uses the e-resident's digital identity card must also:</u></b></p> <p><b><u>1) agree with the application of Estonian law by confirming this with his or her digital signature;</u></b></p> <p><b><u>2) show to the service provider in front of the</u></b></p>
--	--	--	--------------------------------	---

			<p>camera the personal data page of the valid travel document issued by the foreign country.</p> <p>AND IN ADDITION TO THE DIGITAL IDENTIFICATION:</p> <p>2) VIDEO IDENTIFICATION:</p> <p>The provider uses highly reliable technical means, which guarantee truthful identification of a person and make it possible to prevent the alteration or misuse of the forwarded data.</p> <p>The service provider must check whether the information system guarantees the transmission of clear, quality, recordable and reproducible synchronised sound and image, which is sufficient to understand the transmitted content unambiguously and reliably.</p> <p><b>Consideration of an unsuccessful identification of a person and verification of person's identity if:</b></p> <p>(1) 1) the applicant has intentionally submitted data that do not correspond to the identification data entered in the identity documents database or do not coincide with the information or data obtained with other procedures;</p> <p>2) the session expires during the identification of a person, the identification questionnaire or the</p>
--	--	--	--

			<p>interview, or the information flow that transmits synchronised sound and image does not comply with the requirements set out in § 5;</p> <p>3) the natural person or the legal representative of a legal entity has not given the confirmations stipulated in subsections 2 (4) to (6);</p> <p>4) the natural person or the legal representative of a legal entity refuses to comply with the service provider's instructions specified in § 7;</p> <p>5) the natural person or the legal representative of a legal entity uses the assistance of another person without the service provider's permission;</p> <p>6) there are circumstances that give rise to suspicions of money laundering or terrorist financing.</p> <p>(2) The session specified in clause 2) expires when the applicant has not completed any activities in the service provider's information system during a period of 15 minutes.</p> <p>(3) In the event of the circumstances set out in clauses 1) to 6) the service provider rejects the application of the natural person or the legal representative of a legal entity for opening an account or conclusion of a transaction.</p> <p>(4) In the event of the circumstances set out in clauses 1) and 6) the service provider sends a</p>
--	--	--	---



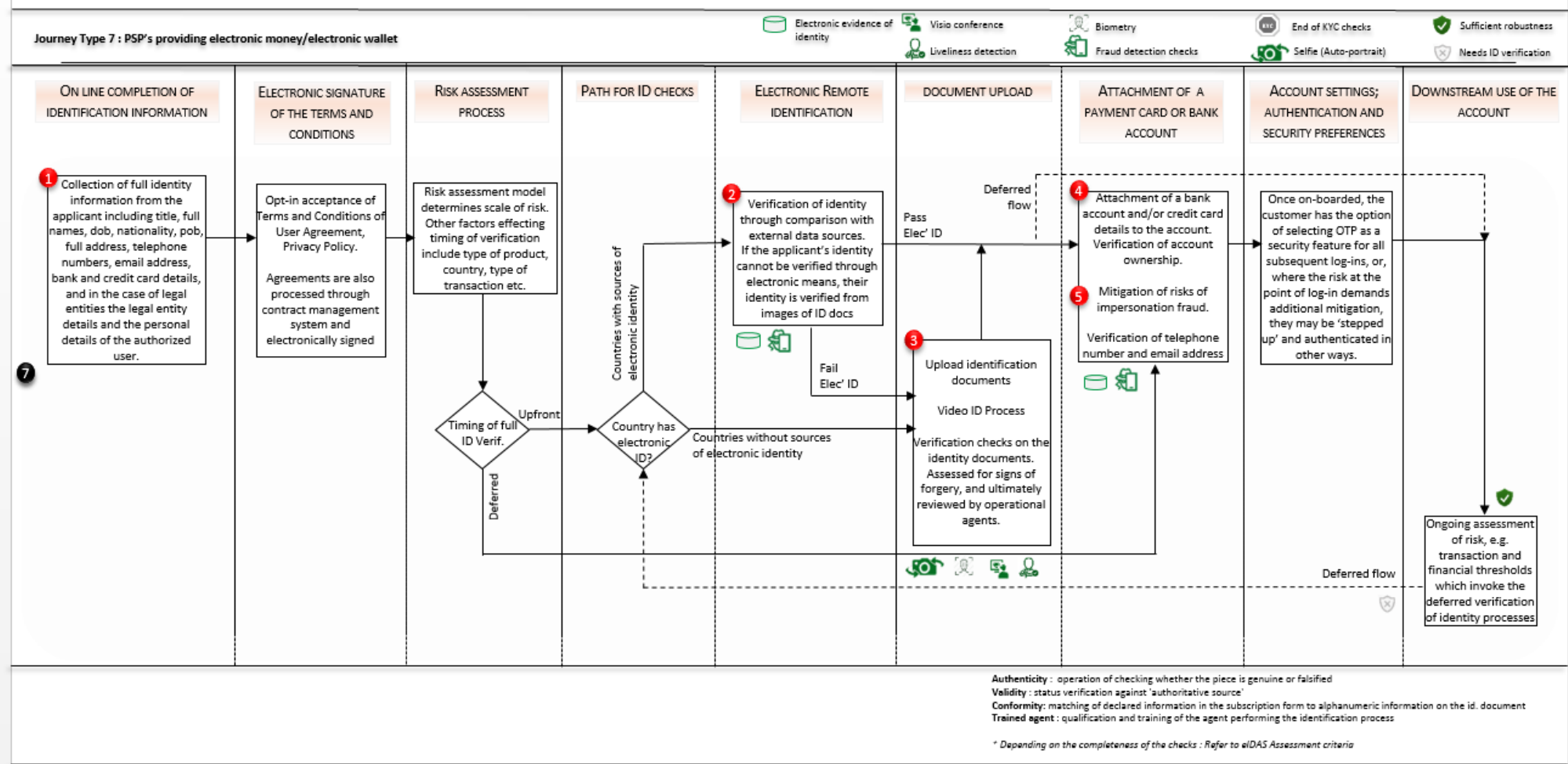
				<p>notice to the Financial Intelligence Unit.</p> <p><b>Requirements for recording and reproducibility of recording</b></p> <p>(1) The service provider must record the information flow containing image and sound in such a manner that allows for it to be reproduced with a quality equal to the initial transmission of synchronised sound and image.</p> <p>(2) The information flow that contains image and sound must be recorded with the time stamp, the client's IP address, the name of the person to be identified and the personal identification code of the person to be identified, whilst the time stamp must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified.</p> <p><b>Requirements for framing the face and document of a person</b></p> <p>The service provider may instruct the person to change his or her position and place themselves and the document <b><u>in the frame to make it possible to identify the person and verify person's identity, including to view the data or images on the document.</u></b></p>
--	--	--	--	---

				<p><b>Interview</b></p> <p>In order to collect and verify the information and data required for the determination of the client profile, the employee of the service provider asks partly structured questions in the course of the interview, proceeding from the results of the identification questionnaire.</p> <p><u>The employee of the service provider must carry on the interview that is mandatory for the establishment of a business relationship in real time.</u></p> <p>The employee of the service provider must assess the client's reaction during the interview, the reliability of the obtained information and data and compliance with the information and data obtained with other procedures, and record his or her opinion and the circumstances that are the basis thereof in the client profile and risk profile.</p> <p><b>Identification questionnaire</b> (CDD requirements)</p> <p>The identification questionnaire is used to ascertain a natural person's residential address, activity profile, area of activity, purpose and nature of establishment of a business relationship, connection of the person's economic or family interests with Estonia, expected volumes of the services</p>
--	--	--	--	--

			<p>used by the person in appropriate cases, the beneficial owner, whether the person is a politically exposed person and other important information.</p> <p>The identification questionnaire is used to ascertain the legal entity's business name, registry code, location and places of operation, including branches located in foreign countries, the entity's legal form, legal capacity, lawful and contractual representatives, beneficial owner(s) and, if appropriate, whether the beneficial owner is a politically exposed person, economic connections with Estonia, contracting states of the European Economic Area and third countries, most important business partners, the legal entity's activity profile, main and secondary areas of activity, purpose and nature of establishment of a business relationship and other important information.</p> <p><b>Determination of the client profile and risk profile</b></p> <p>The service provider prepares the client profile and the risk profile as a part thereof on the basis of the activity guidelines and procedural rules.</p> <p><b>Rules of procedure of a service provider</b></p> <p>The service provider must establish</p>
--	--	--	--

				<p>procedural rules for identification of a person and verification of person`s identity with information technology means.</p> <p><b>Rules of procedure applicable upon the establishment of a business relationship and conclusion of a transaction</b></p> <p>(1) Proceeding from the risks of the service and the Minister of Finance Regulation No 10 of 3 April 2008 'Requirements for procedural rules established by credit and financial institutions and their implementation and inspection of compliance with them', the service provider prepares and implements activity guidelines for the implementation of due diligence measures upon the establishment of a business relationship and the conclusion of a transaction.</p> <p>(2) The procedures set out in sections 2 and 10 are carried out by an employee of the service provider or an automated system.</p> <p>(3) The service provider is obliged to prevent the risks of the automated system being manipulated.</p> <p><b><u>Thus all the above described process can be automated.</u></b></p>
--	--	--	--	--

## Journey 7: Remote on-boarding employed by e-merchants using electronic wallet



Journey 7: Portrays the typical processes that are used to identify and verify a customer’s identity when opening an e-money / e-wallet account. The steps where identification and verification solutions are used are numbered within red circles, and correlate to the numbered headings in this document.

Introduction

The purpose of this document is to draw attention to the commonly used identification solutions within a typical e-money / e-wallet on-boarding journey. The document will consider the availability of those solutions, both domestically and cross-border (within the EU/EEA), the potential risks posed by using such solutions, and how those risks can be mitigated.

Whereas the identification of customers always commences with the collection of information about their identity, contact information and the details of the funding instrument(s) to be attached to their account, the policies and processes intended to verify identity vary between Payment Service Providers (‘PSPs’) and the countries in which they operate.

To be clear, the onboarding flow set out in Journey 7 is a generic simplification of more complex processes deployed by individual companies in this sector. The diagram only provides context for the deployment of solutions supporting verification of a prospective customer’s identity. Although higher risk situations are catered for within the flow, depending on the features of the account, customers may qualify for Simplified Due Diligence.

The identity verification solutions discussed within this document are subjectively assessed by the experience of the experts within the sub-group, and objectively compared with two authoritative benchmarks:

1. The JMLSG Guidance Notes on the identification and verification processes for individual and legal entities (version 13 December 2017)
2. The Annex to the Commission Implementing Regulation (EU) 2015/1502, which sets out the identity proofing standards for the three Levels of Assurance

The meaning of terms ‘identification’ and ‘verification’ correlate to the definition they are given within section 5.3.2 of the JMLSG Guidance Notes.

Step 1: Data Collection

The onboarding flow starts with the prospective customer completing an online application form which captures all relevant identity information from the applicant. This includes their title, forename, surname, date of birth, place of birth, nationality, address, telephone numbers, email address, bank account and/or credit card details.

Consideration	JMLSG (version 13 <sup>th</sup> Dec 2017)	Annex to EU 2015/1502
Sufficiency of identity data elements	Identity elements captured in the data collection process aligns with section 5.3.71	2.1.1 ‘Collect the relevant identity data required for proofing and verification.’ The same requirements apply for LOA Low, Substantial and High.

Step 2: Verification of Identity (data approach)

For the most part it is Credit Reference Agencies (‘CRAs’) who provide online identity verification solutions. These are founded on the extensive records of personal, financial, commercial, and public sector data sources held within their databases, and external sources of data which are dynamically integrated into their identity verification products. The features of these solutions vary between service

providers, but they commonly use the identity elements of data collected by PSPs in the onboarding process to retrieve the information held on the customer within their databases, and then assess the identity elements related to those data files to measure the extent to which the customer's identity can be verified.

These assessment processes typically weigh up the number of data sources associated with the customer, the age of those data sources, and the type of account from which the identity elements were taken, i.e. breadth, depth and quality. PSPs will configure policies within decision systems to automatically assess if the identity information upon the prospective customer is sufficient to open a particular type of account and, if not, the customer will be asked to supplement the verification process with documentary evidence of their identity.

Although the primary purpose for CRAs collecting data on the performance of credit accounts (and other relevant sources) is to enable credit providers to assess risk, it is also legitimate to use the identity elements of 'account performance data' to aid the verification of the identity of individuals.

These sorts of identity verification solutions are relevant in countries with mature Credit Referencing capabilities, and within the EU they are particularly strong in UK, Germany<sup>55</sup>, and Italy. Full Identity data is available in other EU countries, but in general there is less coverage of all the relevant data fields that need to be verified. In other countries there is a reasonable abundance of data on people's names and addresses, but less data on customer's date of birth.

The origin of the data processed by Credit Reference Agencies includes companies in the financial services sector, insurance, utilities, telecoms, as well as Government sources. These data sources include indicators flagging changes in residency, deceased records, access to identity fraud warning files, and other sources which can be categorised by the strength of reliance that is placed upon them. The sources of data, as well as the CRA's, are independent, regulated and reliable.

These data records provide a current and historical picture of the individual's identity that cannot be replicated – meaning that because the data is loaded onto the CRA databases in the moment it is received by them, it is not practically possible for a fraudster to recreate an extensive history for a completely new identity. Therefore, a person's credit file represents their 'footprints in life' which are indelibly recorded over time within the CRAs and the other sources from which such data is gathered. It can portray a clear image about the existence of a person's identity, their present and previous addresses, associations, as well as indicators which give cause to suspect the identity might be compromised.

Therefore, this data can be used to cross check that the identity of an applicant corresponds to that of a real person, residing as stated, with or without any inconsistencies in the information they provided, to a standard necessary to offset the risk of fraud. Furthermore, the transparency of these data files to the owner of the identity means that any nefarious use of their identity is observable to them when their data is referenced, or upon their request, thereby enabling identity fraud to be easily discovered.

Electronic evidence of identity is an efficient method of verifying identity, accessible via both API and transactional web tools, taking typically ~2 seconds for a PSP to complete, and achieving pass rates typically between 75% and 90% depending on the demographic of the applicant and the type of service they are applying for.

The demographics that cannot pass this type of identification process are individuals with 'thin' credit files who do not have enough data recorded at the Credit Bureaus to substantiate that they are who they say they are. Such individuals need to be identified from identity documents.

---

<sup>55</sup> Regarding Germany, German AML law does not provide for an identification procedure based on matching identification data against a CRA data base neither for natural persons nor for legal persons. However, it is conceivable using such an identification method under the concept of low risk allowing to exercise simplified due diligence.



The same data that is used to verify the identity of an individual can also be used to ensure the customer in session with the PSP is the true owner of that identity. This can be done through a process known as 'Knowledge Based Authentication' where the customer is asked questions about themselves which, in aggregate, only they should be able to answer correctly.

Other data points can help verify the customer in session is the owner of the identity, for example cross-referencing the ownership of the financial instrument attached to the e-wallet, location data linking the session to the address of the real owner of the identity, telephone subscriber checks coupled with proof of possession of the device, checking ownership and access to the customer's email address, and other such processes.

PSP's using these sorts of solutions invariably deploy complementary identity verification and fraud detection processes such as those considered in a later part of this document.

Suppliers of identity data do not restrict supply to domestic PSP's. It is equally available to PSP's in any country, on condition that they meet the privacy and security conditions of the solution provider.

Aside from CRAs, and companies re-selling identity services provided by CRAs, there are new innovations in the ways in which PSP's can verify their customer's identity without relying on referencing centralized databases. New identity verification systems may re-shape the method of verifying identity whilst protecting the customer's privacy. Albeit these sorts of propositions are at an early stage of development, they have potential to achieve a robust verification of the customer's identity and provide an electronic identity verification solution for segments of society which lack a sufficient financial profile to pass those tests.

Examples of companies providing these services include CRAs include (the following is a non-exhaustive list): Experian, Equifax, TransUnion, Schufa, CRIF, and providers of CRA identity data such as Trulioo, GB Group, and other companies such as IdentIQ.

<b>Consideration</b>	<b>JMLSG (version 13<sup>th</sup> Dec 2017)</b>	<b>Annex to EU 2015/1502</b>
Evidence of identity verification	Needs to align with sections 5.3.39 to 5.3.50, and 5.3.79 to 5.3.84	Section 2.1.2. LOA Low appears to be met. It is arguable that LOA Substantial is met where the evidence of identity is coupled with verification that it is that customer in session and steps have been taken to minimize the risk of impersonation fraud.
The criteria for using providers of electronic verification of identity solutions	Needs to align with sections 5.3.51 to 5.3.53	Section 2.4. Service providers should have documented information security management practices, policies, approaches, controls commensurate to the level of risk.

### Step 3: Verification of identity (documents)

This approach is relevant for individual applicants and customers whose identity cannot be verified through data sources, or in countries where it is not possible or appropriate to use identity data for verification of the customer's identity. The individual will be asked to upload images of documents from a predefined list of types of acceptable proofs of identity and address.

The customer uploads an image of their identity document which is captured using a scanner, or a camera within a mobile phone. In many cases the customer is guided through the process of providing the PSP with evidence of their identity through the PSP's application on the customer's mobile device. These applications, and third-party SDK's within them, help capture a higher quality image of the

customer's identity document, as well as an image of their face, and a process to detect the facial image is that of a live person – a 'liveness' test. The comparison between the facial image on the identity document and the facial image 'selfie' of the customer uploading the document, is processing which tends to occur on the server side, and not within the device.

A relatively new range of solutions can read the electronic chip within an electronic identity document, thereby capturing the identity details of the individual, and their facial image electronically, which has some advantages over capturing a photographic image of the document.

Video Identification sessions can also be used as a channel for capturing identity documents and the facial image of the customer presenting them, enabling the facial image on the document to be compared with the bearer of it, and the document to be validated as genuine. This can involve both human and automated processes.

Once the identity document(s) have been captured, they can be verified manually and/or automatically to check that they are genuine. Where the facial image of the applicant has been captured, that image is compared with the facial image upon the identity document, and the biographical information upon the identity document is compared manually and/or automatically with the identity information provided by the customer in the application flow. Anti-fraud and forgery checks are completed automatically and/or manually.

The scale of fraud and forgery associated with these processes depends on the competency of the solution provider, the implementation strategies, and training provided to operational agents tasked with reviewing identity documents.

The effectiveness of automated systems and operational agents in detecting forged or altered documents would be improved if the countries issuing identity documents facilitated access to databases of compromised documents and confirmed the details of genuine documents.

Examples of companies offering automated document evaluation services include (the following is a non-exhaustive list): AU10TIX, Mitek, Idmee, iDenfy, WebID, Authada, IDnow, AriadNext, Jumio, ReadID, Ecertic, Lleidonet, electronicID, Veriff, Algoreg.

<b>Consideration</b>	<b>JMLSG (version 13<sup>th</sup> Dec 2017)</b>	<b>Annex to EU 2015/1502</b>
Evidence of identity verification	Needs to align with sections 5.3.73 to 5.3.78	The process for evaluating documentary evidence of identity and it's connection to the genuine owner of that identity needs to be assessed against the tables in section 2.1.2 of the implementing regulations. Expert comment: Section 2.1.2 of the implementing regulations anticipate that PSPs will minimize the risk of the evidence of identity being lost, stolen, suspended, revoked or expired. How can this be achieved in most EU countries where entity that issued the document does not provide a service which allows PSPs to check if the document is compromised and that the document is still valid?
Outsourcing and use of Third Parties	Care to ensure that externally provided processing aligns, where relevant, with sections	Section 2.4 - headline requirements, and specific subsections including 2.4.1

	2.16 – 2.21, 3.35, 4.29, and 5.6.4 – 5.6.23	General provisions; Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.
--	---	--

Step 4: Ancillary identity verification processes

The process of registering and confirming the customer’s ownership and control of the funding instrument(s) associated with an electronic wallet lends credibility to the identity of the applicant and reduces the risk of fraud. This verification process has historically been achieved through ‘micro deposits’ as well as numeric codes distributed in the transaction information of that funding instrument, thereby allowing the real owner of the bank or card account to confirm to the PSP that they are in control of it. If the funding instrument is a card, it may also be ‘confirmed’ where the card issuer challenges the cardholder through the 3DS process. This can be done either when registering the card with the electronic wallet or when making an initial transaction.

Some Credit Reference Agencies can check if the identity details of an individual match those of the bank or card account.

Verifying access and ownership of a funding instrument is also possible through leveraging the Account Information Service Provider ‘AISP’ provisions in PSD2. The use of this process to help verify identity to help meet KYC obligations would be improved if the account data made available by banks were to include the customer’s formal name, address and date of birth. The coupling of verification of identity and authenticating that the customer in session is the owner of that identity increases the level of confidence the identification process.

Confirmation of the customer’s contact information will also help reduce the risk of fraud. For example, confirming the recipients access to the email account, the age of the email account, the recipients control over the phone number, and the link between the subscriber of the phone number and the applicant. These processes can be developed internally by the PSP, though are sometimes supplemented with external data points about the customer’s device, email address, and telephone subscriber details.

Examples of companies offering AISP services that can be used to confirm ownership of the funding instrument include (the following is a non-exhaustive list): Tink, Experian, Equifax, TransUnion, Zoot, Truelayer, Yodlee, Trustly, Plaid, PPRO, Satledge, B+S, Fin Tech Systems, finAPI, Niiio, Figo, Kontomatik, Instantor, Budget Insight, Giropay, Arvato.

Examples of companies offering bank and card verification services include (the following is a non-exhaustive list): Experian, Equifax, TransUnion, Schufa.

<b>Consideration</b>	<b>JMLSG (version 13<sup>th</sup> Dec 2017)</b>	<b>Annex to EU 2015/1502</b>
Evidence of identity verification and fraud detection processes	Needs to align with sections 5.3.79 – 5.3.84, and 5.3.85 to 5.3.91	Section 2.1.2. LOA Low appears to be met. It is arguable that LOA Substantial is met where the evidence of identity is coupled with verification that it is that customer in session and steps have been taken to minimize the risk of impersonation fraud.

Step 5: Typical fraud detection processes

Some countries benefit from mature data sharing arrangements intended to detect fraud by sharing and comparing application information with historical applications and existing accounts. These systems detect fraudulent anomalies between new applications and prior applications within 'closed user groups' that pool application data in a collective effort to prevent fraud. This is a very successful and well-established process, notably in the UK.

Matching new applications to known cases of identity fraud is another tried and tested method of detecting identity risks, as well as protecting victims of identity fraud from suffering further abuse. These data bases can be accessed on a stand-alone basis, or directly from the aforementioned application data sharing schemes.

In some cases, firms capture and share information in consortiums to assess the riskiness of the customer's device, telephone details, and email address. Multiple data points are automatically captured and contrasted with data previously collected to detect suspicious anomalies. These are assessed using predictive models to measure the riskiness of the customer.

Examples of companies offering fraud detection solutions geared to the prevention and detection of identity fraud through data sharing include (the following is a non-exhaustive list): Experian, Equifax, TransUnion, Synectics Solutions, Schufa, CIFAS, National Hunter.	<b>JMLSG (version 13<sup>th</sup> Dec 2017)</b>	<b>Annex to EU 2015/1502</b>
<b>Consideration</b> Mitigate the risk of a false identity, and the risk of impersonation	Needs to align with sections 5.3.85 to 5.3.91	The tables within section 2.1.2 include processes aimed at detecting and minimizing the risk of identity fraud.

### Conclusion

For PSP's providing electronic wallet services, cross-border account opening could be more streamlined once a significant majority of citizens have been issued with eID tokens. Until then, the capability to use them is only realistic in countries with sufficiently high issuance of eID's to justify the costs of integrating them into identity verification processes. In the meantime, PSPs need to find ways of achieving both security and convenience in their customer onboarding processes through identity data, documents and ancillary processes. Experience shows that it is impossible to eliminate all fraud, especially where the attack method is sophisticated but not scaleable. However, investment in refining identity verification solutions, testing new ones, and implementing these in accordance with ESA's 'Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process' (dated 23<sup>rd</sup> January 2018), will ensure the sector can innovate, whilst retaining effective ways to mitigate and manage risk.

## Annex 2: EU Mapping of the use of Digital Identity in bank account opening and the AML Regulations governing it

 **SWEDEN**

eID-solution issued by the Swedish banks : BankID


BankID dominates the eID-market with slightly less than 100% of the market.

eID-solution issued by the Swedish banks, BankID dominates the eID-market with slightly less than 100% of the market.

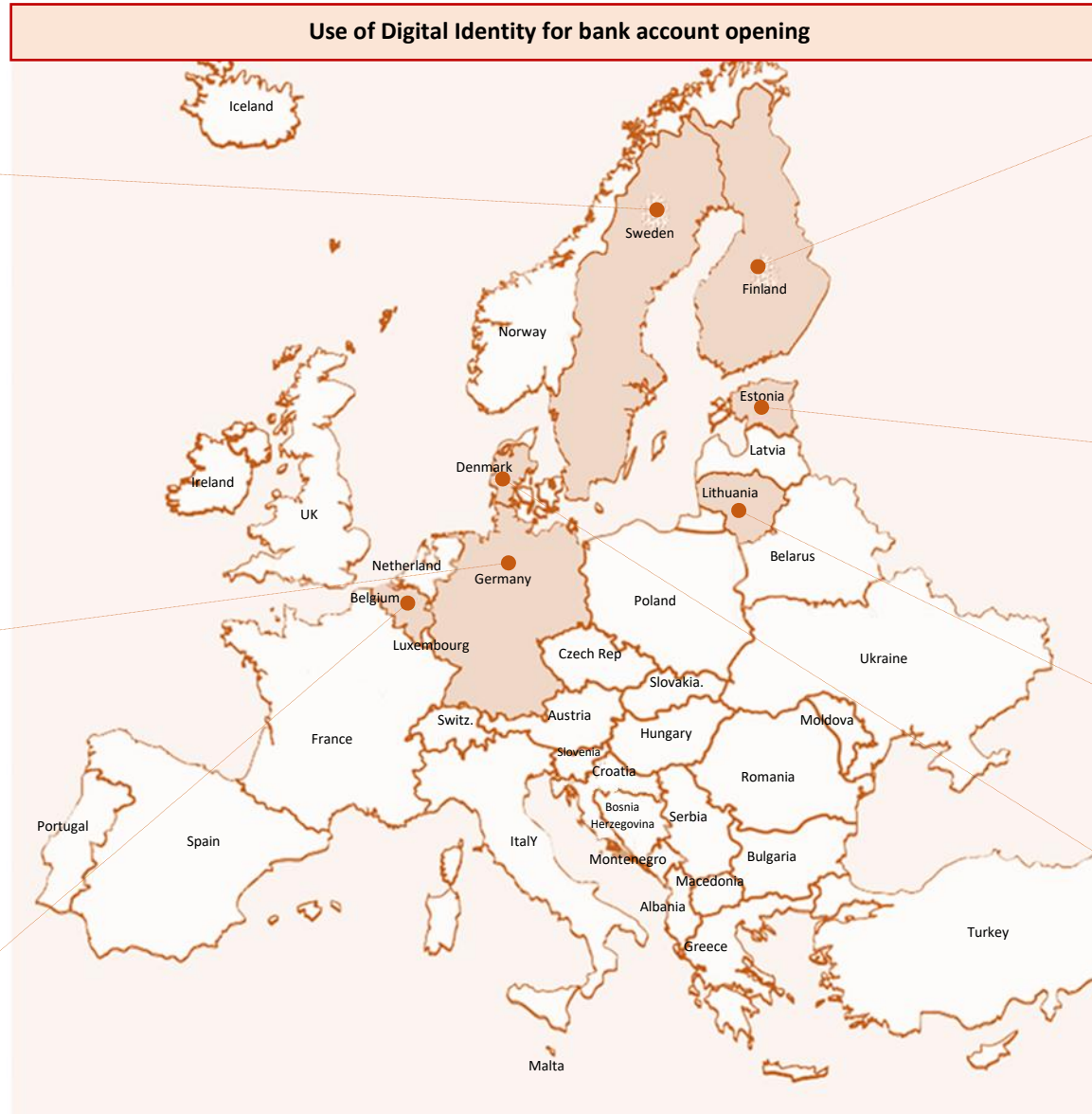
 **GERMANY**


Video identification according to BaFin circular 3/2017 is the most used digital onboarding method.

2 use cases for two German banks customers:  
Linkage of their Verimi account to their bank online banking for a convenient and secured Log On the bank website  
Data fields like IBAN, address and phone number can be uploaded to the Verimi account to prefill data fields of other Verimi partners.  
e.g. ID card and Mobile ID

 **BELGIUM**


eIDs notified under eIDAS with sufficient assurance (eg. ItsMe app)




 **FINLAND**

The remote on-boarding and the use of electronic identification is permitted under AML/CTF


OP Bank and Nordea Bank enable the opening of bank accounts via remote onboarding, if other banks' bank ID's are used for electronic identification

 **ESTONIA**

Allow Estonian residents and e-residents to open a bank account without having to go to a bank branch.  
E-resident cards (approved by LHV, Swedbank and SEB banks)  
ID card and Mobile ID  
Few conditions have been set by the Legislation since the identification is done by info technological facilities (monthly amount of payment limited to €10,000 for a natural person and €25,000 for a legal person; obligation to cancel the long-term contract without providing the advance notice of the expiry of the term)

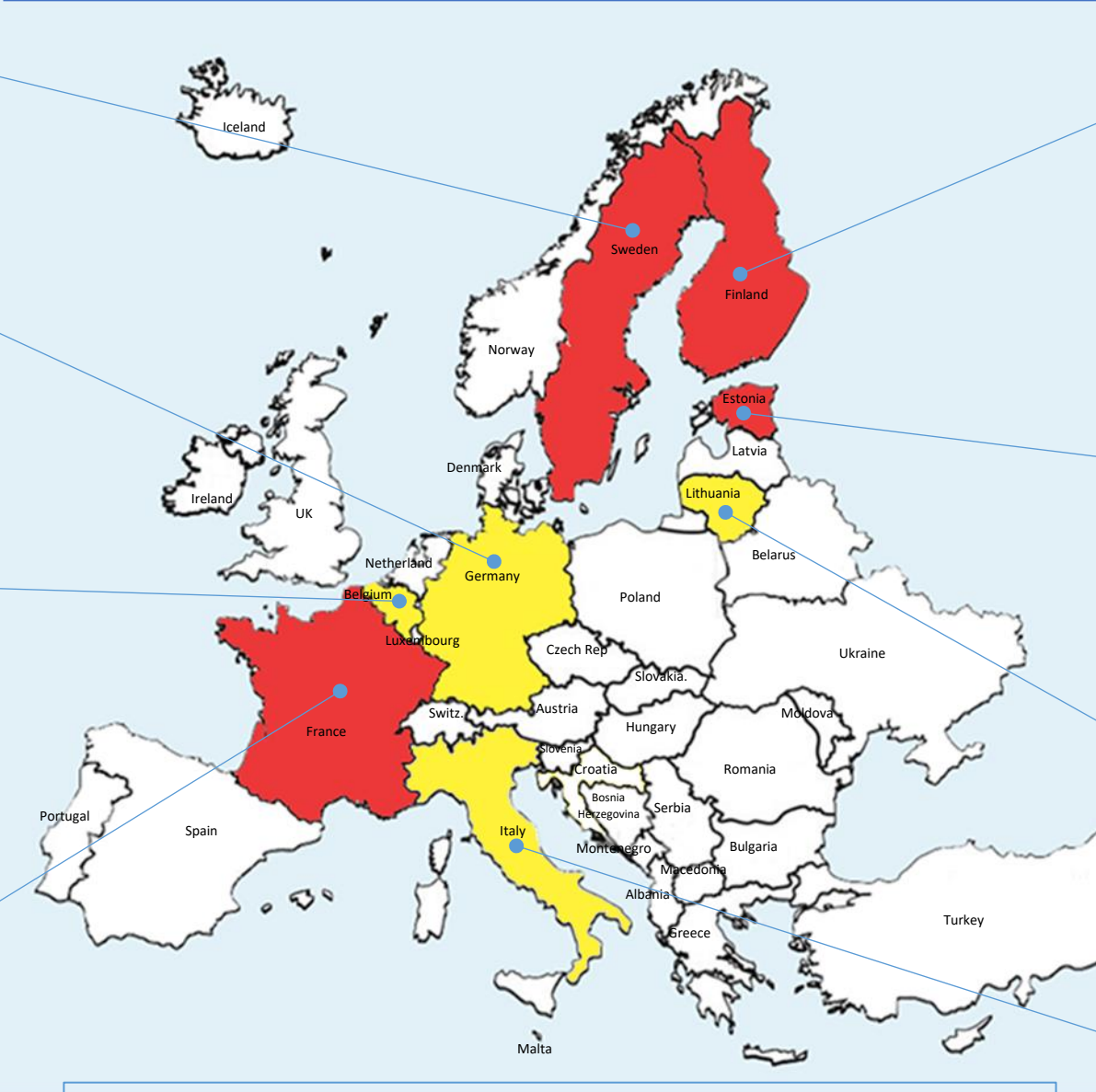
 **LITHUANIA**

It is possible use the m-ID solution and it is used in practice by some banks. Such solution in fact is a qualified electronic signature under the eIDAS (No 910/2014) regulation.

 **DENMARK**

Denmark has an eID system called NemID, which is a public-private partnership between the public sector (Ministry of the Interior) and the banks. NemID is issued to all individuals above the age of 15 who have a Danish Civil Registration Number ("CPR number").

## AML Regulation on use of Digital identity for bank account opening



### SWEDEN

The remote on-boarding and the use of electronic identification is permitted under AML/CFT

Bank-ID is industry standard, and a physical meeting precedes a Bank-ID. Identification non-face-to-face is regulated by the competent authority's regulation FFFS 2017:11.

### GERMANY

Section 12 of the German AML Act establishes three types of digital identification: Electronic chip integrated in government issued ID card, Qualified electronic signature pursuant to eIDAS Regulation in combination with a transaction executed directly from an existing payment account, and Notified electronic identification scheme pursuant to eIDAS regulation with LoA „high“ According to German law digital identification is also possible by disclosure/transfer of an identification record formerly established by an AML-obliged entity; in practice 2FA for approval by the customer has established (Section 17 (1) AML Act and BaFin-AuA No. 8.4).

### BELGIUM

Customer ID should be verified against one or more supporting documents or reliable and independent sources of information which enable obliged entities to confirm this data, in order to have a sufficient degree of certainty that they know the persons concerned (art. 27, § 1, Belgian AML Law).

### FRANCE

Either a notified electronic identification mean level high (sufficient) or a French national electronic identification mean level high (sufficient) see R. 561-5-1 or a notified electronic identity level substantial (to be completed with another AML measure (R561-20 of the Monetary and Financial Code, 5) among the following:

- 1°) an identity document and a further document proving the identity;
- 2°) a verification and certification of the copy of the identity document or register from a third independent from the person who is to be identified;
- 3°) a credit or debit wire transfer from or to an account opened to the customer in the European Union;
- 4°) an identity certification issued from another bank;
- 5°) a substantial level eIDAS electronic identity;
- 6°) a qualified eIDAS signature or an

### FINLAND

The remote on-boarding and the use of electronic identification is permitted under AML/CFT

Act on Preventing Money Laundering and Terrorist Financing, 444/2017, Section 11 - Enhanced customer due diligence related to non-face-to-face identification

### ESTONIA

Estonian Money Laundering and Terrorist Financing Prevention Act (See §31. Identification of person and verification of data using information technology means)

Estonian Identity Act and coherence reading with AML regulation regarding the other cases where identification of the person and verify data with the help of the information technology means is required

### LITHUANIA

The current legal acts do allow the usage of the following eIDAS compliant solutions:

- using electronic identification means as set out in Regulation (EU) No 910/2014 corresponding to the assurance level substantial or high;
- using a qualified electronic signature certificate as set out in Regulation (EU) No 910/2014.

### ITALY

According to article 19 of the Italian AML Law (i.e. legislative decree 231/2007, as modified by legislative decree 90/2017 which implemented directive 849/2015), obliged entities can identify customers remotely provided that some conditions are met. These conditions are listed by the law itself (for instance, according to the law, customers can be identified remotely where they are endowed with high LOA digital identity) or by the implementing regulations on CDD issued by Banca d'Italia (BOI) or IVASS.

■ AML Regulation permitting electronic identity  
■ General Regulation permitting electronic identity (subject to verification)



## Use of video identification for bank account opening



**NETHERLANDS**  
Video identification or equivalent technique is associated to automatic transfer data from the id document to the relevant (liveness check)

**UNITED KINGDOM**  
Video Identification is used in association with electronic verification  
Remote onboarding is used primarily by newer, challenger banks who are online only and do not have branch network.

**BELGIUM**  
Use of video identification is possible since Customer ID should be verified against one or more supporting documents or reliable and independent sources of information which enable obliged entities to confirm this data

**LUXEMBOURG**  
Video identification permitting the delivery by Luxtrust of eIDAS-qualified electronic signature services

**FRANCE**  
Video identification + biometry is used  
(Currently no regulation governs video identification. A regulation on remote onboarding which will validate an eIDAS scheme is being prepared. Both substantial and high e-ID will be in scope of the regulation.  
Solutions are based on picture comparisons between the picture contained in an official identity paper (passport or id card) and a selfie.)

**LIECHTENSTEIN**  
Video identification

**ITALY**  
Video identification and biometrics or other technology solutions

**PORTUGAL**  
Use of video conference (e.g. Caixa Geral de Depositos) in addition with biometrics (Banco BNI Europa)  
For these use cases, the legislation requires financial institutions to have a person, in real time, validating the client's identity.

**SPAIN**  
Video identification systems is used. In some cases, in addition with electronic signature.  
Regulation is in place for both attended and unattended video identification. Widely used for mobile on-boarding by most banks and in some cases also for web-based (*BBVA, Santander, OpenBank, ImaginBank, Self Bank, Evo Banco and Bankia*)

**GERMANY**  
Pursuant to BaFin Circular 3/2017 Video-Identification is a recognized form of identification procedure in accordance with the AML Act in Germany

**LITHUANIA**  
Use of electronic means allowing direct video streaming. Based on the way followed, it permits the recording of the original of the identity document or the facial image of the customer (biometry).

**ESTONIA**  
Video identification (can be completed with biometrics)

**LATVIA**  
Video identification (acquisition of data accrediting the identity of a natural person from a credit institution or payment institution)

**POLAND**  
Use of Video-identification with or without biometry

**SLOVAKIA**  
Video call identification (via special application of the bank)

**AUSTRIA**  
Identification through video-chat has been approved by the Austrian Financial Market Authority (FMA) on 3 January 2017.

**ROMANIA**  
Video identification.

**HUNGARY**  
Real time video identification via comparison of the ID photo with the of customers. Used by OTP Bank, Gránit Bank, TakaréK Kereskedelmi Bank, Cofidis Bank, MKB Bank.

**SLOVENIA**  
Video identification + Identity card check is permitted to on board customer for account opening.

**MALTA**  
Video Identification: The (prospective) customer's identity is verified during a video conference call



## Annex 3: Detailed analysis of eID/KYC\_Assessment criteria

### Considerations and Regulation

This Annex will outline and discuss the eID/KYC\_assessment criteria to support financial institutions in their consideration of any remote on-boarding solutions. The assessment criteria will be considered alongside the European Banking Authority (EBA<sup>56</sup>) opinions, National EU AML Regulations and the UK Joint Money Laundering Steering Group (JMLSG<sup>57</sup>) guidelines.

The key elements of the eID/KYC\_assessment criteria are as follows:-

- i. Documentation**
  - a. Type and content of Documents
  - b. Capture – Video & Photo Capture
  - c. Verification – Authenticity and Validity of Documents
- ii. Identity of the individual**
- iii. Additional Considerations**
  - a. Communications
  - b. Liability
  - c. Governance
  - d. Certification

#### IA. Type and Content of Documents

When obtaining identify information, consideration must be given to the type and nature of documents or sources used, and the information contained within. Requirements from different regulations and guidance across Europe are expanded on below. EIDAS regulation also accepts identity documents for identification schemes other than those under an electronic form.

#### EBA

It is important that firms have regard to the validity and authenticity of data, documentation and information obtained in respect of their customers. The European Supervisory Authorities (ESAs) believe that firms should consider, *inter alia*, whether there are controls in place to ensure that identity documents have not been altered, counterfeited or recycled and therefore firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include limiting the type of acceptable identity documents to those that contain:

- High security features or biometric data including finger prints and a facial image (e.g. e-passports and e-ID);
- A qualified electronic signature created in line with standards set in Regulation (EU) No 910/2014 (especially relevant where a customer is a legal person);
- A feature that links the innovative solution with trade registers or other reliable data sources such as the company registration office database; or

---

<sup>56</sup> **JC 2017 81** OPINION ON THE USE OF INNOVATIVE SOLUTIONS BY CREDIT AND FINANCIAL INSTITUTIONS IN THE CUSTOMER DUE DILIGENCE PROCESS [https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20\(JC-2017-81\).pdf](https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf)

<sup>57</sup> The UK JMLSG is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance. Open source access to JMLSG: <http://www.jmlsg.org.uk/>.

- A feature that adjoins the innovative solution with the government-established CDD data repository or the notified e-ID scheme as defined in Regulation (EU) No 910/2014, if the scheme's assurance level is classified as substantial.

#### National AML Regulations and how these are linked to eIDAS electronic identification means

European Union law now recognises that there are safeguards, in particular eIDAS Electronic identification means, which reduce the risks relating to non-face-to-face business relationships or transactions. There are already a number of different national European AML regulations concerning the different eIDAS identification means, some of which are expanded on below.

Use of electronic identification means issued in the European Union which operate under the electronic identification schemes with the **assurance levels high or substantial** is for example, considered sufficient in [Lithuania](#).

In [France](#), it is sufficient to use either a **notified electronic identification means level high**, a French national electronic identification means level high (see R. 561-5-1 of the Monetary and Financial Code), or a **notified electronic identity level substantial**, to be completed with another AML measure (R561-20 of the Monetary and Financial Code) among the following:

- 1) an identity document and a further document proving the identity; 2) a verification and certification of the copy of the identity document or register from a third party independent from the person who is to be identified; 3) a credit or debit wire transfer from or to an account opened to the customer in the European Union; 4) an identity certification issued from another bank; 5) a substantial level eIDAS electronic identity, or; 6) a qualified eIDAS signature or an advanced signature relying on a qualified eIDAS certificate.

**A qualified certificate or strong electronic identification device** can be used in [Finland](#). It is the same as in France regarding a qualified certificate, but in France requiring an additional means. Indeed there is possibility in France to collect an advanced or qualified electronic signature or seal, based on a qualified certificate containing the identity of the signatory or seal creator, and issued by a qualified trusted service provider registered on a national trust list (in application of Article 22 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). But such an electronic signature is not sufficient and has to be completed with one other measure foreseen in R521-20 of the Monetary and Financial Code.

**Use of advanced signatures** are applicable and considered sufficient in [Sweden](#)<sup>58</sup>. Verification of the identity of a physical person can be conducted remotely by using an electronic identification to create an advanced electronic signature. Legal persons can be on-boarded by verifying the identity of a representative, by identifying and verifying the representative and verifying the authorisation to represent the legal person, and on which circumstances the authorisation rests by verifying the information of the first inset against the legal person's certificate of registration, external register or equivalent.

#### Other Electronic Means

In [Malta](#), **Electronic Verification** consists in the verification of identification details provided by a (prospective) customer on the basis of data read from either an electronic chip embedded in an identification document or from other electronic devices like mobile applications or computer software, subject to the following conditions:

- It has to be recognised as a legally valid means of identity verification in the country of nationality/residence of the (prospective) customer, provided that the said country is an EEA Member State or a reputable jurisdiction;
- The use of the electronic device as a means of identity verification is administered or approved by the government of an EEA Member State or a reputable jurisdiction;

---

<sup>58</sup> E-signatures are regulated by the regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

- The software/hardware used by the (prospective) customer to transmit data and by the obliged entity to read the same has to be administered or approved by the government of an EEA Member State or of a reputable jurisdiction.
- Retention of the following records:
  - Print-out or an electronic copy evidencing that all necessary personal identification details have been verified; and
  - Reference to the system used to transmit and read data.

Electronic verification may also take place through privately run systems like **Bank ID**<sup>59</sup> which is used as long as the above conditions are met.

In Germany, using Verimi and Deutsche Bank as an example, an electronic identity can be obtained by performing a video-identification for which a trained agent performs the assessment. Verimi then generates the electronic identity and provides this identity to Deutsche bank. The bank is able to use the electronic identity for an account opening process subject to relevant conditions being met. Examples of conditions are:-

- a. the underlying ID is still valid,
- b. the eID has been set up with Verimi in the last 24 months,
- c. the underlying documents (i.e. video files) are distributed as well, and
- d. the communication is handled via secure channels including a 2FA authentication from the client.

For the time being, it is not possible under German law to re-use a Verimi ID in a three parties' way, i.e. Bank A generates a digital identity, sends it with customer consent to an identity platform (e.g. Verimi) and Verimi distributes this identity to Bank B.<sup>60</sup>

## JMLSG

UK JMLSG Guidelines state that the firm should obtain the following information in relation to the private individual:

- Full name;
- Residential Address; and
- Date of birth.

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court or local authority, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

Non-government-issued documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another regulated financial services firm, or is supplemented by knowledge that the firm has of the person or entity, which it has documented.

If identity is to be verified from documents, this should be based on:

---

<sup>59</sup> As an example, BankID is used widely in Sweden and Norway. <https://www.bankid.com/en/>

<sup>60</sup> VERIMI does not distribute notified digital identities. His solution uses German AML regulation according to which According to German law digital identification is possible by disclosure/transfer of an identification record formerly established by an AML-obliged entity for an account opening at another bank; in practice 2FA for approval by the customer has established (Section 17 (1) AML Act and BaFin-AuA No. 8.4).

- A government-issued document which incorporates: **the customer's full name and photograph**, and either (a) their residential address; or (b) their date of birth. UK Government-issued documents with a photograph include: valid passport; valid photo-card driving licence (full or provisional); national identity card; firearms certificate or shotgun licence; and identity card issued by the Electoral Office for Northern Ireland.

OR;

- Government, court or local authority-issued document (**without a photograph**) which incorporates the customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the UK financial services sector, which incorporates: the customer's full name and either (a) their residential address; or (b) their date of birth.

Government-issued documents without a photograph include: valid (old style) full UK driving licence; recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit, tax credit, pension, educational or other grant); instrument of a court appointment (such as liquidator, or grant of probate); and current council tax demand letter, or statement.

Examples of other documents to support a customer's identity include current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK or EU, or utility bills. If the document is from the internet, a pdf version may be more reliable (but firms should recognise that some electronic sources may be more easily tampered with, in the sense of their data being able to be amended informally and unofficially, than others. If suspicions are raised in relation to the integrity of any electronic information obtained, firms should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant source should be used). Where a member of the firm's staff has visited the customer at their home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (i.e., equivalent to a second document).

## IB. Video and Photo Capture

Under eIDAS regulation, when capturing photos or videos as part of the identification process, a number of considerations should be given, including that of image quality requirements (e.g. ISO 19794-5, light quality, number of pixels, distance of subject from camera), the potential need for real time video analysis, and how the image is stored/archived. **This is particularly important if the communications channel is via a non-integrated third party (e.g. Skype).** Furthermore, when using remote onboarding solutions, ways to make use of identity evidences containing a photo (or other physical characteristic) and where possible to make use of biometric algorithms to compare the applicant with the claimed identity should also be considered. Other considerations from the EBA and European regulations are expanded on below.

### EBA

As referenced above, the EBA notes that it is important that firms have regard to the validity and authenticity of data, documentation and information obtained in respect of their customers. The ESAs require that firms should consider, *inter alia*, whether there is a risk that:

- **The customer's image visible on the screen is being tampered with during the transmission?** The ESAs believe that competent authorities should ensure that firms have sufficiently robust controls in place to prevent or reduce such risk. These controls may include some or all of the following:
  - A feature whereby a customer is required to have a live chat with an administrator who has received specialised training in how to identify possible suspicious or unusual behaviour or image inconsistencies;
  - A built-in computer application that automatically identifies and verifies a person from a digital image or a video source (e.g. biometric facial recognition);

- A requirement for a screen to be adequately illuminated when taking a person's photograph or recording a video during the identity verification process; and
- A built-in security feature that can detect images that are or have been tampered with (e.g. facial morphing) whereby such images appear pixelated or blurred.
- **An ID document displayed on the screen by a customer during the transmission belongs to another but similar-looking person.** The ESAs consider that firms should ensure that the innovative CDD solution contains built-in features that enable it to identify any discrepancies, or that staff responsible for the identify verification during the transmission have been trained to spot situations where the person on the screen looks different from the person on the ID document.

#### National European AML Regulations on use of video identification

Spain differentiates between **video conference** (with a human employee in real time) and **video identification** (the human employee does not interact with the applicant) due to the different risks involved.

Video conference: Certain requirements need to be met prior to authorisation: reliable and visible client documentation, ex ante customer risk analysis, technical and effectiveness requirements, keep video recordings for at least 10 years among other requirements.

Video identification: video identification poses a greater risk than videoconferencing, since there is no online interaction, but a later control of the recording. Thus, additional requirements are set, among them: client must only use one device, obliged subjects must record the streaming, such recording must be assessed by the obliged subject prior to any business operation, etc. For a complete list of specifications regarding procedures for identifying customers in remote transactions please refer to: [Due diligence | Sepblac<sup>61</sup>](#).

Similarly, in Luxembourg CSSF (Commission de Surveillance du Secteur Financier) guidelines, the **video identification also needs to be performed by a specifically trained employee**, either of the institution or, if applicable, of the external provider. The video identification/verification of the identity of a customer which is not actually performed by a specifically trained natural person, but where the customer is in contact only with a robot, or where the customer simply uploads (a video with) identity documents online, does not qualify as video identification as addressed in the FAQs (See CSSF FAQ AML/CFT and customer on boarding/KYC methods Frequently asked questions on AML/CFT and IT requirements for specific customer on boarding/KYC methods) due to the absence of a live video chat or real-time interaction between the aforementioned trained natural person and the customer. Thus, contrary to the video identification, this kind of online/digital or robo-video-identification, without intervention of a natural person on behalf of the professional, requires the application by the professional of supplementary safeguards in order to mitigate those particular risks linked to the automated character of this kind of identification process.

In Hungary, **secured equipment is required**. The AML Act authorises the Central Bank of Hungary (as the supervisory authority for financial institutions) to determine detailed rules for the minimum requirements of the secure, protected electronic communications equipment and the method of auditing the equipment. However, elsewhere the video may have to be provided by an **external provider**, using trained employees (e.g. as per Estonian regulation Minister of Finance regulation on Requirements and procedure for identification of persons and verification of persons' identity with information technology means). On the contrary, as mentioned above, Luxembourg guidelines<sup>62</sup> provides for different possibilities regarding who can perform the video identification process. The trained individual can perform the video identification process themselves using a tool developed internally; or perform the video identification process themselves using an external tool they have acquired from an external provider; or delegate the identification process to an external provider using their own tool.

<sup>61</sup> <https://www.sepblac.es/en/obliged-subjects/obligations/due-diligence/>

<sup>62</sup> <https://www.cssf.lu/en/supervision/financial-crime/aml-ctf/faq/>

In Slovenian rules of the Ministry for example, there must be a **comparison between the applicant and the presented ID document**, and coherence check between all the information. The person performing the video-electronic identification shall be satisfied that the photograph, any personal description and data from the official identity document are in conformity with the party that initiated the video identification and verifies the logical consistency of all available data (for example, matching the appearance video and video clients in the official identity card or other information).

In Lithuania, according to Law on the prevention of money laundering and terrorist financing, the identity of the customer that is a natural person or a representative of the customer that is a legal person and of the beneficial owner may be established without the physical presence of the customer when using electronic means allowing direct video streaming in one of the following ways:

- a) the original of the identity document or an equivalent residence permit in the Republic of Lithuania is recorded at the time of direct video streaming and the identity of the customer is validated using at least an advanced electronic signature which conforms to the requirements laid down in Article 26 of Regulation (EU) No 910/2014; and
- b) the facial image of the customer and the original of the identity document or an equivalent residence permit in the Republic of Lithuania shown by the customer is recorded at the time of direct video streaming.

In Malta, the (prospective) customer's identity is verified during the course of a video conference call, subject to the following conditions:

- The live video transmission allows for visual and verbal contact between the (prospective) customer and the obliged entity;
- The transmission is of sufficient quality to allow the obliged entity to visualise the face of the (prospective) customer and the details of the identification document being produced by the customer;
- The identification document must be one of those expressly listed in the Implementing Procedures – Part I (valid unexpired passport, national or other identity card, residence card, driving licence, or non-government-issued documents containing photographic evidence recognised as a legal means of identification by the national law of an EU or a reputable jurisdiction) AND must have optical safety features;
- That, on the basis of the document's safety features, verify that the document is not fake or forged;
- Ensure that the facial image and identification details provided by the (prospective) customer tally with those on the identification document;
- During the course of the video call, there is a communication of a pre-transmitted code; and
- Retention of the following records:
  - Audio recording of the conversation between the (prospective) customer and the obliged entity;
  - Screenshots of the video call including of the (prospective) customer, the date and time of the call and of the identification document produced; and
  - Code transmission records.

Estonia, Germany and Austrian regulations provide more precise practical and technical rules for video interview (only permitted for Germany, and either video interview or video identification for Estonia) processes in order to avoid fraudulent identifications. These rules are exposed and commented in Typical on boarding 3 Assessment.

#### IC. Verification of the Validity and Authenticity of Documents

**Validity:** A verification status of the document (whether lost, stolen or expired) is made against an authoritative source (private or public).

**Authenticity:** In order to verify, authenticate and validate documents used in remote on-boarding, there are a number of key considerations and approaches to be followed under eIDAS. A comparison to existing public sources and databases providing detailed information about identity documents, e.g. the Public Register of Authentic travel and identity Documents Online (PRADO). This would be beneficial



in identifying counterfeit documents. Other checks could include ensuring that all features are correct, including syntax, a consistency check (e.g. check-digit<sup>63</sup> validation), whether or not the photo is genuine etc.

Requirements from European regulation and guidance is expanded on below.

#### EBA

In addition to the above references to the ESAs opinion in regard to the validity and authenticity of data, documentation and information obtained in respect of their customers through innovative solutions at on-boarding or during the business relationship, the ESAs believe that firms should consider whether there are controls in place to ensure that identity documents produced during the (video) transmission have not been altered (i.e. changes made to data in a genuine document), counterfeited (i.e. reproduction of an identity document) or recycled (i.e. creation of a fraudulent identity document using materials from legitimate documents)?

The ESAs underline that firms should have sufficient controls in place to prevent or reduce the risk of these breaches, which may include one or more of the following:

- **Built-in features** which enable them to detect fraudulent documents on the basis of the documents' security features (i.e. watermarks, biographical data, photographs, lamination, UV-sensitive ink lines) and the location of various elements in the document (i.e. optical character recognition);
- Features that compare the security features ingrained in the identity document presented during the transmission **with a template** of the same document held in the firms' internal identity document database; or
- Where the **verification is not based on a government-issued identity document**, to the extent permitted by national law and commensurate with the ML/TF risk, features that allow firms to verify the information received from their customers against a combination of multiple reliable and independent sources (including, but not limited to, government registers and databases), which can be supplemented with data mining and social network analysis, IP address analysis, and location or device analysis.

#### National European AML Regulations

Malta allows for the **verification of identity by reference to electronic copies of identity documents**. The use of electronic systems, including mobile apps, that allow a series of automated checks to be carried out on copies of identification documents uploaded through the said systems. The system must allow the following checks to be carried out:

- Visual Checks – Automatic comparison of the facial features of the (prospective) customer shown on the photographic image visible on the identification document with the facial features shown on a separate photo taken and sent by the (prospective) customer contemporaneously with the transmission of the identification document so as to determine that the individual is one and the same.
- Authentication Checks – Verify automatically the authenticity and validity of the identification document submitted by performing at least a number of established checks:
  - Verify security features
  - Examine the lamination for signs of tampering
  - Compare the document with standard templates
  - Read and validate the MRZ code
  - Verify that the document is unexpired.
- In addition electronic copies of the identification document uploaded and of the photograph provided by the (prospective) customer are to be retained by the system, indicating the time

---

<sup>63</sup> This is often the last part of a numeric field which is derived from the first part (e.g. modulo '97)



and date when these were uploaded or otherwise provided, and the system must have safeguards against any possible data alternation.

In Slovenia, similar checks are required on the identity documents for video identification which also permit further checks (use of the document's safety features that the document is not fake or forged):

- Visible verification of the existence of optical characters, including holographic or other equivalent protective elements (for example, safety threads, variable colours and the like), which must be clearly visible even with the horizontal and vertical inclination of the official identity document;
- Checking the formal signs of the official identity document and matching them according to the type of official identity document (graphic design, character size, character spacing, typography and the like);
- Verification of the matching of the data already obtained with the information shown in the official identity document;
- Checking the validity of the official identity document and the correctness of the alphanumeric characters of its serial number;
- A visual check of the possible post-installation of the photograph, the intrinsic lamination surrounding the official identity document, or other trademarks showing its intrinsic character;
- Verifying the logical consistency of the data derived from the document (for example, the correctness of the date of issue and expiration, the correctness of the birth date, their mutual match, and the like).

The verification of optical characters and formal signs of the official identity document referred to in the first two points above, may also be carried out using appropriate software support.

## JMLSG

The Money Laundering regulations require that customer due diligence must be carried out on the basis of **documents or information obtained from a reliable source which is independent of the customer**. It is therefore important that the evidence used to verify identity meet this test, both at onboarding stage and subsequently when due diligence is revised/updated.

The reliable sources, independent of the customer, might either be a document or documents produced by the customer, or electronically by the firm, or by a combination of both. Documents issued or made available by an official body are regarded as independent of the customer, even if they are provided or made available to the firm by the customer. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification.

**Authenticity of the documents:** some consideration should be given as to whether the documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity. Examples of sources of information include CIFAS, the Fraud Advisory Panel and the Serious Fraud Office. Commercial software is also available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

## II. Identity of the Individual

For remote registration of identities under eIDAS, identity proofing should be based on the review of more than one piece of identity documentation. In certain instances, the person whose the identity is claimed should be informed of the ongoing registration by an alternative channel, not specified or provided by the applicant, in order to counter identity spoofing.

Where possible, and when applicable, knowledge based verification processes could also be used to strengthen the validity of the claimed identity.

Importantly, for an electronic/digital check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register), or at a single point in time, is not normally enough on its own to verify identity.

In order to enhance the anti-impersonation controls further, additional verification could be sought that the provided elements (documents, biometric data) have not been previously associated to another identity (as far as is reasonably possible, but at a minimum in the providers system).

Additional considerations, and requirements, from European regulation, EBA and JMLSG guidance is expanded on below.

## EBA

### *Delivery Channel Risk*

Directive (EU) 2015/849 considers that non-face-to-face business relationships or transactions without sufficient safeguards are potentially higher risk than face-to-face business relationships. Therefore, there is an expectation that firms carry out an assessment of ML/TF risks associated with non-face-to-face business relationships and the extent to which the use of innovative solutions can address, or might further exacerbate, those risks.

Consideration should be given to the **risk that potential customers who are on-boarded via the innovative CDD solution are not who they claim to be** as they are impersonating another person or using another person's personal data or identity documents (i.e. identity fraud). Safeguards that could mitigate these risks may include the verification of a customer's identity on the basis of a notified e-ID scheme, as defined in Regulation (EU) No 910/2014, where the scheme's assurance level is classified as high, or a combination of other checks that ensure the information obtained during the transmission can be linked to a particular customer, for example:

- The verification of a customer's identity based on multiple factors and data sources, for example, where the customer's personal information is verified on the basis of a government-issued photographic document, combined with information obtained during the live chat with an administrator and information obtained from the government or other reliable and independent sources and databases;
- Built-in features that allow firms to detect their customers' native language based on their written communications with them;
- A requirement that all CDD documentation contains a qualified electronic signature created in line with standards set in the Regulation (EU) No 910/2014; or
- Verifying a customer's identity on the basis of more traditional processes such as sending a letter to the customer's verified home address.

## National European AML Regulations

### *Identification – A Two-Stage Process*

#### Poland

The client identification process should be considered a relatively simple **two stage process**. First, it may consist of the provision of personal data by the client (e.g. by e-mail, by filling in the form on the website of the obligated institution). Then second, the issue of verification of the customer's identity, aimed at confirming that the client is who he claims to be.

For this purpose, the obliged institution is required to use, in accordance with article 37 of the Act, a document confirming the identity of a natural person, a document containing valid data from the extract of the relevant register (in the case of a legal person or an organisational unit without legal personality) or other documents or data or information originating from a reliable and independent source.

Thus, the legislator left the obligated institution the opportunity to choose what documents, data or information will be the basis of the above-mentioned verification, indicating only that they must come from a reliable and independent source.

The subject provision of the Act is consistent with article 13, paragraph 1, letter a of the Directive (EU) 2015/84 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council repealing the Directive Of European Parliament and Council 2005/60 / EC and the Commission Directive 2006/70 / EC (Journal of Laws No. 141 of 05/06/2015, p. 73).

As a rule, in the verification of the client's identity without its physical presence, the most trusted instruments are electronic identification means referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93 / EC (OJ L 257, 28/08/2014, p. 84), including qualified electronic signatures.

#### *Information from Third Parties*

Using **information from third parties** about the customer or the beneficial owner in accordance with regulatory provisions.

#### *Lithuania*

Information about a person's identity is confirmed with a qualified electronic signature supported by a qualified certificate which conforms to the requirements of Regulation (EU) N° 910/2014. Qualified electronic signatures from third countries supported by a qualified certificate for electronic signature shall be recognised under Article 14 of Regulation (EU) No 910/2014.

#### *Finland*

Identification and identity verification performed by the post office: contracts and/or other documents can be sent as registered mail against acknowledgement of receipt, so that the customer collects the delivery personally. The post office delivers the acknowledgement of receipt to the supervised entity.

#### *Spain*

In Spain, identity confirmation between participants in the Spanish Electronic Clearing System (known in Spanish as SNCE). In the context of remote on boarding, firms which are participant in the Spanish Electronic Clearing System might request other participant which have business relationships with the customer in place to confirm identification data. This can only be used to meet formal identification requirement. *(For a complete list of specifications regarding procedures for identifying customers in remote transactions please refer to: Due diligence | Sepblac.)*

#### *Information Checked Against Registers:*

#### *Finland*

In non-face-to-face identification, identity verification may require a combination of several different methods and gathering additional information from the customer. If necessary, the information provided by the customer should be checked against information available in public registers, such as the Population Information System, Credit Information Register and Trade Register. For reliable customer identification, it is not necessarily sufficient that the supervised entity establishes that the funds have been transferred from an account in the credit institution.

#### *Belgium*

Belgian AML-Law (art. 28) also foresees that firms that have remotely on-boarded Belgian residents as customers, have the possibility to access the Belgian National Registry to carry out additional verifications regarding the identity of the customer. An e-ID card can also be used to verify the ID provided directly against the information in the Belgian National Registry.

## *Commercial Electronic Databases*

### *Malta*

Another electronic means of identity verification is through the use of commercial electronic databases, but in certain cases their use on their own is not considered sufficient as these can only serve to establish whether an individual actually exists – these databases do not allow the obliged entity to determine if the (prospective) customer is actually the individual he purports to be. Hence, additional measures are required to complete verification of identity.

Furthermore, not all commercial electronic databases can be used as there are a number of requirements, including:

- Recognition through registration with the data protection authorities of the country where it is set up to store personal data;
- Use of a range of positive information sources linking a (prospective) customer to both current and previous circumstances;
- Access to negative news information sources;
- Access to a wide range of alert data sources; and
- Transparent processes that enable the obliged entity to know what checks were carried out, what the results of these checks were and the level of certainty they provides as to the identity of the (prospective) customer.

In addition, the verification process should at least comprise verification from:

- One match from one source on (i) the individual's full name and (ii) current permanent residential address; and
- One match from another source on (i) the individual's full name and (ii) either his current permanent residential address or his date of birth.

It is also necessary that the commercial electronic database allows the obliged entity to capture and store the information used for verification purposes.

## *Counter Verification*

### *Sweden*

Counter verification of the identity using an alternative channel (not specified by the applicant) in order to counter identity spoofing. Firms should contact the physical person by sending a confirmation to that person's residential address or equivalent and credible information of address, or make sure that the person sends a certified copy of identification, or by other equivalent means.

## *JMLSG*

### *Evidence of Identity*

Evidence of identity can be obtained in a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photo card driving licenses, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation, including, in appropriate circumstances, written assurances from persons or organizations that have dealt with the customer for some time.

An increasing amount of data on individuals is held electronically/digitally, in various forms, and by various organizations. Like documents, sources of electronic information about individuals can, of course, vary in integrity and in reliability and independence in terms of their technology and content. Electronic databases, however, are becoming ever more sophisticated and widespread, and are likely to be increasingly used; firms should be satisfied that their choice of such sources meets the CDD test of reliability and independence.

In practical terms, for face-to-face verification, production of a valid passport or photo card driving license (so long as the photograph is in date) should enable most individuals to meet the identification requirement for AML/CTF purposes. The firm's risk-based procedures may dictate additional checks for the management of credit and fraud risk, or may restrict the use of certain options, e.g., restricting the acceptability of National Identity Cards in face-to-face business in the UK to cards issued only by EEA member states and Switzerland.

When using an electronic/digital source to verify a customer's identity, firms should ensure that they are able to demonstrate **that they have both verified that the customer exists, and satisfied themselves that the individual seeking the business relationship is, in fact, that customer (or beneficial owner).**

Electronic verification may be carried out by the firm either direct, using as its basis the customer's full name, address and date of birth, or through an organization which meets the defined criteria. It is important that the process of electronic verification meets an appropriate level of confirmation before it can be judged to satisfy the firm's legal obligation.

For verification purposes, a firm may approach an electronic/digital source of its own choosing, or the potential customer may elect to offer the firm access to an electronic/digital source that he/she has already registered with, and which has already accumulated verified evidence of identity, and which meets defined criteria.

Some electronic sources focus on using primary identity documents, sometimes using biometric data. Others accumulate corroborative information which in principle is separately available elsewhere. Some sources are independent of the customer, whilst others are under their 'control' in the sense that their approval is required for information to be included.

Commercial organizations that provide electronic verification of identity use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Some organizations confirm that a given, predetermined 'level' of authentication has been reached.

#### *Data Sources Accessible Online*

A number of commercial organizations which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such organizations use databases of both positive and negative information, and many also access high-risk alerts that utilize specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a PEPs or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

**Positive information** (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Some electronic sources or digital identity schemes specify criteria-driven levels of authentication that are established through the accumulation of specific pieces of identity information.

Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others where no such proof is required. The information maintained should be kept up to date, and the organisation's verification – or re-verification - of different aspects of it should not be older than an agreed period, set by the firm under its risk-based approach.

**Negative information** includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

#### *Management of the Risk of Impersonation Fraud*

Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non-face-to-face business, such as applications submitted by post, there are other factors that may, taken together, aggravate the typical risks:

- The ease of access to the facility, regardless of time and location;

- The ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
- The absence of physical documents; and
- The speed of electronic transactions.

#### *Remote Identification – Additional Verification Checks*

Where identity is verified electronically, copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms should consider:

- Verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or
- Requesting the applicant to confirm a secret code or PIN, or biometric factor that links him/her incontrovertibly to the claimed electronic/digital identity; or
- Requiring the first payment to be carried out through an account in the customer's name with a UK or UE regulated credit institution, or an assessed low risk jurisdiction; or
- Requiring copy documents to be certified by an appropriate person.

The source(s) of information used to verify that an individual exists may be different from those sources used to certify that the potential customer is in fact that individual.

### III. Additional Considerations

**Communications** must be secured e.g. through Transport Layer Security (TLS) or cryptographic protocols to guarantee authentication and integrity of transactions, as well as confidentiality. For example, for use of video in Hungary, the AML Act authorises the supervisory authority for financial institutions to determine detailed rules for the minimum requirements of the secure, protected electronic communications equipment and the method of auditing the equipment.

Furthermore, any use of **authoritative and third party sources**/databases to confirm an identity and/or an individual document should also be adequately protected in terms of confidentiality, integrity and availability. **Liability** models also need to be considered when using, and when assessing, a provider. Indeed, the amount of liability may reflect the confidence in the reliability of the system.

It is advised that a provider should have an effective counter-**fraud** policy and monitor false match rates for its product, considering a number of factors including age, gender and nationality. The provider should record and monitor all errors during a remote on-boarding process for the involved identity and deploy additional verifications when the case appears to be suspect (e.g. cumulative scoring mechanisms). Additionally, and where possible, localisation and MNO's (Mobile Network Operators) data should be taken into account. From an internal point of view a provider should implement segregation of duties so that one employee cannot be able to complete an identity registration process alone.

There are also **geographical risks** to consider, as noted in the EBA guidelines. Specifically, it notes that: the key feature of most commonly used innovative CDD solutions is that they enable firms to on-board customers remotely and verify their identity via the internet, regardless of customers' location or distance from the firm. This means that customers are no longer required to live in close proximity to firms to use their services, and do not have to be physically present for the identification purposes. Therefore it's important that firms have the ability to assess geographical risks presented by a business relationship, including through controls firms may have in place that capture their customers' location (e.g. through device fingerprinting or GPS data on mobile phones) to establish if they are based in a jurisdiction associated with higher ML/TF risks.

This also opens up an idea worth further exploration related to **specific device usage. Should all devices be accepted?** Are there specific types, or individual devices, that should be blacklisted? Conversely, should there be a so-called whitelist or certified product list? Would "rooted" devices be allowed? Etc.



Naturally, as per any process, adequate **governance** is required and there should be the ability to conduct relevant and suitable (and timely) audits, both internally and externally. JMLSG guidelines state that a commercial organization should have processes that allow the enquirer to capture and store the information they used to verify an identity.

## Certification

The Level of Assurance of remote identity registration solution should be assessed by a conformity assessment body (or equivalent) and solutions should be certified (e.g. ISO27001, or other certification to be considered).

## JMLSG

Before using a commercial organisation for electronic verification of identity, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate, and independent of the customer. This judgement may be assisted by considering whether the identity provider meets the following criteria:

- It is recognised, through registration with the Information Commissioner's office to store personal data;
- Unless it is on the Information Commissioner's list of credit reference agencies, it is accredited, or certified, to offer the identity verification service through a governmental industry or trade association process that involves meeting minimum published standards;
- It uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;
- It accesses negative information sources, such as data bases relating to identity fraud and deceased persons;
- It accesses a wide range of alert data bases;
- It published standards, or those of the schemes under which is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;
- Arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed, and
- It has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

## Risk Mitigation

### EBA

**Where innovative solutions are used to assess ML/ TF risks associated with a business relationship, are all available data and information used in this process, and are they considered reliable?**

To ensure that firms have developed a holistic view of the ML/TF risks presented by a particular business relationship, the ESAs believe that competent authorities should assess **whether or not data necessary to carry out the risk assessment are pulled from multiple reliable and independent sources**, which may be in different languages, and may include data from the customer's account profile and web login activity, government- or third-party-issued watch-lists, online news and publications, social media, and public databases.

**Is there a risk that a customer could be intimidated, threatened or under duress during the transmission of the identity verification?** In the ESAs view, firms should have strong controls a feature whereby a customer is required to have a live chat with an administrator who is well trained to spot any abnormalities in the customer's behaviour, in place to identify possible coercion, which may



include a built-in technical feature in the innovative solution or a feature whereby a customer is required to have a live chat with an administrator who is well trained to spot any abnormalities in the customer's behavior, which may assist in identifying situations where the customer is behaving suspiciously (e.g. psychological profiling).

## **RISK ASSESSMENT**

The Belgian AML Law does not impose specific measures to be taken by firms under supervision when they are on-boarding customers via a remote (non-face-to-face) distribution channel. The Belgian AML Law fully adheres to the risk based approach of AMLD4. Therefore, it is up to the firms to assess the risks related to each individual customer and to take appropriate measures to mitigate the identified risks. The individual risk assessment of a customer should include an assessment of the risks related to the distribution channel used for on-boarding the customer. In that regard, annex III to the Belgian AML-Law indicates that the use of a remote on-boarding channel should be considered by the firms as an indicator for a potential higher risk related to the business relationship.

## **AGREGATION OF SEVERAL MEANS:**

In non-face-to-face identifications, identity verification may require a combination of several different methods and gathering additional information from the customer. If necessary, the information provided by the customer should be checked against information available in public registers, such as the Population Information System, Credit Information Register and Trade Register. For reliable customer identification, it is not necessarily sufficient that the supervised entity establishes that the funds have been transferred from an account in the credit institution. (Finland)

*When electronic identification means are not used*, the identification is made on the basis of copies of identity documents and the carrying out of additional measures to cater for any risk arising from the remote nature of the business relationship. (Malta)

### **Alternative method in case of non use of electronic identification means, consisting in cumulative measures for verifying the identity (Sweden) :**

- collecting information regarding the person's name, address, social security number or equivalent,
- verifying the information above towards external registers, certificates, or other equivalent documentation, AND
- contact the physical person by sending a confirmation to that person's residential address or equivalent and credible information of address, or make sure that the person sends a certified copy of identification, or by other equivalent means

### **Risk based approach according to which one or several means should be used (Latvia)**

Remote identification possible outside three cases [ *the customer or the beneficial owner of the customer is a politically exposed person, a family member of the politically exposed person, or a person closely associated to the politically exposed person and uses a service the monthly credit turnover of which exceeds EUR 3000;*

*2) the customer is a shell arrangement;*

*3) the customer uses services of a private banker]* and managed under a risk approach (Latvia):

If the customer identification is performed without the participation of the customer in the onsite identification procedure in person, the subject of the Law shall implement one or several of the following measures, using the risk-assessment based approach:

- 1) obtain additional documents or information attesting to the customer's identity;
- 2) carry out verification of the additionally submitted documents or obtain confirmation of another credit institution or financial institution registered in the Member State attesting that the customer has a business relationship with this credit institution or financial institution, and the credit institution or financial institution has carried out the onsite customer identification;

- 3) ensure that the first payment within the scope of the business relationship is carried out through the account which has been opened in the customer's name at the credit institution to which the requirements for the prevention of money laundering and terrorism financing requirements arising from this Law and the legal acts of the European Union apply;
- 4) request personal presence of the customer in the execution of the first transaction;
- 5) if the customer is a natural person - resident -, obtain information attesting to the customer's identity from the document which the customer has signed with a secure electronic signature.

### **Combination of several means of different natures (Spain)**

#### **1 among the following determined by law**

a) customer's identity is evidenced in accordance with the provisions of applicable regulations on electronic signature; b) the first deposit comes from an account in the customer's name at an entity domiciled in Spain, in the European Union or in equivalent third countries; or c) some of the requirements foreseen in Regulations are verified.

**and in addition one of:** a) The customer's identity is evidenced in accordance with the provisions of applicable regulations on electronic signatures; b) The customer's identity is evidenced by means of a copy of the relevant identity document, provided that the copy is issued by a notary public; c) The first deposit comes from an account in the customer's name at an entity domiciled in Spain, in the European Union or in equivalent third countries; or d) The customer's identity is evidenced by other secure procedures for customer identification in remote transactions, provided that such procedures have been previously authorised by Sepblac (Identity confirmation between participants in the Spanish Electronic Clearing System; Video conference; video identification).

### **USE OF COMMERCIAL ELECTRONIC DATABASES IN ADDITION TO IDENTIFICATION MEASURES**

Another electronic means of identity verification is through the use of commercial electronic databases **BUT** in this case their use on their own is not considered sufficient as these can only serve to establish whether an individual actually exists – these databases do not allow the obliged entity to determine if the (prospective) customer is actually the individual he purports to be. Hence, additional measures are required to complete verification of identity.(Malta)

**DEPORT ON THE IDENTIFICATION MADE BY A THIRD PARTY:** *Bank transfer, Post acknowledgment of receipt.*

## **JMLSG**

### **Risk analysis**

The extent of verification in respect of non-face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in itself increase the risk attaching to the transaction or activity. A firm should take account of such cases in developing their systems and procedures.

### **Additional verification checks**

Where identity is verified electronically, copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms should consider:

Verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or

Requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs or other secret data may be set up within the electronic/digital identity, or may be supplied to a verified mobile phone, or through a verified bank account, on a one-time basis, or as follows:

The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

Requiring the first payment to be carried out through an account in the customer's name with a UK or UE regulated credit institution, or an assessed low risk jurisdiction;

Verifying additional aspects of the customer's identity:

Telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before the transactions are permitted, using it to verify additional aspects of personal identity information that have been previously verified during the setting up of the account;


Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);

Internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;


Other card or account activation procedures.


**Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact.** It is therefore important to be clear on the appropriate approach in these circumstances


Annex 4: Existing EU Member states' AML regulations on remote on-boarding journeys

Countries	Remote on-boarding journeys	Regulation	Examples of Banks	Examples of Service/product providers	Customer Acceptance <sup>64</sup> (three degrees of acceptance : low, medium, high)
 Austria	Automatic transfer data from the id document to the relevant form + Video identification	<p>Identification through video-chat has been approved by the Austrian Financial Market Authority (FMA) on 3 January 2017</p> <p>There are provisions in the national AML/CFT law regarding the customer on-boarding process, which foresee certain requirements that have to be fulfilled in order to be compliant with the AML/CFT regulations. The Austrian national AML/CFT law (Financial Market Anti-Money Laundering Act) stipulates four different options for non-face-to-face customer on-boarding procedures: 1) video identification (specified by a FMA-regulation); 2) electronic signature/registered mail; 3) e-identity pursuant to EU Directive Nr. 910/2014; 4) first payment is through an already identified account (where the customer was identified in the means of the 4AMLD).</p>	<p>ERSTE GROUP</p> <p>Various banks in Austria use video identification. The Austrian FMA collects data about banks using video identification in its risk analysis tool and therefore keeps a list containing information whether a bank is using video identification and if yes, which provider is used.</p>	<p>IDnow, WebID, CRIF, Austrian Post, A-Trust</p>	<p>1. Video identification: Customer acceptance is medium</p> <p>2. Qualified electronic signatures (eIDAS): Customer acceptance is low</p> <p>3. eID of Austrian citizen card and eIDs notified under eIDAS fulfilling certain criteria:</p>

<sup>64</sup> Input provided by Expert Group members working for the European Banking Federation (EBF)


					Customer acceptance low
 Belgium	<p>Customer ID should be verified against one or more supporting documents or reliable and independent sources of information which enable obliged entities to confirm this data, in order to have a sufficient degree of certainty that they know the persons concerned (art. 27, § 1, Belgian AML Law).</p> <p>Within these boundaries, all types of remote on-boarding are possible (E-id, video verification, etc.).</p>	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT</p> <p>The Belgian AML Law does not impose specific measures to be taken by firms under supervision when they are on-boarding customers via a remote (non-face-to-face) distribution channel. The Belgian AML Law fully adheres to the risk based approach of AMLD4. Therefore, it is up to the firms to assess the risks related to each individual customer and to take appropriate measures to mitigate the identified risks. The individual risk assessment of a customer should include an assessment of the risks related to the distribution channel used for on-boarding the customer. In that regard, annex III to the Belgian AML-Law indicates that the use of a remote on-boarding channel should be considered by the firms as an indicator for a potential higher risk related to the business relationship.</p> <p>When a firm concludes that a business relationship represents a higher risk, art. 27, § 4, of the Belgian AML Law states that particular attention should be given to the verification of the ID of the customer (enhanced CDD measures). In that regard, the Belgian AML-Law (art. 28) also foresees that firms that have remotely on-boarded Belgian residents as customers, have the possibility to access the Belgian National Registry to carry out additional verifications regarding the identity of the customer. An E-id card can also be used to verify the ID provided directly against the information in the Belgian National Registry.</p> <p>Finally, it is also worth noting that the Belgian NBB AML Regulation stipulates that for the purposes of verification of identity, a specific identification technology may be accepted as a supporting document or reliable and independent source of information within the meaning of the Belgian AML Law, if an analysis of the reliability of this technology so justifies (in this regard, Belgian firms should also take into account the ESAs Opinion on the use of innovative solutions in the customer due diligence process).</p>	<p>The aforementioned goes for all banks (and other financial institutions).</p>	<p>ItsMe is (electronic identification mean pre-notified Level Substantial/High) proposed by banks. A link is made by the customer's previous bank between the national ID card. ItsMe is sufficient for remote onboarding identification. If not used, the applicant has to send a copy of his ID card and checks are made by the bank towards the</p>	<p>Few people directly use the national ID card, due to the need of a reader.</p> <p>Video identification solutions (Implicitly permitted by Supervisory authorities as "Innovative solutions") are not used as customers prefer to use It's Me.</p> <p>ItsMe is convenient. Used by young people. General acceptance for ItsMe is medium.</p>


				national register.	
 Bulgaria	Remote on-boarding, based on qualified trust service	<p>The method of remote electronic identification based on a trust service is regulated on a pan-European level. It was introduced by the 5<sup>th</sup> AML Directive as an allowed method for remote identification for financial services. The Member States must implement the Directive by 10<sup>th</sup> of January 2020. Bulgaria is already compliant with eIDAS and the trust service is provided by a registered trust service provider (e.g. EvroTrust). The method is compliant with PSD2, since it is based on multi-factor strong authentication and is in line with GDPR and with rules for protection of consumers.</p> <p>The method EvroTrust relies on:</p> <ol style="list-style-type: none"> <li>1. National ID documents – checked for validity from technological controls and checked in a national reliable sources (register for national ID documents, population register, commercial register, etc.);</li> <li>2. Biometrical and 3D liveness check are made automatically, which makes the on-boarding below 1 minute;</li> <li>3. The method for identification to obtain qualified trust service certificate is certified for eIDAS compliance by conformity assessment auditors and giving same assurance as to a physical presence according to Art. 24 (1) (d) eIDAS;</li> <li>4. The method does not only identifies the client remotely, but also complete the onboarding by initiating and signing relevant contracts, GTC, declarations, etc., by a qualified e-signature, and securing basic KYC controls;</li> <li>5. The time of the identification &amp; signatures is attested by a qualified time stamp;</li> <li>6. The liability for wrong identification/signing is borne by Evrotrust as a trust service provider according to eIDAS. The liability is insured;</li> <li>7. The solution provide for complete digital transformation, since it also integrates a qualified electronic delivery service and creates legally binding proofs of evidence for the delivery of identification/signed documents;</li> <li>8. The supervision is always performed as a second level of control for all identifications.</li> </ol>	Raiffeisenbank Bulgaria, ProCredit Bank Bulgaria, UniCredit Bulbank (Bulgaria) TrustChain (Hungary)	Evrotrust	

		The method is used for completely remote opening of bank accounts, loan origination, credit cards issuance, etc.			
 Czech Republic	Electronic identification under eIDAS, reliance on third parties, verification via a first payment	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT</p> <p>The AML/CFT Act enables the following ways to undertake identification without the physical presence of a customer:</p> <ol style="list-style-type: none"> <li>1. via reliance on a third party which is also an obliged entity,</li> <li>2. via reliance on identification undertaken by a public administration office,</li> <li>3. via a provider of services pursuant to the eIDAS regulation and</li> <li>4. via remote identification when specific conditions are fulfilled: <ul style="list-style-type: none"> <li>- the customer provides copies of two identification documents,</li> <li>- the customer provides a proof of existence of an account with an EU credit institution</li> <li>- the first payment is made through the above-mentioned account.</li> </ul> </li> </ol> <p>Nevertheless, on boarding journeys may include a static selfie together with ID document (picture or future client with ID, to serve as safeguard in case of questioning of client identification</p>	Czech National Bank Komerční Banka	<b>Use of remote onboarding based on verification of the identity of the client by the qualified trust service provider.</b> (Bank may identify a customer who is a natural person or a natural person acting on behalf of a customer which is a legal person without his/her physical presence, if: <ol style="list-style-type: none"> <li>a) the customer provides the Bank with his/her</li> </ol>	Regarding remote onboarding based on verification of the identity of the client by the qualified trust service provider, customer acceptance is low.



				identification and additional data requested by the law for identification b) the Bank verifies the identity of the relevant natural person with a qualified trust service provider under directly applicable European Union regulation regulating electronic identification and trust services for electronic transactions within the internal market and c) the obliged entity has no doubts about the	
--	--	--	--	--	--

				real identity of the customer.)	
 Denmark	Denmark has since 2010 an eID system called NemID, which is a public-private partnership between the public sector (Ministry of the Interior) and the banks. NemID is issued to all individuals above the age of 15 who have a Danish Civil Registration Number (“CPR number”).	Due to security level not considered as secured enough, in a CDD process the sole use of NemID as an identification mean is insufficient. Here the undertaking requires further verification sources relating to the customer unless the customer relationship is considered to be low risk.  A new solution should exist and be notified in 2021.  Existing remote on boarding processes rely on the national eID (NemID) supplemented by an upload of a copy of passport or driver’s license, or national health insurance card. An electronic signing using NemID chip is proceeded.	Some banks can issue NemID to their customer		Customer acceptance to this on boarding way is high.

 Estonia	E-resident cards ID card and Mobile ID Video identification (can be completed with biometrics)	<p>Allow Estonian residents and also e-residents to open a bank account without having to go to a bank branch.</p> <p>On June 15<sup>th</sup> 2016 the Parliament of Estonia introduced changes in the current legislation, making it easier to open a bank account in Estonia without visiting a bank branch. It is a welcome and anticipated change as the main obstruction keeping e-residents from doing business in Estonia, has been just that.</p> <p>Currently, the identification of persons participating in a transaction or using a service must be performed while the person or their representative is in the same place with the bank representative. Under the new amendment identification by means of information technology solutions will be equivalent to in person identification.</p> <p>The goal of the amendment is to make becoming an e-resident easier, make using e-services user-friendlier and offer e-residents and Estonian residents the opportunity to open a bank account without the need to visit the bank office.</p> <p>The changes are equally beneficial for non-residents and Estonians who live and work abroad. The service is meant for any holder of the Estonian ID, digi-ID, or e-resident's card.</p> <p>The banks' right to choose and limits</p> <p>The banks' reserve the right to decide whether they accept the application of e-residents. The credit and financial institutions also reserve the right to not provide any services or only provide them with limited service capacity.</p> <p>Due to the fact the identification is done by info technological facilities, the legislation has set following conditions:</p> <p>The total amount of payments in one calendar month cannot exceed €10,000 for a natural person and €25,000 for a legal person.</p> <p>Banks have the obligation to cancel the long-term contract without providing the advance notice of the expiry of the term if:</p> <p>The person does not appear at a place of residence or permanent establishment despite repeated requests.</p> <p>The application for the e-residency permit is declined, it's validity is stopped or it becomes invalid.</p>	<p>The e-Resident smart ID card is approved by <u>LHV</u>, <u>Swedbank</u> and <u>SEB</u> banks.</p> <p>Traditional journey for e-resident consist of:</p> <p>E-resident id provides with a physical smart card (digital-ID), which will allow them use of Estonian public and private services online. Once applied for e-Residency and received one's e-Resident ID card, the applicant visits a local bank office. The e-Residency does not guarantee a bank account. The decision to approve/deny banking services to an e-resident is made at the sole</p>		
--	--	---	---	--	--


		<p>The amendment to the Money Laundering and Terrorist Financing Prevention Act (Applicable since October 25<sup>th</sup> 2016) implies that banks will be able to replace the requirement of the applicant being present in person with a person identification process consisting of three stages. Namely, an information technology solution will be used for interviewing the person, and the interview will be saved. To identify the person, the document issued in Estonia for digital person identification, the personal identification document issued by a foreign state and the person's identification data entered in the database of personal identification documents will be used. Additionally, the bank will have to further enhance its measures for the prevention of money laundering.</p> <p>Technical conditions for the video, i.e. will the video identification be just as secure as visiting a bank in person?</p> <p>Authentication by information technology is equivalent to verifying the identity of a customer face to face. In both cases, the "know your customer" requirements must be fulfilled, and the person wishing to become a customer must fill in a form and respond to questions from the bank in the form of a direct interview. Authentication using an IT tool allows the bank to perform database queries simultaneously with the authentication process, using face recognition software if desired. Insofar as a recording is made of the authentication process, the bank can review the process later if needed. Authentication using an IT tool, the quality of information stream and information system itself are subject to requirements established by a Minister of Finance regulation.</p> <p>On 25<sup>th</sup> of October the Minister of Finance regulation (which determines the precise requirements and rules regarding opening a bank account without going to a bank office by using a real-time video bridge. The regulation is to come into force on Oct. 31. The video bridge enables to check the applicant's facial features against the photo on the ID and in the database of the Police and Border Guard Board may be used for identification and verification of identity. The bank representative will also conduct an interview with the applicant to determine his risk profile (background, origin of assets, purpose of establishing a business relationship). The whole process will be recorded and the recording archived.</p> <p>If the applicant is a foreign national, it is acceptable to provide an ID (passport, driver's license) issued by the country along with the digital e-residency identification.</p>	<p>and absolute discretion of the bank.</p> <p>The e-Resident smart ID card is approved by <u>LHV</u>, <u>Swedbank</u> and <u>SEB</u> banks. For compliance reasons, opening a bank account today required a face-to-face meeting. From 2016, it is possible for banks to permit the opening of an Estonian bank account from abroad.</p> <p>Steps for opening a bank account:</p> <p>Visit a bank in Estonia.</p> <p>Submitting an application for a new account, and wait for approval.</p> <p>Upon approval, digitally signing the contract with the e-Resident card and returning via e-mail to the bank.</p> <p>Eligibility to open an online payment</p>		
--	--	---	--	--	--

		<p>However, banks will retain the right to identify a person by being at the same location as them.</p> <p>Estonian Money Laundering and Terrorist Financing Prevention Act  § 31. <i>Identification of person and verification of data using information technology means</i>  (1) <i>A credit institution and a financial institution must identify a person and verify data with the help of information technology means where a business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country and where the due diligence measures are not applied while being physically in the same place as the person or their representative.</i>  (2) <i>A credit institution and a financial institution must identify a person and verify data with the help of information technology means where a business relationship is established with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month, and where the due diligence measures are not applied while being physically in the same place as the person or their representative.</i>  (3) <i>A document issued by the Republic of Estonia for digital identification of a person or another electronic identification system with assurance level 'high' which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114) is used for identification of a person and verification of data with the help of information technology means.</i>  (4) <i>Where a person is a foreign national, the identity document issued by the competent authority of the foreign country must be used for the identification of the person and verification of data in addition to the means specified in subsection 3 of this section.</i>  (5) <i>Additionally, information originating from a credible and independent source is used for identifying a person and verifying data. To identify an e-resident and verify data, a credit institution and a financial institution has the</i></p>	<p>service provider account.</p>		
--	--	---	----------------------------------	--	--


		<p>right to use personal identification data entered in the database of identity documents.</p> <p>(6) The technical requirements of and procedure for identification of persons and verification of data using information technology means are established by a regulation of the minister responsible for the field.</p> <p>(7) The regulation specified in subsection 6 of this section sets out in greater detail at least requirements for disclosure of information, rules of procedure applicable to the establishment of a business relationship and to the making of an occasional transaction, requirements for activities related to the declarations of intent of the parties to a transaction, organisation of questionnaire surveys and mandatory real-time interviews held upon establishment of a business relationship, conditions of processing of the photograph of a person, and requirements for the quality of the synchronised audio and video stream during the aforementioned procedures as well as for recording and for the reproducibility of recordings, and, based on the national risk assessment specified in § 11 of this Act, the regulation may establish limits different from the ones specified in subsection 2 of this section to situations where the provisions of this section do not need to be applied.</p> <p>See Requirements and procedure for identification of persons and verification of persons' identity with information technology means Passed 21.10.2016 Annex 48:  <a href="https://www.riigiteataja.ee/en/eli/ee/RHM/reg/504112016001/consolide">https://www.riigiteataja.ee/en/eli/ee/RHM/reg/504112016001/consolide</a></p> <p>Identity Documents Act  Passed 15.02.1999  RT I 1999, 25, 365  Entry into force 01.01.2000  <a href="https://www.riigiteataja.ee/en/eli/504112013003/consolide">https://www.riigiteataja.ee/en/eli/504112013003/consolide</a></p> <p>According to the amendments of the Money Laundering and Terrorist Financing Prevention Act which endorsed the provision of 4.AMLD (Entry into force 27.11.2017, partially 01.01.2018) remote on-boarding of customers is possible in certain circumstances using two main solutions:</p> <p>(i.1) Identification of natural by means of electronic identification and trust services for electronic transactions (Estonian ID-card, or E-resident's card.</p>			
--	--	---	--	--	--

		<p>Beside ID-card the Mobile-ID, and Smart-ID can be used for making the same procedures as with an ID card). Then identifying person by means of electronic identification and trust services for electronic transactions the identification data should be verified by using at least two different sources;</p> <p>(i.2) Identification of legal person by using information originating from a credible and independent source. Where the obliged entity has access to the commercial register, register of non-profit associations and foundations or the data of the relevant registers of a foreign country, the submission of the documents relevant for the identification is not obligatory. The identity of legal person could be verified based on documents, which has been authenticated by a notary or certified by a notary, or officially, or based on other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions. The identification data should be verified by using at least two different sources in such an event.</p> <p>Measures as provided in (i.1) and (i.2) cannot be applied then total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month.</p> <p>(ii) A credit institution and a financial institution must identify a person and verify data on a face-to face basis or with the help of information technology means (the video identification) when:  a total sum of outgoing payments exceeds above mentioned thresholds; or  Business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country and where the due diligence measures are not applied while being physically in the same place as the person or their representative.</p> <p>The technical requirements of and procedure for identification of persons and verification of data using information technology means are established by a regulation, available:  <a href="https://www.riigiteataja.ee/en/eli/509012019003/consolide">https://www.riigiteataja.ee/en/eli/509012019003/consolide</a></p>			
--	--	--	--	--	--




 Finland	<p>Bank ID, mobile ID, national ID card</p> <p>Also other remote onboarding journeys are possible depending on their implementation (case-by-case evaluation)</p>	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT          Act on Preventing Money Laundering and Terrorist Financing, 444/2017, Section 11</p> <p><i>Enhanced customer due diligence related to non-face-to-face identification</i>  <i>If the customer is not physically present when he or she is identified and his or her identity verified (non-face-to-face identification), obliged entities shall take the following measures to reduce the risk of money laundering and terrorist financing:</i></p> <p>1) <i>verify the customer's identity on the basis of additional documents, data or information obtained from a reliable source;</i>          2) <i>ensure that the payment relating to the transaction is made from a credit institution's account or into the account that was opened earlier in the customer's name; or</i>          3) <i>verify the customer's identity by means of an identification device referred to in the Act on Strong Electronic Identification and Electronic Signatures (617/2009) or a qualified certificate for electronic signature as provided in Article 28 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 and repealing Directive 1999/93/EC or other secure and verifiable electronic identification technology.</i></p> <p>FIN-FSA Regulation on Customer due diligence; Prevention of money laundering and terrorist financing</p> <p><i>(46) In non-face-to-face identifications, identity verification may require a combination of several different methods and gathering additional information from the customer. If necessary, the information provided by the customer should be checked against information available in public registers, such as the Population Information System, Credit Information Register and Trade Register. For reliable customer identification, it is not necessarily sufficient that the supervised entity establishes that the funds have been transferred from an account in the credit institution.</i></p> <p><i>(47) A party that offers the service of strong electronic identification as referred to in the Identification Act should notify the register of the Finnish Communications Regulatory Authority and comply with the authority's regulations.<sup>37</sup> Section 17 of the Identification Act includes provisions on initial identification of an applicant for a strong electronic identification device. The applicant for such an identification device should be identified in person in</i></p>	<p>- OP Bank and Nordea Bank enable the opening of bank accounts via remote onboarding, if other banks' bank ID's are used for electronic identification</p>	<p>Use of a bank ID promoted by the banks.</p>	
--	---	--	--	--	--

		<p>connection with its first application for identification device as referred to in the Identification Act.</p> <p>(48) Identification and identity verification of, and delivery of identifier (access codes) to, applicants other than those applying for strong electronic identification device as referred to in the Identification Act should also be performed with due diligence, preferably in person. Alternatively the supervised entity may use registered letters and acknowledgements of receipt, in which case the applicant collects the identifiers from the post office. When neither the supervised entity nor any other party meets the customer face-to-face. Instead the customer identification can be based on:  a qualified certificate or strong electronic identification device as referred to in the Identification Act  identification and identity verification performed by the post office: contracts and/or other documents can be sent as registered mail against acknowledgement of receipt, so that the customer collects the delivery personally. The post office delivers the acknowledgement of receipt to the supervised entity.</p>			
--	--	--	--	--	--

	Video identification + biometry	See Video identification	Société Générale	IDEMIA	
 France	Electronic signature	<p>See article R. 561-20 6° of the Monetary and Financial Code:</p> <p><i>Collect an advanced or qualified electronic signature or valid advanced or qualified electronic seal based on a qualified certificate containing the identity of the signatory or seal creator and issued by a qualified trusted service provider registered on a national trust list in application of Article 22 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.</i></p> <p>But such an electronic signature is not sufficient and has to be completed with one other measure foreseen in R521-20 Code monétaire et financier. SEE UNDER Electronic identity.</p>	BNP Paribas Banque Populaire Caisse d'Epargne Caixa Bank Société Générale	IDEMIA	In most journeys banks act as registry authorities, by customers identifying, for the account of trust services providers, those delivering electronic certificates for electronic signatures. As the process is easy to use, depending on the weight of documentation to be signed, customer acceptance is good (medium).

<p>ID Documents checks</p>	<p>Check of documents=&gt; R561-20 Monetary and Financial Code regarding AML stipulates:</p> <p><i>For the purposes of 1 ° of Article L. 561-10, and where the measures provided for in 1 ° and 2 ° of R. 561-5-1 cannot be implemented, the persons mentioned in Article L. 561-2 verify the identity of their client by applying at least two of the following:</i></p> <p>1 ° <i>Obtain a copy of a document mentioned in 3 ° to 5 ° of article R. 561-5-1 as well as an additional supporting document to confirm the client's identity;</i></p> <p>2 ° <i>Implement measures of verification and certification of the copy of an official document or an official register extract mentioned in 3 ° to 5 ° of Article R. 561-5-1 by an independent third party the person to identify.</i></p> <p>(Not written in the regulation, but provided this third party reaches reliability level.)</p>	<p>HSBC</p>	<p>HoneyTrust</p>	
<p>Video identification / Video conference</p>	<p>No regulation governs video identification. It does not constitute as such an eIDAS scheme, neither does it fall within ACPR (Banking Authority) remit due to its technical feature.</p>			<p>Video identification as it is more convenient than video conference, seems to be more appreciated by customers, than video conference. It is faster, there is no need of appointment or to make the journey at office time.</p>

	Electronic identity	<p>Either a notified electronic identification mean level high (sufficient) or a French national electronic identification mean level high (sufficient) see R. 561-5-1 or a notified electronic identity level substantial (to be completed with another AML measure (R561-20 of the Monetary and Financial Code, 5) among the following:</p> <p>1°) an identity document and a further document proving the identity; 2°) a verification and certification of the copy of the identity document or register from a third independent from the person who is to be identified; 3°) a credit or debit wire transfer from or to an account opened to the customer in the European Union; 4°) an identity certification issued from another bank; 5°) a substantial level eIDAS electronic identity; 6°) a qualified eIDAS signature or an advanced signature relying on a qualified eIDAS certificate.</p>		<p>The only existing electronic identification means are for the time being Level low and cannot be sufficient. One bank already uses them as a way of directly collecting electronic information (though France Connect node).</p>	<p>Customers seem to be interested in use of France Connect even for bank on boarding journeys.</p>
--	---------------------	--	--	---	---

 Germany	Video identification	BaFin Circular 3/2017 (GW) - video identification procedures: considering identification by video chat is comparable with face to face. This video identification needs to be made in a form of a real time interaction with a human being. German regulator does not allow an automated video.  <a href="https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html">https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html</a> . If the service provider meets these conditions, the identification is valid as if the identified person is present.	Hanseatic Bank Credit Plus Bank Deutsche Bank Postbank Targo bank Varengold Noris bank N26 Commerzbank	WebID Largely proposed by banks. Can be proposed everywhere, provided that it is equivalent to a face to face, and fulfils BAFIN requirements.	High customer acceptance.
	Cross channel (face to identification)	General AML regulation regarding face to face.	N26	PostIdent	
	Video identification + biometry	There is no specific regulation. It relies on Bafin Circular regarding video identification procedures. See above.	N26  Commerzbank	IDnow PostIdent	


	Electronic identity	<p>There are two use cases for Deutsche Bank customers to use electronic IDs:</p> <p>1. Existing Deutsche Bank customers can link their Verimi account to the Deutsche Bank Online-Banking for a convenient and secured Log On the bank website.</p> <p>2. Additionally, data fields like IBAN, address and phone number can be uploaded to the Verimi account to prefill data fields of other Verimi partners.</p> <p>The reuse of identifications currently is accepted by the German Federal Supervisory Authority, subject to certain conditions and it is likely that the conditions will be clarified in the German AML Act after the implementation of the AMLD5.</p> <p>.For electronic identity card =&gt; Cf. section 12 para 1 no. 2 of the German Anti-Money Laundering Act (Geldwäschegesetz – GwG)</p>		National ID card	
--	---------------------	--	--	------------------	--






		<p><a href="https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586">https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586</a></p>		<p>Verimi is only supported by banks. Verimi needs a payment service provider licence to be re-used and considered as an identification for the account of another bank. Otherwise, the transmitting bank will have to identify the person again. Transmission to a second bank is subject to conditions:</p> <p>The bank is able to use the digital identity for an account</p>	
--	--	--	--	--	--

				<p>opening process if several criteria are met, e.g.: (i) the underlying ID is still valid, (ii) the eID has been set up with Verimi in the last 24 months, (iii) the underlying documents (i.e. source data video files) are distributed as well, and (iv) the communication is handled via secure channels including a 2FA authentication together with an authorization from the client. It is currently not possible</p>	
--	--	--	--	--	--

				<p>under German law the re-use in a 3-party-scenario, i.e. bank A generates the digital identity, sends it based on customer consent to an identity platform (e.g. Verimi) and Verimi distributes this identity to bank b (based on customer consent).</p>	
--	--	--	--	--	--


	eIDAS-qualified electronic signature	Cf. section 12 para 1 no. 3 of the German Anti-Money Laundering Act (Geldwäschegesetz – GwG) <a href="https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586">https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586</a>	-various credit institutions and other obliged entities		
	ID Documents checks	Cf. section 12 para 1 no. 1 or no. 5 of the German Anti-Money Laundering Act (Geldwäschegesetz – GwG) <a href="https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586">https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.html?nn=8356586</a>		PostIdent	
 Greece	<b>1. Electronic signature</b> (e.g. qualified or advanced signature) for consumers and enterprises, according to eIDAS.	Electronic signature service providers should be regulated in any one of the EU Member States, but should not be required to register and be approved in each EU Member State individually.			Customer acceptance is high regarding enterprises and low regarding consumers.
	<b>2. Innovative solutions in the customer due diligence process</b>	<p>During the 1st semester of 2019, it is expected that Bank of Greece (i.e. national central bank) will adopt and subsequently publish a new delegated act, which will incorporate and specify in detail the provisions of AMLD4 and AMLD5. This act will also contain provisions that will allow credit institutions and other market players to design and use innovative digital on-boarding solutions for the identification of their clientele (consumers and enterprises). Such innovative KYC solutions may include (but not be limited to) videoidentification and biometrics processes via multiple channels, such as: smartphones, websites and ATMs with camera integration.</p> <p>It should be noted that for this particular topic, the following legal acts have been published:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC and</li> <li><input type="checkbox"/> Opinion of the ESAs Joint Committee on the use of innovative solutions in the customer due diligence process.</li> </ul>			(A medium customer acceptance is expected.)
	<b>3. New biometric ID cards</b>	Until 2020, all existing ID cards of Greek citizens will be replaced by new ones that will include biometric data, fingerprints and facial images. This development is expected to facilitate the digital on-boarding process in relation to consumers.			(A high customer acceptance is expected.)

 Hungary	Video Identification	<p>According to the Hungarian AML Act, service providers may perform the CDD requirements via a secure, protected electronic communications equipment operated by the service provider preliminarily audited in the manner specified by the supervisory body.</p> <p>The AML Act authorises the MNB (as the supervisory authority for financial institutions) to determine detailed rules for the minimum requirements of the secure, protected electronic communications equipment and the method of auditing the equipment.</p> <p>The MNB Decree no. 19/2017 (VII.19) created the possibility and elaborated the details of the real-time video identification.</p> <p>The MNB Decree no. 45/2018 (XII.17) further sophisticated the possibilities of identification. Besides the already-existing real-time video identification, it created the possibility of identification via the comparison of the ID photo with the face of the customer. This method can only be used in cases of low-risk customers (the low risk cases are determined in the Decree).</p>	OTP Bank; Gránit Bank; Takarék Kereskedelmi Bank; Cofidis Bank; MKB Bank.		Medium customer acceptance
 Ireland	Not specifically addressed in AML legislation in Ireland	<p>The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, (as amended) (the “Act”), Ireland’s primary piece of anti-money laundering legislation has been drafted in a technology neutral manner. A designated person (obliged entity) is not prohibited from using technological solutions in order to meet their AML/CFT obligations under the Act. When undertaking the identification and verification of customers and beneficial owners, Section 33 (2) (a) of the Act requires <i>“identifying the customer, and verifying the customer’s identity on the basis of documents (whether or not in electronic form), or information, that the designated person has reasonable grounds to believe can be relied upon to confirm the identity of the customer, including –</i></p> <p><i>documents from a government source (whether or not a State government source), or</i></p> <p><i>any prescribed class of documents, or any prescribed combination of classes of documents”.</i></p> <p>Furthermore, Section 33 (3) of the Act qualifies the requirement by stating: <i>“Nothing in subsection (2)(a)(i) or (ii) limits the kinds of documents or</i></p>	KBC Bank Ireland plc	No National e-id scheme.  Banks are working together to explore a bank led e-id scheme.  Some banks use video onboarding for certain customers.	

		<p><i>information that a designated person may have reasonable grounds to believe can be relied upon to confirm the identity of a customer.”</i></p> <p>As can be seen from the legislative provisions under the Act, there is no legal impediment under AML legislation in Ireland preventing a designated person from accepting any form of document to identify or verify a customer or beneficial owner as long as the designated person has reasonable grounds to believe that it can be relied upon.</p>			
 Italy	<ol style="list-style-type: none"> <li>1. Video conference</li> <li>2. (Video identification and biometrics or other technology solutions)</li> <li>3. eIDAS electronic signature and digital identity</li> <li>4. Information from</li> </ol>	<p>According to article 19 of the Italian AML Law (i.e. legislative decree 231/2007, as modified by legislative decree 90/2017 which implemented directive 849/2015), obliged entities can identify customers remotely provided that some conditions are met. These conditions are listed by the law itself (for instance, according to the law, customers can be identified remotely where they are endowed with high LOA digital identity) or by the implementing regulations on CDD issued by Banca d'Italia (BOI) or IVASS.</p> <p>More in detail, BOI's Regulation on CDD (i.e. "<i>Disposizioni in materia di adeguata verifica della clientela</i>" adopted on July 30<sup>th</sup> 2019) lays down specific rules for the video-conference procedure (a real-time process) applicable in case the customer is a natural persons. This procedure - mirroring the video conference procedure that identity providers have to follow in compliance with the Italian Authority responsible for the electronic identification scheme (Agency for Digital Italy- AGID) instructions - is assumed to be secure. Therefore financial institutions can identify and verify their customers following this procedure without the need of carrying out further specific analysis of its robustness and its potential weaknesses.</p> <p>Out of this case, according to the BOI Regulation on CDD, firms are allowed to on-board customers via a remote (non-face-to-face) distribution channel provided that the following conditions are met:</p>	Few uses in Italy for the time being.		

	third parties	<p>1. the firm has identified - in a document to be approved by the board members – the specific identity verification tools it intends to use to identify customers remotely; the document has to illustrate the risk analysis carried out by the firm on the advantages and the weaknesses of each single tool to be used;</p> <p>2. the firm has assessed the risks related to each individual customer and has taken appropriate measures to mitigate the identified risks.</p> <p>Provided that these conditions are met, firms are entitled to use other innovative solutions to identify and verify their customers, including non-live video chat and biometric tools.</p>			
--	---------------	--	--	--	--




 Latvia	Video identification/ secure electronic signature/ other technological solutions (acquisition of data accrediting the identity of a natural person from a credit	Remote identification is allowed according to the Law on the Prevention of Money Laundering and Terrorism Financing. On July 3, 2018 the government adopted the Regulation providing more detailed regulation for remote identification procedures. The Regulation defines which are the situations when the remote identification is not allowed, defines rights and obligations of the institution regarding the remote identification of a customer, performance of video identification and use of technological solutions in the remote identification of a customer (see link below).  Law on the Prevention of Money Laundering and Terrorism Financing <i>Section 22. Enhanced Customer Due Diligence</i>	<b>1. Video identification</b>  The regulation establishes how a video identification must be performed.		Acceptance medium for video identification.
---	---	--	--	--	---

	<p>institution payment institution) or</p>	<p>[..]  <i>(2) The subject of the Law shall apply enhanced customer due diligence in the following cases:</i>  <i>1) upon establishing and maintaining a business relationship or executing an occasional transaction with a customer who has not participated in the onsite identification procedure in person, except in the case when the following conditions are fulfilled:</i>  [..  <i>b) the customer identification, by means of technological solutions including video identification or secure electronic signature, or other technological solutions, is being performed to the extent and in accordance with the procedures stipulated by the Cabinet;</i>  [..  <i>Section 23. Non-participation of the Customer in the Onsite Identification Procedure in Person</i>  <i>(1) If the customer identification is performed without the participation of the customer in the onsite identification procedure in person, the subject of the Law shall implement one or several of the following measures, using the risk-assessment based approach:</i>  <i>1) obtain additional documents or information attesting to the customer's identity;</i>  <i>2) carry out verification of the additionally submitted documents or obtain confirmation of another credit institution or financial institution registered in the Member State attesting that the customer has a business relationship with this credit institution or financial institution, and the credit institution or financial institution has carried out the onsite customer identification;</i>  <i>3) ensure that the first payment within the scope of the business relationship is carried out through the account which has been opened in the customer's name at the credit institution to which the requirements for the prevention of money laundering and terrorism financing requirements arising from this Law and the legal acts of the European Union apply;</i>  <i>4) request personal presence of the customer in the execution of the first transaction;</i></p>	<p><b>2. Identification with a secure electronic signature, electronic identity</b></p> <p>Electronic signature is issued by the Latvia State Radio and Television Centre. There are several technological platforms for example eID card, eID mobile. Along with purpose-built banks' solutions, it can be used as authentication tool for some Internet banks currently.</p>		<p>Acceptance High</p>
--	--	---	--	--	------------------------

		<p>5) if the customer is a natural person - resident -, obtain information attesting to the customer's identity from the document which the customer has signed with a secure electronic signature.</p> <p>(2) The subject of the Law shall perform the customer identification, only with the customer participating in the onsite identification procedure in person in the following cases:</p> <p>1) the customer or the beneficial owner of the customer is a politically exposed person, a family member of the politically exposed person, or a person closely associated to the politically exposed person and uses a service the monthly credit turnover of which exceeds EUR 3000;</p> <p>2) the customer is a shell arrangement;</p> <p>3) the customer uses services of a private banker.</p> <p>(3) When authorising a person who is not an employee of the subject of the Law to identify a customer, the subject of the Law shall be responsible for the identification of the customer in accordance with the requirements of this Law.</p> <p>(4) The subject of the Law, on the basis of the risk assessment, may carry out the customer identification without the participation of the customer in the onsite identification procedure in person when the customer has not been identified by the subject of the Law, its employee or authorised person, if the subject of the Law has performed the risk assessment, and the customer identification measures implemented without the participation of the customer in the onsite identification procedure in person correspond to the money laundering and terrorism financing risks.</p> <p>As set out in the Law on the Prevention of Money Laundering and Terrorism Financing (also - AML/CFT Law) Section 23(3) the Cabinet of Ministers shall determine the extent of and procedures for the customer identification by means of technological solutions including video identification or secure electronic signature, or other technological solutions.</p> <p>The Cabinet of Ministers adopted Regulation No. 392 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer" which allows for using the following tools:</p> <p>Regulation Nr. 392 of the Cabinet of Ministers of the Republic of Latvia, adopted on 3 July 2018 "Procedures by which the Subject of the Law on the</p>	<p><b>3. Other technological solutions</b></p> <p>Such as, under specific terms and conditions</p> <p>a) acquisition of data accrediting the identity of a natural person from a credit institution or payment institution by using an identification payment or another method which enables capturing data;</p> <p>b) comparison of the photograph of a personal identity document and an electronic self-portrait.</p>		<p>Acceptance medium</p>
--	--	--	---	--	--------------------------


		<p>Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer":</p> <p><a href="https://likumi.lv/ta/en/en/id/300147-procedures-by-which-the-subject-of-the-law-on-the-prevention-of-money-laundering-and-terrorism-financing-performs-the-remote-identification-of-a-customer">https://likumi.lv/ta/en/en/id/300147-procedures-by-which-the-subject-of-the-law-on-the-prevention-of-money-laundering-and-terrorism-financing-performs-the-remote-identification-of-a-customer</a></p>			
--	--	---	--	--	--

 Liechtenstein	1. Video identification 2. Electronic signature – permitted by law but not used				Video identification: Low acceptance  Electronic signature: not used
 Lithuania	Video identification, qualified signature, identification means, use of third-party information	The remote on-boarding and the use of electronic identification is permitted under AML/CFT  LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING  1. The identity of the customer that is a natural person or a representative of the customer that is a legal person and of the beneficial owner may be established without the physical presence of the customer only in the following cases: 1) when using information from third parties about the customer or the beneficial owner in accordance with the procedure laid down in Article 13 of this Law; 2) when using electronic identification means issued in the European Union which operate under the electronic identification schemes with the assurance levels high or substantial, as specified by 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 (OJ 2014 L 257, p. 73) (hereinafter: ‘Regulation (EU) No 910/2014’); 3) when information about a person’s identity is confirmed with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of Regulation (EU) No 910/2014. Qualified electronic signatures from third countries supported by a qualified certificate for electronic signature shall be recognised under Article 14 of Regulation (EU) No 910/2014; 4) when using electronic means allowing direct video streaming in one of the following ways:	Luminor – video identification and e-signature;  Citadele, BigBank – e-signature;	Identy, SK ID Solutions AS, Onfido.	

		<p>a) the original of the identity document or an equivalent residence permit in the Republic of Lithuania is recorded at the time of direct video streaming and the identity of the customer is validated using at least an advanced electronic signature which conforms to the requirements laid down in Article 26 of Regulation (EU) No 910/2014;</p> <p>b) the facial image of the customer and the original of the identity document or an equivalent residence permit in the Republic of Lithuania shown by the customer is recorded at the time of direct video streaming;</p>			
 Luxembourg 9	1. Video identification permitting the delivery by Luxtrust of eIDAS-qualified electronic signature services	<p>Luxembourg's financial sector is supervised by the Commission de Surveillance du Secteur Financier 'CSSF'. The IT requirements for specific customer on-boarding/KYC methods, and frequently asked questions regarding the use of identification / verification through video chat are published at the following link:</p> <p><a href="http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080318.pdf">http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080318.pdf</a></p> <p>"Identification/Verification of identity through video chat" (hereafter "video identification"), means the performance of the identification/verification of the identity of the customer by a professional of the financial sector under the supervision of the CSSF (hereafter the "professional") through an online video conference.</p> <p>The professional uses this process in order to support and execute certain tasks for the purpose of fulfilling his customer identification and verification of identity obligations as required i.e. by the Law of 12 November 2004 on the fight against money laundering and terrorist financing ("the Law").</p> <p>Notwithstanding this possibility, it shall be stressed that all other anti-money laundering and counter-terrorist financing ("AML/CTF") professional obligations (e.g. requirements with respect to AML/CTF outsourcing (if applicable), adequate training, internal controls, suspicions reporting, etc.) will have to be strictly applied by the professional.</p> <p>Regarding who can perform the video identification process, the professional has the following possibilities:</p>	For Smartcard certificates, Signing Stick or Signing Server certificates :  <a href="#">Banque BCP</a> <a href="#">Banque et Caisse de l'Epargne de l'Etat, Luxembourg</a> <a href="#">Banque de Luxembourg</a> <a href="#">Banque Raiffeisen</a> <a href="#">BGL BNP Paribas</a> <a href="#">BIL Banque Internationale à Luxembourg</a> <a href="#">Chambre de Commerce</a> <a href="#">Fortuna Banque S.C.</a> <a href="#">ING Luxembourg</a>	LuxTrust	

	<p><b>2. Electronic signature</b></p>	<p>Perform the video identification process himself using a tool developed internally, or  Perform the video identification process himself using an external tool he has acquired from an external provider, or  Delegate the identification process to an external provider using his own tool.</p> <p>In each of these scenarios, the video identification needs to be performed by a specifically trained employee, either of the professional or, if applicable of the external provider.</p> <p>The video identification/verification of the identity of a customer which is not actually performed by a specifically trained natural person but where the customer is in contact only with a robot, or where the customer simply uploads (a video with) identity documents online, does not qualify as video identification as addressed in the present FAQs due to the absence of a live video chat or real-time interaction between the aforementioned trained natural person and the customer.</p> <p>Thus, contrary to the video identification, this kind of online/digital or robo-video-identification, without intervention of a natural person on behalf of the professional, requires the application by the professional of supplementary safeguards in order to mitigate those particular risks linked to the automated character of this kind of identification process.</p> <p>Further requirements are detailed in the FAQ's.</p> <p>The AML legal framework does not refer per se to electronic signature. However, the Civil Code states that "the signature necessary for the completion of a binding contract identifies the person who affixes it and manifests its adherence to the content of the contract. Such signature can be handwritten <b>or electronic</b>. (See art. 1322-1 of the Code). "Luxtrust" being the Luxembourg "qualified trust service provider" according to Regulation N° 910/2014.</p>	<p><a href="#">LuxTrust S.A. Post Société Générale Bank and Trust</a></p> <p>Refer to the following link with the complete list of the entities:  <a href="https://www.luxtrust.lu/fr/simple/18">https://www.luxtrust.lu/fr/simple/18</a></p>		
--	---------------------------------------	---	---	--	--



		regarding identification of customer through “ <i>reliable source</i> ” including electronic identification means.			
	<b>3. Upcoming draft Law to comply with eIDAS Regulation + requirements of AMLD5</b>				
 Malta	<p>1. Video Identification</p> <p>2. Electronic Verification (E-IDs)</p> <p>3. Verification of Identity by reference to electronic copies of identity documents</p> <p>4. Commercial Electronic Databases</p>	<p>There has never been any restriction on the ability of obliged entities to on-board customers remotely as long as AML/CFT obligations, including verification of identity, are adhered to and any risks resulting from the remoteness element are adequately mitigated. It is also relevant to point out that neither primary nor secondary legislation lay down how AML/CFT obligations are to be met as this is then provided for in the Implementing Procedures – Part I issued by the Financial Intelligence Analysis Unit (“FIAU”).</p> <p>The said Implementing Procedures provide for how verification of identity can be carried out in these circumstances, i.e. either on the basis of copies of identity documents and the carrying out of additional measures to cater for any risk arising from the remote nature of the business relationship/occasional transaction, or through the use of a number of electronic means described hereunder. It is to be noted that the said Implementing Procedures are considered binding on obliged entities. Copy of the same can be accessed through the following link:</p> <p><a href="http://www.fiumalta.org/library/PDF/misc/27.01.2017-Implementing%20Procedures%20Part%20I2017.pdf">http://www.fiumalta.org/library/PDF/misc/27.01.2017-Implementing%20Procedures%20Part%20I2017.pdf</a></p> <p>The relative sections of the Implementing Procedures are indicated in brackets when the particular means of identity verification is described hereunder. A copy of the same is also being provided for ease of reference.</p>			


		<p><u>Current Position at Law</u></p> <p>As of 27 January 2017 obliged entities have been able to carry out verification of identity through one of the electronic means referred hereunder. The technological solutions adopted by obliged entities have to meet a number of requirements which are intended to ensure that the verification of identity process carried out by any of these means is sufficiently robust and reliable. These requirements are set out in the Implementing Procedures – Part I and are summarised hereunder:</p> <p>Video Identification [Implementing Procedures – Part I: Section 3.1.1.2(ii)(b)(2)]</p> <p>The (prospective) customer’s identity is verified in the course of a video conference call subject to the following conditions:</p> <p>Live video transmission allowing for visual and verbal contact between the (prospective) customer and the obliged entity Transmission of sufficient good quality to allow the obliged entity to visualise the face of the (prospective) customer and the details of the identification document being produced by the customer The identification document must be one of those expressly listed in the Implementing Procedures – Part I with optical safety features Verify on the basis of the document’s safety features that the document is not fake or forged Ensure that the facial image and identification details provided by the (prospective) customer tally with those on the identification document Communication in the course of the video call of a pre-transmitted code Retention of the following records</p> <p>Audio recording of the conversation between the (prospective) customer and the obliged entity Screenshots of the video call including of the (prospective) customer, the date and time of the call and of the identification document produced Code transmission records</p> <p>Electronic Verification (E-IDs) [Implementing Procedures – Part I: Section 3.1.1.2(ii)(b)(4)]</p>			
--	--	--	--	--	--

		<p>Consists in the verification of identification details provided by a (prospective) customer on the basis of data read from either an electronic chip embedded in an identification document or from other electronic devices like mobile applications or computer software, subject to the following conditions:</p> <p>It has to be recognised as a legally valid means of identity verification in the country of nationality/residence of the (prospective) customer, provided that the said country is an EEA Member State or a reputable jurisdiction</p> <p>The use of the electronic device as a means of identity verification is administered or approved by the government of an EEA Member State or a reputable jurisdiction</p> <p>The software/hardware used by the (prospective) customer to transmit data and by the obliged entity to read the same has to be administered or approved by the government of an EEA Member State or of a reputable jurisdiction.</p> <p>Retention of the following records:</p> <p>Print-out or an electronic copy evidencing that all necessary personal identification details have been verified</p> <p>Reference to the system used to transmit and read data.</p> <p>Electronic verification may also take place through privately run systems like Bank ID as long as the above conditions are met.</p> <p>Verification of Identity by Reference to Electronic Copies of Identity Documents [Implementing Procedures – Part I: Section 3.1.1.2(ii)(b)(3)]</p> <p>The use of electronic systems, including mobile apps, that allow a series of automated checks to be carried out on copies of identification documents uploaded through the said systems. The system must allow the following checks to be carried out:</p> <p>Visual Checks – Automatic comparison of the facial features of the (prospective) customer shown on the photographic image visible on the identification document with the facial features shown on a separate photo taken and sent by the (prospective) customer contemporaneously with the</p>			
--	--	--	--	--	--


		<p>transmission of the identification document so as to determine that the individual is one and the same.</p> <p>Authentication Checks – Verify automatically the authenticity and validity of the identification document submitted by performing at least a number of established checks:</p> <p>Verify security features  Examine the lamination for signs of tampering  Compare the document with standard templates  Read and validate the MRZ code  Verify that the document is unexpired.</p> <p>In addition electronic copies of the identification document uploaded and of the photograph provided by the (prospective) customer are to be retained by the system, indicating the time and date when these were uploaded or otherwise provided, and the system must have safeguards against any possible data alternation.</p> <p>Commercial Electronic Databases  [Implementing Procedures – Part I: Section 3.1.1.2(ii)(b)(1)]</p> <p>Another electronic means of identity verification is through the use of commercial electronic databases <u>BUT</u> in this case their use on their own is not considered sufficient as these can only serve to establish whether an individual actually exists – these databases do not allow the obliged entity to determine if the (prospective) customer is actually the individual he purports to be. Hence, additional measures are required to complete verification of identity.</p> <p>Not all commercial electronic databases can be used as there are a number of requirements set out in the Implementing Procedures – Part I, these being:</p> <p>Recognition through registration with the data protection authorities of the country where it is set up to store personal data;  Use of a range of positive information sources linking a (prospective) customer to both current and previous circumstances;  Access to negative information sources;</p>			
--	--	--	--	--	--

		<p>Access to a wide range of alert data sources; Transparent processes that enable the obliged entity to know what checks were carried out, what the results of these checks were and the level of certainty they provide as to the identity of the (prospective) customer.</p> <p>In addition, the verification process should at least comprise verification from:</p> <p>One match from one source on (i) the individual's full name and (ii) current permanent residential address; and One match from another source on (i) the individual's full name and (ii) either his current permanent residential address or his date of birth.</p> <p>It is also necessary that the commercial electronic database allows the obliged entity to capture and store the information used for verification purposes.</p> <p>Should an obliged entity decide to adopt any such verification of identity method, it would need to actually run the software or solution itself as outsourcing is not allowed at present.</p> <p><u>Planned Changes</u></p> <p>The FIAU is at present revising its Implementing Procedures – Part I and it is set to carry out some changes even in relation to the verification of identity solutions described above. While the above will still remain the main electronic identification methods provided for, the revised Implementing Procedures will:</p> <p>Revisit some of the conditions and requirements imposed for the use of any of the above systems to ensure that there are no unnecessary obstacles to the use of the same, including the watering down of any conditions and requirements that may be unnecessarily burdensome.</p> <p>In the case of Electronic Verification (E-ID), reference is also being introduced to systems and means regulated by Regulation (EU) 910/2014 so as to also reflect the provisions of Directive (EU) 2018/843 and ensure that it is possible to verify a (prospective) customer's identity on the basis of the systems and means provided for in the said regulation.</p>			
--	--	---	--	--	--



		<p>Provide for the outsourcing of certain AML/CFT functions, including carrying out verification of identity, subject to specific conditions. Thus, it will no longer be necessary for obliged entity to acquire software or other solutions but they may engage a third party to carry out verification of its (prospective) customers' identity through any of the methods described above.</p> <p>It is planned that the revised version of the Implementing Procedures – Part I be issued towards the end of February. Copy of the Consultation Document can be accessed through the following link:</p> <p><a href="http://www.fiumalta.org/library/PDF/misc/2018.10.30%20-%20Consultation%20Document%20-%20Revised%20Version%20of%20the%20FIAU%20Implementing%20Procedures%20Part%20I.pdf">http://www.fiumalta.org/library/PDF/misc/2018.10.30%20-%20Consultation%20Document%20-%20Revised%20Version%20of%20the%20FIAU%20Implementing%20Procedures%20Part%20I.pdf</a></p>			
--	--	---	--	--	--


 Netherlands	Video identification	<p>The rules as in the Netherlands' AML/CFT act do not prohibit the usage of remote on-boarding nor does it prescribe the exact techniques that can be used in the process. The act prohibits the offering of financial services without identifying and verifying the identity of the client. The element of non-face-to-face is considered higher risk (as laid down in the 4AMLD) which warrants financial institutions to take additional measures to mitigate this higher risk.</p>	Video identification is used. Depends on banks proposing it.		Medium acceptance: Customers appreciate video identification.
	eIDAS based solutions (based on prior on-boarding by FIs)	<p>In practices this means FI's must take steps to ensure the person requesting financial services matches the given identity by verifying the identity. There are currently several techniques being used, some notable examples are; Video identification and verification</p> <p>The usage of the data on the chip of the id-document in combination with other mitigating measures as video id, selfie with a liveness check</p> <p>eIDAS based ID-services are currently being developed by the larger banks based on prior on-boarding by these institutions within the eIDAS rules. The main issue is that the AML/CFT rules do not exactly match the eIDAS on-boarding requirements which leaves room for discussion on the level of assurance. Some of the eIDAS levels of assurance do not guarantee that the identity of the person has been verified.</p>	<p>Government runs an e-id level low, Digitale Identiteit "DigiD", consisting in a user name and password.</p> <p>Banks promote a substantial ID, called IDIN (supported by the banks like ItsMe in Belgium.)</p>	Dutch blockchain coalition is also aiming to provide an electronic eID.	Medium acceptance: Customers appreciate IDIN.
	Automatic transfer data from the id document to the relevant + Video identification or equivalent technique (liveness check)				




 Poland	Video-identification with or without biometry	<p>There is no legal interdiction to implement a remote on-boarding process, if the compliance with Polish AML law is ensured. Currently such process using video-identification (with or without facial biometry), independently on automatisa-tion's level, needs final decision about on-boarding made by bank's employee.</p> <p>According to art. 33 para. 4 of the Act of March 1, 2018 on Counteracting Money Laundering and Terrorism Financing (Journal of Laws, item 723, as amended) - hereinafter referred to as the Act - "<i>the obligated institutions shall apply customer due diligence measures to the extent and with an intensity taking into account the identified money laundering and terrorist financing risk related to business relationships or an occasional transaction as well as its assessment</i>". This means that it is up to the risk identified by the obligated institution and its evaluation to determine the extent to which the institution is obliged to apply CDD towards his client.</p> <p>One of the CDD measures is to identify the client of the obligated institution and verify its identity. From the information received by the General Inspector of Financial Information, it appears that the scope of its application raises doubts in the event that the client is not physically present in the obligated institution in order to establish business relationships or conduct occasional transactions. That is why - bearing in mind the best functioning of the national system of counteracting money laundering and financing of terrorism – the General Inspector of Financial Information issued guidelines on this subject. The client identification process should be considered a relatively simple process. It may consist in giving by the client its personal data (eg. by e-mail, by filling in the form on the website of the obligated institution), indicated in art. 36 par. 1 of the Act. Another issue is the verification of the customer's identity, aimed at confirming that the client is who he claims to be. For this purpose, the obliged institution is obliged to use - in accordance with art. 37 of the Act - a document confirming the identity of a natural person, a document containing valid data from the extract of the relevant register (in the case of a legal person or an organizational unit without legal personality) or other documents or data or information originating from a reliable and independent source.</p>			
---	---	--	--	--	--


		<p>Thus, the legislator left the obligated institution the opportunity to choose what documents, data or information will be the basis of the above-mentioned verification, indicating only that they must come from a reliable and independent source. The subject provision of the Act is consistent with art. 13 para. 1 letter a of the Directive (EU) 2015/84 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council repealing the Directive Of European Parliament and Council 2005/60 / EC and the Commission Directive 2006/70 / EC (Journal of Laws No. 141 of 05/06/2015, p. 73).</p> <p>As a rule, in the verification of the client's identity without its physical presence, the most trusted instruments are electronic identification means referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93 / EC (OJ L 257, 28/08/2014, p. 84), including qualified electronic signatures.</p> <p>If it is not possible to use the above electronic identification means, the obliged institution should apply - in accordance with art. 43 par. 2 point 7 of the AML Act – enhanced CDD</p>			
--	--	---	--	--	--


 Portugal	Video identification		Caixa Geral de Depositos		Low level of acceptance
	Video identification + biometrics	<p>Regarding the <u>use of biometrics in addition to video</u>, in the Portuguese legal framework this question is not relevant, since when it comes to video conference, the local legislation requires financial institutions to have a person, in real time, validating the client's identity.</p> <p>As such, the use of biometric to validate data is an option to be taken by each financial institution, and they only need to prove that their system is strong enough.</p> <p>Legally, in Portugal, this solution is not particularly relevant</p>	Banco Europa BNI	DigitalSign	
	eIDs notified under eIDAS	Banks are currently working with the National Administrative Modernization Agency – AMA- with the objective of implementing a digital onboarding using eIDs notified under eIDAS – “Chave Móvel Digital”. Currently eID is only used by some banks for home banking client authentication.			
 Romania		<p>According to the Romanian legal framework, any adjustment of the KYC policy must be prior approved by National Bank of Romania (NBR is an independent public institution) and no good practices on remote onboarding were outlined at the industry level, up to now.</p> <p>According to the Romanian legal framework, there is no legal interdiction to implement a remote onboarding process. But in this respect, the bank should define some additional KYC measures to be priory presented to National Bank of Romania.</p> <p>The concrete adequate measures must be defined based on a bank internal assessment of Compliance, Legal, IT, Information Security, Risk, Marketing, Data Protection Officer.</p>	<b>Video identification</b> Using conventional ID documents is present in Romania for KYC purposes Although not widely used. However, the process is not completely instant and digital end-to-		Not widely used.

			end. Also, a copy of the ID document needs to be scanned and sent to the bank and a payments transaction is required.		
 Slovakia	Automatic transfer data from ID- document via special application of the bank ( clients can downloads to their smartphone) + face biometry data, or other comparable form of data + video call identification (via special application of the bank)	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT</p> <p>Remote on-boarding process was incorporated (and is effective since 15<sup>th</sup> March 2018) in Act No. 297/2008 Coll. (AML Act). Process is determined only for natural not legal person.</p> <p>§ 8 Verification of identification</p> <p>Verification of identification shall be understood for the purposes of this Act in the case of a natural person, the verification of data pursuant to Article 7 (1) a) in its identity document, if provided, and verification of the form of a person with the form in his identity document for his physical presence or by the use of technical means and procedures, if the obliged entity, after taking into account the circumstances of the business relationship and the security risks of the technology used evaluates, that by such means and procedures it is possible to carry out verification of identification at a level, which is in terms of credibility of the outcome of the verification, is similar to verification of physical presence;</p> <p>National bank of Slovakia (NBS) in co-operation with FIU has prepared and published Opinion of the National Bank of Slovakia's Financial Market Supervision Division No 1/2018 ( 10<sup>th</sup> December 2018).</p> <p>The aim of this Opinion is to bring to the supervised entities (obliged entities according to the AML Act) a regulatory expectation and view of the NBS on the technologies used to identify and verify the identification of a natural person without his physical presence.</p> <p><b>1. Remote customer on boarding (online) procedure:</b></p> <ul style="list-style-type: none"> <li>-scan of a national ID card and a 2nd document is required, and</li> <li>-penny transfer, or</li> </ul>	-Tatra banka -365 bank		Medium acceptance

		<p>-courier who verifies client´s identity (face-to-face)</p> <p><b>2. Technical means comparable to face to face physical presence identification and verification (currently based on face biometry)</b>  Legal base:  Based on an amendment of the Slovak AML Act in March 2018, it is possible to perform remote identification and verification of natural persons with technical means.  Technical mean: a software solution with secured digital interface enabling the acquisition and transmission of data, documents and information by means of technical tools and their processing, meeting the following regulatory requirements:  a) acquisition of authentic biometric data or other comparable identification data and its trustful verification,  b) detection of discrepancy in the biometric or other comparable identification data during the data transmission and setting of matching criteria,  c) verification of acquired biometric or other comparable data with data from internal or external sources or a combination thereof  d) the authentic biometric or other comparable identification data provide, as to the result, comparable degree of authenticity, validity and completeness of identification data as in case of identification in physical presence of the client,  e) acquisition of additional personal identification data (e.g. ID card)  f) verification of authenticity and validity of additional personal data (e.g. comparison of the ID card with data in internal or external sources or a combination thereof, incl. verification of the security features of the ID card),  g) identification of non-standard behaviour of the identified client during the nonverbal or verbal communication with the client or throughout the monitoring process  Opinion of National Bank of Slovakia on usage of technical means for identification purposes is available here.</p> <p><b>3. Usage of national ID card for customer onboarding is under discussion</b></p>			<p>Medium acceptance</p> <p>Medium expected</p>
--	--	---	--	--	---


 Slovenia	Video identification	<p>Identity card check + video identification is permitted to on board customer for account opening.</p> <p>No formal pre-approval or license from regulators is needed to introduce remote onboarding. Nevertheless, there are rules of the Ministry (adopted under AMLFT Act), which determine what kind of verification must be done on ID document, when performing video onboarding</p> <p>This is an excerpt of Rules of the Ministry:  <i>(4) The person performing the video identification must make sure that the authenticity of the official identity document and the matching of the data is authentic in the following ways:</i></p> <ol style="list-style-type: none"> <li><i>1. Visible verification of the existence of optical characters, including holographic or other equivalent protective elements (for example, safety threads, variable colors and the like), which must be clearly visible even with the horizontal and vertical inclination of the official identity document;</i></li> <li><i>2. checking the formal signs of the official identity document and matching them according to the type of official identity document (graphic design, character size, character spacing, typography and the like);</i></li> <li><i>3. verification of the matching of the data already obtained with the information shown in the official identity document;</i></li> <li><i>4. checking the validity of the official identity document and the correctness of the alphanumeric characters of its serial number;</i></li> <li><i>5. a visual check of the possible post-installation of the photograph, the intrinsic lamination surrounding the official identity document, or other trademarks showing its intrinsic character;</i></li> <li><i>6. verifying the logical consistency of the data derived from the document (for example, the correctness of the date of issue and expiration, the correctness of the birth date, their mutual match, and the like).</i></li> </ol> <p><i>(5) The verification of optical characters and formal signs of the official identity document referred to in points 1 and 2 of the preceding paragraph may also be carried out using appropriate software support.</i></p>			
---	----------------------	--	--	--	--

		<p>(6) The person performing the video-electronic identification shall be satisfied that the photograph, any personal description and data from the official identity document are in conformity with the party that initiated the video identification and verifies the logical consistency of all available data (for example, matching the appearance video and video clients in the official identity card or other information with which the taxpayer already has, and the like).</p>			
 Spain	<p>Electronic signature + Video identification systems</p>	<p>Article 12 of Law 10/2010 allows obliged entities to enter to non-to face transactions as long one of these conditions are meet: a) customer's identity is evidenced in accordance with the provisions of applicable regulations on electronic signature; b) the first deposit comes from an account in the customer's name at an entity domiciled in Spain, in the European Union or in equivalent third countries; or c) some of the requirements foreseen in Regulations are verified.</p> <p>According to Article 21 of the AML Regulation approved by Royal Decree 304/2014, also points out that one of the four following conditions must be met (two in addition to the ones foreseen in Law): a) The customer's identity is evidenced in accordance with the provisions of applicable regulations on electronic signatures; b) The customer's identity is evidenced by means of a copy of the relevant identity document, provided that the copy is issued by a notary public; c) The first deposit comes from an account in the customer's name at an entity domiciled in Spain, in the European Union or in equivalent third countries; or d) The customer's identity is evidenced by other secure procedures for customer identification in remote transactions, provided that such procedures have been previously authorised by Sepblac.</p> <p>Sepblac has established a series of minimum specifications regarding 3 procedures for identifying customers in remote transactions (which not require individual authorisations to obliged entities):</p> <p><u>Identity confirmation between participants in the Spanish Electronic Clearing System</u> (known in Spanish as SNCE) In the context of remote on boarding, firms which are participant in the Spanish Electronic Clearing System might request other participant which have business relationships with the customer in place to confirm identification data. This can only be used to meet formal identification requirement. For a complete list of specifications</p>	<p>The Spanish banks BBVA; OpenBank (Santander); ImaginaBank (Caixabank); SelfBank; Evo Banco and Bankia are using these remote onboarding systems.</p> <p>There are also non Spanish banks that offers these options in Spain, for example N26 or CIM Banque.</p> <p>These two processes (video conference and video identification) are not proposed by all banks, due to the fact that it is costly. Only big</p>	<p>There is a national government ID but which is not used.</p> <p>What regards companies, certificates are used. High customer acceptance.</p> <p>High level of acceptance for both video identification processes</p>	

		<p>regarding procedures for identifying customers in remote transactions please refer to: <a href="#">Due diligence   Sepblac</a>.</p> <p><u>Video conference.</u> Certain requirements need to be met prior to authorisation: reliable and visible client documentation, ex ante customer risk analysis, technical and effectiveness requirements, keep video recordings for at least 10 years among other requirements.</p> <p>For a complete list of specifications regarding procedures for identifying customers in remote transactions please refer to: <a href="#">Due diligence   Sepblac</a>.</p> <p><u>Video identification.</u> Video identification poses a greater risk than videoconferencing, since there is no online interaction, but a later control of the recording, then involving a human being for recording examination. Thus, additional requirements are set, among them: client must only use one device, obliged subjects must record the streaming, such recording must be assessed by the obliged subject prior to any business operation, etc. For a complete list of specifications regarding procedures for identifying customers in remote transactions please refer to: <a href="#">Due diligence   Sepblac</a></p>	banks propose them.		(automatic and video conference)  Video identification is much more used by customers than video conference.
 Sweden	<p>Electronic signature via (Mobile) Bank-ID</p>	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT</p> <p>Bank-ID is industry standard, and a physical meeting precedes a Bank-ID. Identification non-face-to-face is regulated by the competent authority's regulation FFFS 2017:11.</p> <p>FFFS 2017:11, chapter 3, article 5, states: An obliged entity shall verify the identity of a physical person on distance by using an electronic identification to create an advanced electronic signature in accordance with the law (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering (English: "with completing provisions to EU's regulation on electronic identification"), which completes 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.</p>	<p>All major banks: -Swedbank -SEB -Handelsbanken -Nordea (branch) -Danske Bank (branch)</p>	<p><b>1. eID-solution issued by the Swedish banks, BankID</b> BankID dominates the eID-market with slightly less than 100% of the market.</p>	High acceptance



		<p>According to FFFS 2017:11, chapter 3, article 7, legal persons can be on-boarded by verifying the identity of a representative by:</p> <ul style="list-style-type: none"> <li>- identifying and verifying the representative according to provision 5 stated above, and</li> <li>- verifying the authorization to represent the legal person and on which circumstances the authorization rests by verifying the information of the first inset against the legal person's certificate of registration, external register or equivalent.</li> </ul>		<b>2. eIDs notified under eIDAS</b>	Not used
				<b>3. Qualified electronic signature under EIDAS</b>	Not used
	Without IT means	<p>According to FFFS 2017:11, chapter 3, article 5, customers can also be on-boarded without electronic identification, by verifying the physical persons identity by:</p> <ul style="list-style-type: none"> <li>- collecting information regarding the person's name, address, social security number or equivalent,</li> <li>- verifying the information above towards external registers, certificates, or other equivalent documentation, and</li> <li>- contact the physical person by sending a confirmation to that person's residential address or equivalent and credible information of address, or make sure that the person sends a certified copy of identification, or by other equivalent means.</li> </ul> <p>According to FFFS 2017:11, chapter 3, article 7, legal persons can be on-boarded by verifying the identity of a representative by:</p> <ul style="list-style-type: none"> <li>- identifying and verifying the representative according to provision 5 stated above, and</li> <li>- verifying the authorization to represent the legal person and on which circumstances the authorization rests by verifying the information of the first inset against the legal person's certificate of registration, external register or equivalent.</li> </ul>	All obliged entities		

 UK	Video Identification, electronic verification	<p>The remote on-boarding and the use of electronic identification is permitted under AML/CFT</p> <p>Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 permit a risk based approach to undertaking CDD measures.</p> <p>Regulation 28:</p> <p>1) This regulation applies when a relevant person is required by regulation 27 to apply customer due diligence measures.</p> <p>(2) The relevant person must —</p> <p>(a) identify the customer unless the identity of that customer is known to, and has been verified by, the relevant person;</p> <p>(b) verify the customer’s identity unless the customer’s identity has already been verified by the relevant person; and</p> <p>(c) assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.</p> <p>(12) The ways in which a relevant person complies with the requirement to take customer due diligence measures, and the extent of the measures taken—</p> <p>(a) must reflect—</p> <p>(i) the risk assessment carried out by the relevant person under regulation 18(1);</p> <p>(ii) its assessment of the level of risk arising in any particular case;</p> <p>(b) may differ from case to case.</p> <p>(13) In assessing the level of risk in a particular case, the relevant person must take account of factors including, among other things—</p> <p>(a) the purpose of an account, transaction or business relationship;</p> <p>(b) the level of assets to be deposited by a customer or the size of the transactions undertaken by the customer;</p> <p>(c) the regularity and duration of the business relationship.</p> <p>(18) For the purposes of this regulation—</p>	Remote onboarding is used primarily by newer, challenger banks who are online only and do not have branch network. <p>1. Government eID scheme (GOV.UK Verify) is not currently reusable in the private sector.</p> <p>2. Some institutions allow digital document upload facilities (such as photos of physical ID documents e.g. passports) in their onboarding process.</p>	A definitive list is not held.	Impersonation for the purposes of fraud is the key risk. <p>Medium acceptance</p>
---	---	--	--	--------------------------------	---

		<p>(a) except in paragraph (10), “verify” means verify on the basis of documents or information in either case obtained from a reliable source which is independent of the person whose identity is being verified;</p> <p>(b) documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the relevant person by or on behalf of that person.</p> <p>Joint Money Laundering Steering Group guidance interprets UK law for banks and other financial institutions</p> <p><u>Criteria for use of a provider of electronic verification of identity</u></p> <p>5.3.51 Some commercial organisations providing electronic/digital verification are free-standing and set their own operating criteria, whilst others may be part of an association or arrangement which, in order to admit organisations to ‘membership’ require them to demonstrate that they meet certain published criteria – for example, in relation to data sources used, or how recent the information is- and carry out some form of checks on continuing compliance.</p> <p>5.3.52 Before using a commercial organisation for electronic verification of identity, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate, and independent of the customer. This judgement may be assisted by considering whether the identity provider meets the following criteria:</p> <ul style="list-style-type: none"> <li>➤ it is recognised, through registration with the Information Commissioner’s Office, to store personal data;</li> <li>➤ unless it is on the Information Commissioner’s list of credit reference agencies (see <a href="https://ico.org.uk/for-the-public/credit/">https://ico.org.uk/for-the-public/credit/</a>), it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards;</li> <li>➤ it uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;</li> <li>➤ it accesses negative information sources, such as databases relating to identity fraud and deceased persons;</li> </ul>			
--	--	--	--	--	--

	<p>           &gt; it accesses a wide range of alert data sources;            &gt; its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;            &gt; arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed; and            85            &gt; it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.         </p> <p>5.3.53 In addition, a commercial organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity.</p> <p><b><u>B – ELECTRONIC EVIDENCE</u></b></p> <p>5.3.79 When using an electronic/digital source to verify a customer's identity, firms should ensure that they are able to demonstrate that they have both verified that the customer exists, and satisfied themselves that the individual seeking the business relationship is, in fact, that customer (or beneficial owner).</p> <p>5.3.80 Electronic verification may be carried out by the firm either direct, using as its basis the customer's full name, address and date of birth, or through an organisation which meets the criteria in paragraphs 5.3.51 and 5.3.52.</p> <p>5.3.81 For verification purposes, a firm may approach an electronic/digital source of its own choosing, or the potential customer may elect to offer the firm access to an electronic/digital source that he/she has already registered with, and which has already accumulated verified evidence of identity, and which meets the criteria in paragraphs 5.3.51 and 5.3.52.</p> <p>5.3.82 Some electronic sources focus on using primary identity documents, sometimes using biometric data. Others accumulate corroborative information which in principle is separately available elsewhere. Some</p>			
--	--	--	--	--

		<p>sources are independent of the customer, whilst others are under their 'control' in the sense that their approval is required for information to be included.</p> <p>5.3.83 As well as requiring a commercial organisation used for electronic verification to meet the criteria set out in paragraphs 5.3.51 and 5.3.52, it is important that the process of electronic verification meets an appropriate level of confirmation before it can be judged to satisfy the firm's legal obligation.</p> <p>5.3.84 Commercial organisations that provide electronic verification of identity use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Some organisations confirm that a given, predetermined 'level' of authentication has been reached. Firms should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.3.46-5.3.50, and cumulatively meet an appropriate level of confirmation in relation to the risk assessed in the relationship.</p> <p><u>C - MITIGATION OF IMPERSONATION RISK</u></p> <p>5.3.85 Whilst some types of financial transaction have traditionally been conducted on a non-face-to-face basis, other types of transaction and relationships are increasingly undertaken in this way: e.g., internet and telephone banking, online share dealing.</p> <p>5.3.86 Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non face-to-face business, such as applications submitted by post, there are other factors that may, taken together, aggravate the typical risks:</p> <ul style="list-style-type: none"> <li>➤ the ease of access to the facility, regardless of time and location;</li> <li>➤ the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;</li> <li>➤ the absence of physical documents; and</li> <li>➤ the speed of electronic transactions.</li> </ul>			
--	--	---	--	--	--

	<p>5.3.87 The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in itself increase the risk attaching to the transaction or activity. A firm should take account of such cases in developing their systems and procedures.</p> <p>5.3.88 Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.</p> <p>5.3.89 Where identity is verified electronically, copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms should consider:</p> <ul style="list-style-type: none"> <li>• verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or</li> <li>• requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs or other secret data may be set up within the electronic/digital identity, or may be supplied to a verified mobile phone, or through a verified bank account, on a one-time basis, or</li> <li>• following the guidance in paragraph 5.3.90.</li> </ul> <p>5.3.90 The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:</p> <ul style="list-style-type: none"> <li>➤ requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction;</li> <li>➤ verifying additional aspects of the customer's identity (see paragraph 5.3.29);</li> <li>➤ telephone contact with the customer prior to opening the account</li> </ul>			
--	---	--	--	--

		<p>on a home or business number which has been verified (electronically or otherwise), or a “welcome call” to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;</p> <ul style="list-style-type: none"> <li>&gt; communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);</li> <li>&gt; internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;</li> <li>&gt; other card or account activation procedures;</li> <li>&gt; requiring copy documents to be certified by an appropriate person.</li> </ul> <p>5.3.91 The source(s) of information used to verify that an individual exists may be different from those sources used to verify that the potential customer is in fact that individual.</p>			
--	--	--	--	--	--

## Annex 5: Digital On-boarding for Bank Accounts in Spain

The below presents the results of a bank study conducted on the user experience for the on-boarding process of digital accounts in Spain. The research includes the 8 largest banks operating in Spain. Together, they account for 80% of the retail market share. Both web and mobile on-boarding process have been reviewed for individual customers.

The majority of banks allow an end to end digital process for account opening. Different banks are requesting different data fields and using different measures for validation and compliance. There are still significant customer pain points along the process given the current technology needed to comply with AML and KYC regulations, particularly with video conference with live agent, uploading documents and need to visit a branch in some cases.

At present, there are no instances of eID solution being used to open a bank account. Use of eiD solution will certainly facilitate the remote onboarding process.



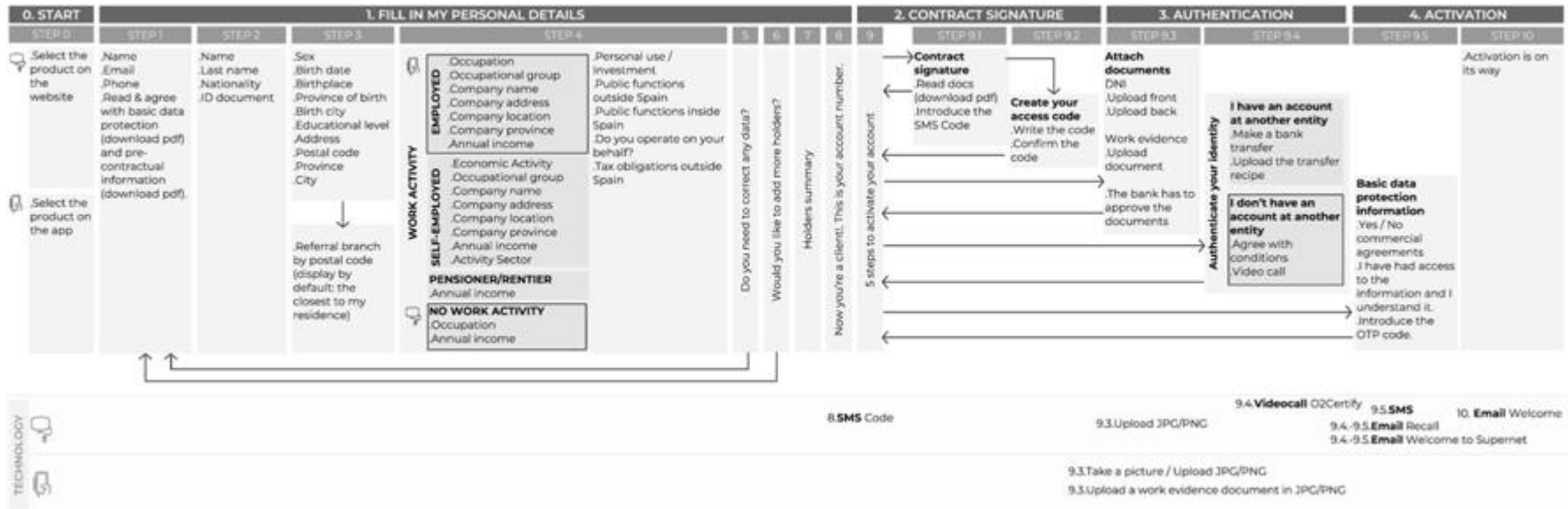
### 3. RESEARCH

#### GENERAL STEPS

With slight variations all banks follow a similar process with the same steps, which include:

PRODUCT SELECTION	GATHER CONTACT DATA	GATHER PERSONAL DATA	OCCUPATIONAL DATA	DATA VALIDATION	UPLOAD DOCUMENTS	AUTHENTICATION	CONTRACT SIGNING	PASSWORD SELECTION	END
<ul style="list-style-type: none"> <li>.Select the product</li> <li>.Select complementary products</li> <li>.Select the number of holders</li> </ul>	<ul style="list-style-type: none"> <li>.Name</li> <li>.Last name</li> <li>.Email</li> <li>.Phone</li> <li>.Agree with basic data protection information &amp; pre-contractual information</li> </ul>	<ul style="list-style-type: none"> <li>.ID document</li> <li>.Nationality</li> <li>.Birth date</li> <li>.Birthplace</li> <li>.Province of birth</li> <li>.Birth city</li> <li>.Sex</li> <li>.Educational level</li> <li>.Civil Status</li> <li>.Language</li> <li>.Address</li> <li>.Postal code</li> <li>.Province</li> <li>.City</li> </ul>	<ul style="list-style-type: none"> <li>.Occupation</li> <li>.Company name</li> <li>.Company address</li> <li>.Activity sector</li> <li>.Kind of contract</li> <li>.Seniority</li> <li>.Main purpose of the account</li> <li>.Annual/Monthly income</li> <li>.Income origen</li> <li>.Other incomes?</li> <li>.Public functions</li> <li>.Do you operate on your behalf?</li> <li>.Tax revenues</li> <li>.Tax obligations outside Spain</li> <li>.Other tax residence?</li> <li>.Residence permit in the USA?</li> <li>.Regular transfers abroad?</li> </ul>		<ul style="list-style-type: none"> <li>.ID document both sides</li> <li>.Work evidence</li> </ul>	<ul style="list-style-type: none"> <li>.Different methods:                             <ul style="list-style-type: none"> <li>- Video call</li> <li>- Other account number (IBAN or transfer recipe)</li> <li>- Send a postman to your home.</li> <li>- Go yourself somewhere [office/post-office]</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Read &amp; sign all the documentation (usually with a SMS code)</li> </ul>	<ul style="list-style-type: none"> <li>Create your user and your password.</li> </ul>	<ul style="list-style-type: none"> <li>.Account activation or request of additional activities from the consumer</li> </ul>

BANK 1



BANK 2

1. START	2. COMPLETE MY PERSONAL DETAILS		3. AUTHENTICATION			4. CONTRACT SIGNATURE			5. UPLOAD DOCUMENTS	6. END	
STEP 0	STEP 1	STEP 2	STEP 3			STEP 4	4.1	4.2	4.3	STEP 5	STEP 6
.Name .Last name .ID document .Birth date .Tax residence in Spain? .Email .Create your access code .Do you have a promotional code? .Read & agree with basic data protection (download pdf) and pre-contractual legal information (download pdf)	.This is your account number .Mobile phone .Confirm mobile phone .Address .Sex .Nationality .Would you like to add more holders or authorized representatives?	.Work activity ( <u>employed</u> / self-employed / pensioner / rentier / no-activity) .Sector: public / private .Occupation (two available methods: search or select) .Company name .How did you generate your capital and heritage? .Tax revenues > 150.000€ per year? .Public functions outside / inside Spain .Do you operate on your behalf? .Main purpose of the account .Tax obligations outside Spain	<b>Account number at another entity</b> .Introduce the IBAN code	<b>Videocall</b> .Agree with the Terms of Use of the service .Name .ID document .The assistant takes a photo .The assistant takes a photo of your ID document (front / back) .The assistant checks the pictures quality and data	<b>Face to face - Correos</b> <b>Post-office</b> .Choose a post-office (map) .Go there with your ID document <b>Home</b> .Introduce an address (your residence by default) .Choose your time band	.Yes / No commercial agreements	.Introduce the SMS code to access to the signature service	.Draw your signature .Signature validation	<b>DNI</b> .Upload front .Upload back <b>Work evidence</b> .All pages of the document	.Activation is on its way .The bank has to approve your documents and your identity .You will receive a welcome pack and your signature key	

TECHNOLOGY	0. Email Welcome	1. Email to my holders/representatives to complete the process on their own.	3. SMS Correos Alert	3. SMS Correos Visit time (hour)	4.1-4.2. Sign DocuSign	4.3. Email Signature	5. Upload JPG/PNG	6. Email Account activated	6. Post mail Digital signature	6. Post mail Welcome Pack
 										

**BANK 3**

0. START		1. ACCESS		2. CONTACT DATA		3. AUTHENTICATION		4. ECONOMIC ACTIVITY		5. PERSONAL DETAILS		6. IDENTIFICATION		7. CONTRACT SIGNATURE		8. FINAL STEPS	
STEP 0	1	2	3	4	5	6	7	8	9	10							
<p>Choose the product</p> <p>Alert: you need your mobile, your ID document and an account number</p>	One holder	User Password Confirm password Read & agree with basic data protection (download pdf)	Email Confirm your email Mobile Confirm your mobile	<p><b>Upload my ID document</b></p> <p><b>Now</b> Upload front Upload back</p> <p><b>Later</b></p>	Work activity Contract type Annual income Company (tax name) Address (automatically filled) CNAE (automatically filled) Public functions	Name Last name Birth date Sex Birth country Address Other tax residence? Residence permit in the USA? Main purpose of the account Income origin Monthly income	<p><b>Account number at another entity</b> Introduce the IBAN code Make your first transfer</p> <p>Postman</p>	Agree & sign all the documentation (download pdf) Introduce the SMS code	<p><b>Work evidence</b> Upload it now</p> <p>By email Subject: your Id document</p> <p>Postman Make a call Use the code</p>	Activation is on its way You will receive an SMS and an email You will receive your card at your residence Rate your experience							
<p>Become a client</p> <p>Choose the product</p> <p>Alert: you need your dni, reliable internet connection, and being in a well-lit and quiet place.</p>	Two holders			<p>ID document front ID document back Take a selfie</p>			<p><b>6. CONTRACT SIGNATURE</b> 7</p> <p>Agree &amp; sign all the documentation (download pdf) Introduce the SMS code</p>	<p><b>7. IDENTIFICATION</b> 8</p> <p>Video call Show my DNI to the assistant different times in different positions</p>	<p>This is your account number</p> <p><b>Work evidence</b> By email Subject: your Id document</p> <p>Postman Make a call Use the code</p>								

TECHNOLOGY	4.Upload JPG/PNG		5.Company data automatically filled		6.SMS Code		9.Email Next steps	
	4.Take photo / Upload JPG/PNG		5.Company data automatically filled		6.Personal details automatically filled	7.SMS Code	8.Video call Supplier no identified	9.Upload JPG/PNG/PDF

BANK 4

0. START	1. FILL IN MY PERSONAL DETAILS				2. USE OF THE ACCOUNT		3. AUTHENTICATION			4. MANAGE MY DATA	5. CREATE MY ACCOUNT		6. SIGN			7. END	
STEP 0	1	2	3	4	STEP 5		STEP 6		STEP 7	STEP 8	STEP 9	STEP 10	STEP 11	12	13	14	15
Are you a CaixaBank client?  Data protection Are you a CaixaBank client?	Promos bringing my income / my salary paid. Email Mobile phone Be an imaginer Friend code Agree with data treatment	Confirm your mobile phone	Alert: You need your DNI and your phone to continue	Name Last name ID document Sex Birth date Nationality Birthplace Province of birth Address Province City	<p><b>DNI</b></p> <p><b>Take or upload photo from my computer</b> Upload/Take photo of the front Upload/Take photo of the back</p> <p><b>Upload photo from the mobile</b> Scan the QR code/Use this URL+this code .Take /Upload photos with the mobile .Click on "Receive photos from my mobile"</p> <p><b>DNI</b></p> <p><b>Take or upload photo from my mobile</b> Upload/Take photo of the front Upload/Take photo of the back</p>	<p><b>STUDENT</b></p> <p>Residence permit in the USA Regular transfers abroad Main purpose of the account Public functions Tax obligations outside Spain</p> <p><b>WORK ACTIVITY</b></p> <p><b>EMPLOYED</b> Activity sector Company Seniority Income range Other incomes?</p> <p><b>SELF-EMPLOYED</b> Activity sector Income range CNAE code Tax register declaration Financial documents Third parties benefits Other incomes?</p> <p><b>PENSIONER/RENTIER</b> Income range Other incomes?</p> <p><b>UNEMPLOYED</b> Monthly income Income range</p>	Account number at another entity Introduce the IBAN code	<p><b>Account number at another entity</b> Introduce the IBAN code</p> <p><b>Videocall</b> Agree with Terms of Use of the service Show my DNI to the assistant different times in different positions Check my data with the assistant Agree with the use of the SMS code as electronic signature</p>	<p><b>Choose my bank card</b> Imaginbank card "Los 40" card</p> <p><b>Check my personal details</b> Name Last name Id document Sex Birth date Nationality Birthplace Province of birth Address Province City Work activity details</p>	Yes / No commercial agreements	Create password Confirm password	I want to sign now	Agree with "Contrato marco" (download pdf) Agree with "Contrato imagin" (download pdf)	Introduce the SMS code	Introduce the SMS code	Download the app The card will arrive at my residence before 15 days Make a bank transfer	Validation in 5 days

TECHNOLOGY

5. Upload JPG/PNG/Take a photo  
5. QR reader

7. Video call Supplier no identified

11.SMS Code  
14. Post mail Credit card

10-11.Email Recall

BANK 5


0. START		1. PERSONAL DETAILS		2. RESIDENCE	3. EMPLOYMENT DATA	4. AUTHENTICATION	5. PRODUCT & PERMITS		6. VALIDATION	7. FINAL STEPS			
STEP 0	1	2	3	5	6	7	8	9	10	11	12	13	14
.Become a client	.One holder	Video call → Account at another entity →	<b>Scan your DNI</b> .Front/Back → .JD document .Name .Last name .Birthdate .Birth country .Nationality .Birth province .Birth city .Sex .Mobile phone .Confirm your mobile phone .Email .Confirm your email .Contact preferences .Create your access code .Confirm your access code	.Address .Postal code .Province .City .Country .Tax residence (same/other) .Referral branch by postal code (display by default: the closest to my residence)	.Work activity .Occupation (Role) .Occupational activity .Public functions .Income origin .Main purpose of the account .Do you operate on your behalf?	<b>Account at another entity</b> .Introduce the IBAN  <b>Office</b> .Choose your time band  <b>Postman</b>	<b>Salary paid in the current account</b>  <b>Cuenta_ON Nómina</b>  <b>No salary paid in the current account</b>  <b>Cuenta_ON</b>  <b>Cuenta fácil</b>	.Yes / No commercial agreements	.Attach ID document front .Attach ID document back  .Read & agree with basic data protection (download pdf) and pre-contractual information (download pdf).  .Introduce the SMS code	.Next steps  ↓ <b>Log in</b> .User .Access Code	.Choose your signature .Confirm your signature .Introduce the SMS code	.Agree & sign all the documentation (download pdf) .Choose the secret code for your card .Confirm the secret code	.This is your account number .Summary of legal documents (download pdf)

TECHNOLOGY		3.Video call Supplier no identified	10.Upload JPG/PNG 10.SMS Code	11.Email Next steps 12.SMS Code 2
		3.Video call Supplier no identified	10.Take photo / Upload JPG/PNG 10.SMS Code	11.Email Next steps 12.SMS Code 2

**BANK 6**





**BANK 7**

0. START	1. PERSONAL DETAILS	2. RESIDENCE	3. EMPLOYMENT DATA	4. ACCESS CODE	5. DIGITAL AUTHENTICATION	6. UPLOAD DOCUMENTS	7. NEXT STEPS
STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6	STEP 7	STEP 8
Email ID document Birth date Read & agree with pre-contractual information (download pdf).	Sex Name Last name Birth country Nationality Second nationality Tax residence Mobile phone Educational level Civil status More than one tax residence	Search bar Address Postal code City	Main purpose of the account Income origen Work activity Occupation Activity sector Company Monthly income Seniority Contract also a "Cuenta Naranja"	 .Numeric key .Confirm numeric key .Contracted services in other banks	IBAN of another entity account	<b>ID document</b> <b>Now</b> Upload front Upload back or Upload front+back (together) <b>Later</b> Upload it to the "Client Area"/Send it by mail	.This is your account number .Take note of the quantity of the transfers received in my other account. .Log in into the client area of ING and write down these quantities
				<b>4. UPLOAD DOCUMENTS</b> <b>STEP 5</b> <b>ID document</b> <b>Now</b> Upload front Upload back or Upload front+back (together) <b>Later</b> Upload it to the "Client Area" Send it by email	<b>5. ACCESS CODE</b> <b>STEP 6</b> Numeric key Confirm numeric key Contracted services in other banks	<b>6. DIGITAL AUTHENTICATION</b> <b>STEP 7</b> <b>IBAN</b> IBAN of another entity account <b>Video Call</b> Download the APP Log in (ID document, birth date) Start the video call (access code) Introduce SMS Code	<b>7. WELCOME</b> <b>STEP 8</b> Activate notifications Profile

 <b>Seguridad Norton Secured</b>	<b>4. Email</b> Data protection document	<b>7. Upload</b> JPG/PNG	<b>8. SMS</b> Transfers alert <b>8. Email</b> Contract Copy <b>8. Postmail</b> Welcome Pack
	<b>4. Email</b> Data protection document	<b>5. Take photo / upload</b> JPG/PNG <b>7. Video call</b> <b>7. SMS</b> Code	<b>8. Email</b> Contract Copy



**BANK 8**

1. START	1. PERSONAL DETAILS	2. CONFIRM MY PERSONAL DETAILS	3. SIGN UP		4. HOW CAN I CONTINUE		
STEP 0	STEP 1	STEP 2	STEP 3	STEP 4	STEP 6	STEP 5	STEP 7
 <ul style="list-style-type: none"> <li>.Select the product</li> </ul>	<ul style="list-style-type: none"> <li>.Email</li> <li>.Name</li> <li>.Last name</li> <li>.Sex</li> <li>.Civil status</li> <li>.Birth country</li> <li>.Nationality</li> <li>.Tax residence country</li> <li>.Other tax residence</li> <li>.Address</li> <li>.City</li> <li>.Postal code</li> <li>.Work activity</li> <li>.Sector: public / private</li> <li>.Occupation</li> <li>.Company</li> <li>.Public functions</li> <li>.Personal phone / office phone / mobile phone</li> <li>.Would you like to add more holders?</li> <li>.Read &amp; agree with data protection</li> </ul>	<ul style="list-style-type: none"> <li>.Read &amp; agree with pre-contractual information</li> <li>.Account contract (download pdf)</li> <li>.Legal information (download pdf)</li> <li>.News &amp; charges board (download pdf)</li> <li>.Conflicts of interest policy summary (download pdf)</li> <li>.Read &amp; agree with all documents / conditions of my account.</li> </ul>	<ul style="list-style-type: none"> <li>.Currency</li> </ul>	<ul style="list-style-type: none"> <li>.This is your user / access code</li> <li>.This is your phone banking code</li> <li>.This is your account number</li> </ul>	<ul style="list-style-type: none"> <li>.Log in client area</li> </ul>	<ul style="list-style-type: none"> <li>.Looking for the customer care phone center</li> </ul>	<ul style="list-style-type: none"> <li>.Upload ID document</li> <li>.No instructions for uploading work evidence</li> </ul>
 <ul style="list-style-type: none"> <li>.Become a customer</li> <li>.Ring us up</li> </ul>							

TECHNOLOGY		7. Upload JPG/PNG
		

## 4. FINDINGS

LAST STEP\*

	PENDING STEPS	
	PC	MOBILE
<b>BANK 1</b>	BANK INTERNAL VALIDATION (up to 2 days)	BANK INTERNAL VALIDATION (up to 2 days)
<b>BANK 2</b>	BANK INTERNAL VALIDATION (up to 5 days)	BANK INTERNAL VALIDATION (up to 2 days)
<b>BANK 3</b>	BANK INTERNAL VALIDATION (up to 10 days)	NONE
<b>BANK 4</b>	NONE	BANK INTERNAL VALIDATION
<b>BANK 5</b>	NONE	NONE
<b>BANK 6</b>	-	-
<b>BANK 7</b>	The bank will make two transfers to the user, then she will have to access to the 'Client area' and confirm those amounts as a final validation.	NONE
<b>BANK 8</b>	NOT CLEAR	NO MOBILE PROCESS

## 4. TOOLS & PROVIDERS

### TECHNOLOGIES

With the exception of Santander and Openbank, the institutions do not provide consumers with the details of the third tech third party providers they use for their on-boarding processes. The table below describes the tools used but can not identify the specific providers:

	AUTHENTICATION > OTHER ACCOUNT	AUTHENTICATION > VIDEO CALL	DOCUMENTATION > UPLOAD	DOCUMENTATION > TAKE PHOTOS	DATA PROTECTION AGREEMENT	CONTRACT SIGNATURE
<b>BANK 1</b>	Upload bank transfer note	<b>O2Certify</b>	<b>Tiger</b> JPG/PNG	<b>Tiger</b> Only in mobile	SMS Code	SMS Code
<b>BANK 2</b>	Introduce IBAN	<b>Branddocs</b>	JPG/PNG	-	-	<b>DocuSign</b>
<b>BANK 3</b>	Introduce IBAN	Only in mobile Supplier no identified	JPG/PNG/PDF	Only in mobile	-	SMS Code
<b>BANK 4</b>	Introduce IBAN	Supplier no identified	JPG/PNG	Mobile > directly PC > directly/QR Reader	-	SMS Code
<b>BANK 5</b>	Introduce IBAN	Supplier no identified	JPG/PNG	Only in mobile	SMS Code	SMS Code
<b>BANK 6</b>	-	-	-	-	-	-
<b>BANK 7</b>	Introduce IBAN	Only in mobile Supplier no identified SMS Code	JPG/PNG	Only in mobile	-	SMS Code
<b>BANK 8</b>	-	-	JPG/PNG (at the client area)	-	-	-

---

**Annex 6:**  
**Dissenting opinions from**  
**members of the expert group**

***Expert group on electronic identification and remote KYC processes – comments  
by Austrian Financial Market Authority***

Priority group 1:

Overall, the report gives a general overview of some of the existing remote on-boarding solutions available in Europe (and to some degree about the usage of these solutions). Some parts of the report are very detailed and provide a comprehensive description of the different “journeys” (as the report labels the different procedures).

However, I have still some concerns about the publication of the whole report. The report e.g. highlights some private solutions but does not include all public and private procedures available in the different Member States. Furthermore, despite multiple comments made by myself, Austria is not included in all cases where remote on-boarding solutions are possible in Austria. In general, I have some concerns if the report covers all different remote on-boarding solutions in Europe. As I mentioned a few times in the past I would have preferred to have a breakdown/overview of the legal basis in all Member States regarding remote identification and which systems are used in the different Member States. This would be a good starting point for comparing the different implementations concerning remote identification by Member States.

Having said that, in my view the report provides a good basis for the European Commission for its further work to harmonize the on-boarding procedures (e.g. during a 6AMLD or an AML-Regulation). However, there would still be some work to do on the report before an endorsement and publication.

Bundesministerium der Finanzen, Germany

Priority Group 1 - Final report Priority Group 1's mandate was to draft a report to provide an overview and assessment of existing remote on-boarding solutions and the extent of their use by customers in the banking sector. The German delegation provided extensive commentary on the report, some of which has been incorporated into the final version of the document. However, concerns with regards to the final text remain. The report singles out particular private solutions, such as Verimi, which gives the impression that these are representative of the German market. It thereby fails to account for the full spectrum of public and private solutions that exist and falsely suggests higher prevalence/customer acceptance in the market for those cited. In addition, references in the text to eIDAS guidance supporting the determination of different levels of assurance (LOAs) are insufficiently comprehensive to ensure alignment with the eIDAS specifications. This creates confusion on the conformity of the LOAs cited with necessary security requirements. Finally, the report risks misrepresenting the German video identification which is currently a permitted procedure for remote identification.







