



Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU

FINAL REPORT

A study prepared for the European Commission

DG Communications Networks, Content & Technology by:



This study was carried out for the European Commission by:

PwC EU Services EEIG



Internal identification

Contract number: 30-CE-0839055/00-91

SMART number 2016/0094

DISCLAIMER

By the European Commission, Directorate-General for Communications Networks, Content & Technology.

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

ISBN 978-92-79-77867-4

doi:10.2759/94773

© European Union, 2018. All rights reserved. Certain parts are licensed under conditions to the EU.

Table of Contents

EXECUTIVE SUMMARY	6
RESUME EXECUTIF	9
CHAPTER 1 INTRODUCTION	12
OBJECTIVES.....	12
SCOPE	13
SHORT SUMMARY OF THE METHODOLOGY.....	15
STRUCTURE.....	16
CHAPTER 2 ON-BOARDING PROCESSES, REQUIREMENTS AND REGULATION	17
ON-BOARDING PHASES	17
EIDAS REGULATION	18
DOCUMENT CLASSIFICATION TYPES.....	20
KYC/AML REQUIREMENTS.....	21
CHAPTER 3 COMPLIANCE MEANS	25
REQUIRED ATTRIBUTES	25
IDENTITY ATTRIBUTES	25
KYC ATTRIBUTES	28
ON-BOARDING PROCESS REQUIREMENTS	29
VERIFICATION	30
COLLECTION.....	30
MANAGEMENT	31
SUMMARY	32
CHAPTER 4 KYC PROCESSES AND LOAS OF EIDAS	33
NON-DIGITAL AND MIXED PROCESSES.....	33
DIGITAL AND POTENTIAL DIGITAL	43
CHAPTER 5 FLOWCHART AND TEXT COMMENTARY	49
STRUCTURE AND NOTATION	51
ON-BOARDING OF A NATURAL PERSON.....	53
PHASE 1 - APPLICATION.....	55
PHASE 2 – VERIFICATION	56
PHASE 3 – COLLECTION	64
PHASE 4 – MANAGEMENT.....	65
ON-BOARDING OF A LEGAL PERSON	67
PHASE 1 - APPLICATION.....	69

PHASE 2 – VERIFICATION	69
PHASE 3 – COLLECTION	79
PHASE 4 - MANAGEMENT	80
FULLY DIGITAL CROSS-BORDER ON-BOARDING PROCESS FLOW	82
CHAPTER 6 CONCLUSION	85
GLOSSARY	87
ANNEX I EIDAS ELEMENTS AND MAPPING	89
EIDAS ELEMENTS	89
MAPPING OF EIDAS TO THE ON-BOARDING PROCESS	90
MAPPING OF EIDAS ELEMENTS AND ON-BOARDING PROCESS STEPS	90
MAPPING OF ON-BOARDING PROCESS STEPS TO REQUIREMENTS THAT MIGHT BE ADDRESSED BY EIDAS LOAS	91
MAPPING OF IDENTITY AND KYC ATTRIBUTES TO EIDAS SAML ATTRIBUTES PROFILE	94
ANNEX II AML REQUIREMENTS	97
EXAMPLES IN WHICH ELECTRONIC IDENTIFICATION MEANS ARE ALLOWED IN SOME OF THE SURVEYED MEMBER STATES INCLUDE:	97
EXAMPLES OF THE DIVERGENT CASES OF RECORD KEEPING OBSERVED IN SURVEYED MEMBER STATES:	97
EXTRACTS FROM THE DIRECTIVE (EU) 2015/849 ('4AMLD') AND PROPOSED AMENDMENTS (5AMLD) IN RELATION TO EIDAS	98
ANNEX III CONSOLIDATED FINDINGS	102
ANNEX IV COMMON AND DIVERGENT COMPLIANCE MEANS	105
VERIFICATION	105
COLLECTION	108
ANNEX V SAMPLE OF EMERGING DIGITAL SOLUTIONS	111
ANNEX VI BACKGROUND ON EUROPEAN PASSPORTS	113
ANNEX VII OPPORTUNITIES FOR THE FUTURE	115
KYC PORTABILITY	115
CROSS-BORDER OPPORTUNITIES AND INCENTIVES	115
KYC ATTRIBUTES	116

List of Tables

TABLE 1. THE PHASES OF ON-BOARDING IDENTIFIED FOR THE STUDY	17
TABLE 2. EIDAS LOAs IN THE CONTEXT OF AN ELECTRONIC IDENTIFICATION SCHEME	19
TABLE 3. OVERVIEW OF THE MANAGEMENT MECHANISMS FOR BOTH IDENTITY AND KYC ATTRIBUTES OF NATURAL AND LEGAL PERSONS.....	31
TABLE 4. MAPPING OF MIXED PROCESS STEPS IN ON-BOARDING OF A NATURAL PERSON TO DIGITAL PROCESS	35
TABLE 5. MAPPING OF MIXED PROCESS STEPS IN ON-BOARDING OF A LEGAL PERSON TO DIGITAL PROCESS.....	38
TABLE 6. DESCRIPTION OF POTENTIAL FULLY DIGITAL PROCESS STEPS IN ON-BOARDING OF A NATURAL PERSON.....	43
TABLE 7. DESCRIPTION OF POTENTIAL FULLY DIGITAL PROCESS STEPS IN ON-BOARDING OF A LEGAL PERSON.....	47
TABLE 8. FLOWCHART SYMBOLS	51
TABLE 9. KEY TERMS DESCRIPTION	87
TABLE 10. EIDAS KEY ELEMENTS OVERVIEW	89
TABLE 11. MAP OF ON-BOARDING PROCESS STEPS TO THE EIDAS LOAs ELEMENTS	90
TABLE 12. MAPPING OF ON-BOARDING PROCESS STEPS TO REQUIREMENTS THAT MIGHT BE ADDRESSED BY EIDAS LOAs FOR NATURAL PERSONS.....	91
TABLE 13. MAPPING ON-BOARDING PROCESS STEPS TO REQUIREMENTS THAT MIGHT BE ADDRESSED BY EIDAS LOAs FOR LEGAL PERSONS.....	92
TABLE 14. MAPPING OF IDENTITY ATTRIBUTES TO EIDAS SAML ATTRIBUTES.....	94
TABLE 15. MAPPING THE MINIMUM DATA SET FOR A NATURAL PERSON IDENTITY ATTRIBUTES FOLLOWING REGULATION 2015/1501 TO EIDAS SAML ATTRIBUTES.....	94
TABLE 16. MAPPING THE MINIMUM DATA SET FOR A LEGAL PERSON IDENTITY ATTRIBUTES FOLLOWING REGULATION 2015/1501 TO EIDAS SAML ATTRIBUTES	95
TABLE 17. NATURAL PERSON ATTRIBUTES USED BY SURVEYED FINANCIAL INSTITUTIONS	102
TABLE 18. LEGAL PERSON ATTRIBUTES USED BY SURVEYED FINANCIAL INSTITUTIONS	103
TABLE 19. NATURAL PERSON IDENTITY ATTRIBUTES VERIFICATION MECHANISMS	105
TABLE 20. LEGAL PERSON IDENTITY ATTRIBUTES VERIFICATION MECHANISMS	106
TABLE 21. NATURAL PERSON KYC ATTRIBUTES VERIFICATION MECHANISMS.....	106
TABLE 22. LEGAL PERSON KYC ATTRIBUTES VERIFICATION MECHANISMS	106
TABLE 23. NATURAL PERSON IDENTITY ATTRIBUTES COLLECTION MECHANISMS.....	108
TABLE 24. LEGAL PERSON IDENTITY ATTRIBUTES COLLECTION MECHANISMS	109
TABLE 25. NATURAL PERSON KYC ATTRIBUTES COLLECTION MECHANISMS.....	109
TABLE 26. LEGAL PERSON KYC ATTRIBUTES COLLECTION MECHANISMS	109
TABLE 27. SAMPLE EMERGING DIGITAL SOLUTIONS SAMPLE	111

List of Figures

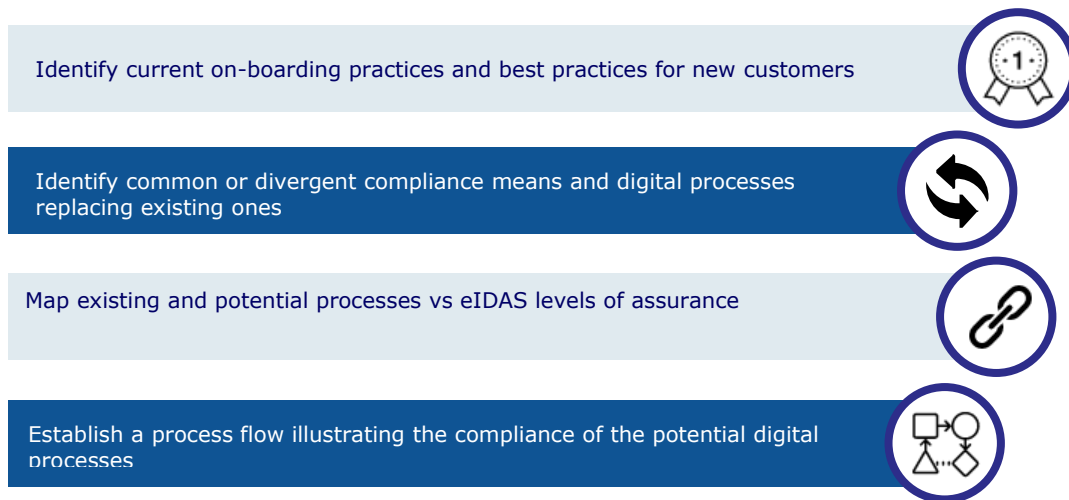
FIGURE 1. EIDAS ELECTRONIC IDENTIFICATION SCHEME PROCESS TO OBTAIN AN ELECTRONIC IDENTIFICATION MEANS TO BE USED FOR AUTHENTICATION	18
FIGURE 2. NATURAL AND LEGAL PERSON IDENTITY ATTRIBUTES.....	26
FIGURE 3. OVERVIEW OF THE COMMON AND DIVERGENT IDENTITY ATTRIBUTES USED FOR A NATURAL AND A LEGAL PERSON AT THE SURVEYED FINANCIAL INSTITUTIONS.....	27
FIGURE 4. NATURAL AND LEGAL PERSON KYC ATTRIBUTES.....	28
FIGURE 5. OVERVIEW OF THE COMMON AND DIVERGENT KYC ATTRIBUTES FOR A NATURAL AND LEGAL PERSON.....	29
FIGURE 6. OVERVIEW OF COMMON AND DIVERGENT MECHANISMS USED FOR ON-BOARDING	32
FIGURE 7. SAMPLE WORKFLOW FOR ESTABLISHING A RELATIONSHIP WITH A CUSTOMER ONLINE.....	49
FIGURE 8. EIDAS CONTRIBUTION TO CUSTOMER ON-BOARDING PROCESS.....	50
FIGURE 9. ON-BOARDING PROCESS FOR A NATURAL PERSON	53
FIGURE 10. VERIFICATION OF DOCUMENT'S AUTHENTICITY AND THE APPLICANT'S IDENTITY.....	56
FIGURE 11. AUTHENTICITY CHECK – DOCUMENT TYPE 2/3	57
FIGURE 12. IDENTITY CHECK – DOCUMENT TYPE 2/3	59
FIGURE 13. FRAUD CHECK OF THE DOCUMENT	61
FIGURE 14. FRAUD/PEP CHECK OF THE APPLICANT	62
FIGURE 15. COLLECT INFORMATION.....	64
FIGURE 16. MANAGE INFORMATION.....	65
FIGURE 17. ON-BOARDING PROCESS FLOW OF A LEGAL PERSON.....	67
FIGURE 18. VERIFICATION THE DOCUMENT'S AUTHENTICITY AND THE APPLICANT'S IDENTITY	69
FIGURE 19. AUTHENTICITY CHECKS OF THE DOCUMENTS	70
FIGURE 20. IDENTITY CHECK OF THE APPLICANT, BENEFICIARIES AND LEGAL REPRESENTATIVE.....	72
FIGURE 21. FRAUD CHECK OF THE DOCUMENTS.....	75
FIGURE 22. FRAUD/PEP CHECKS OF THE APPLICANT, BENEFICIARIES AND LEGAL REPRESENTATIVE.....	76
FIGURE 23. COLLECT INFORMATION.....	79
FIGURE 24. MANAGE INFORMATION.....	81
FIGURE 25. ONLINE ON-BOARDING PROCESS – ALTERNATIVE PROCESS.....	82
FIGURE 26. GEOGRAPHIC SPREAD AND DIVISION OF FINANCIAL INSTITUTIONS THAT PARTICIPATED IN THE STUDY	102
FIGURE 27. MACHINE READABLE PASSPORTS	113

EXECUTIVE SUMMARY

This report is the outcome of the SMART 2016/0094 study on eID and digital on-boarding¹.

The eIDAS Regulation (Regulation EU No 910/2014) is a major step towards building the Digital Single Market (DSM). It has the potential to allow financial institutions to more easily meet the legal obligations in the fields of know-your-customer (KYC), of Anti-Money Laundering (as per the 4th Anti-Money Laundering Directive, 4AMLD), and of strong authentication of parties (as per the Payment Services Directive 2, PSD2).

The objectives of the study were to:



The study consists of four tasks that broadly correspond to the objectives outlined above.

The identification of current on-boarding practices and best practices combined desk research and interviews of eleven financial institutions from European Member States. This included both traditional financial institutions and financial institutions with only an online presence. Analysis allowed to consolidate both the common and divergent on-boarding mechanisms. This demonstrates that direct reliance on a copy of a government issued document is the common verification mechanism, and a face-to-face meeting is the common collection mechanism. The situation diverges in case the financial institution has no physical office, and the interaction takes places electronically. For the overview of common and divergent mechanisms used for on-boarding please refer to *Chapter 3 Compliance means, Figure 6*. The main factors underlying the differences regarding the use of compliance means at the surveyed

¹ On-boarding in the banking sector means a process which precedes entering into a business relationship with a new customer. If the on-boarding process is done electronically and at a distance (e.g. online), it is referred to as digital on-boarding.

financial institutions relate to local legislation, technology maturity and third-party available solutions in the different Member States.

Some of the surveyed institutions already employ innovative technologies developed by third-party providers for both the verification and collection of customer information, such as Member State specific eID solutions, high quality video call and photo, and third-party tokens. The fact that such technical solutions are allowed locally by the AML law in certain Member States increases the opportunity for the digitalisation of the (remote) on-boarding process, also across borders. The use of a centralised electronic repository accessible at company-wide level, i.e. by different local branches located in different countries, facilitates information sharing and portability.

The common process steps for on-boarding of natural and legal persons by the surveyed financial institutions can be summarised in four phases. These are Application, Verification, Collection and Management, as described in *Table 1. The phases of on-boarding identified for the study* are outlined in *Chapter 2 On-boarding processes, requirements and regulation*.

On-boarding processes of financial institutions can benefit from using identification means provided under eIDAS notified schemes. For the purpose of the study, a classification of document types based on best practice was introduced. This classification can be summarised as follows:

- Type 1 Physical document without Machine Readable Zone (MRZ) or chip;
- Type 2 Physical document with Machine Readable Zone;
- Type 3 Physical document with both MRZ and chip;
- Type 4 Logical document, implemented in digital media only.

The digitalisation of the on-boarding process steps allows financial institutions to increase their outreach. Digitalising the verification and collection steps will reduce the burden of potentially error-prone manual process steps. However, it is important to guarantee a high level of assurance regarding the claimed identity and authenticity of the provided documents. Several digital solutions existing today already support an innovative digital on-boarding process. They can simplify the verification and collection steps for both the user (i.e. applicant) and their clients (i.e. financial institution). The use of eIDAS compliant means can further enhance the portability of verified identity information across Member States.

The analysis performed demonstrates that it is reasonable to conclude that eIDAS compliant means can support the verification steps of the on-boarding processes for the electronic identification of natural and legal persons. The appropriate level of assurance can be selected by the financial institutions, according to their risk management.

The main potential contribution of eIDAS to on-boarding processes is illustrated in *Figure 8. eIDAS contribution to customer on-boarding process* in *Chapter 5 Flowchart and Text commentary*. The flowcharts indicate where and how eIDAS can contribute in

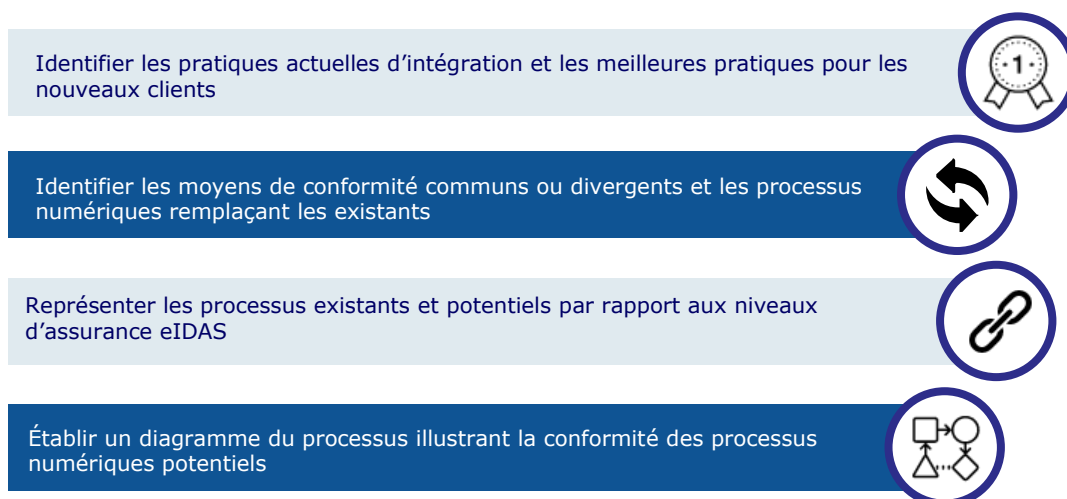
each on-boarding phase, both for natural and legal persons. These flowcharts can be used to evaluate where electronic on-boarding can benefit from the legal effects brought about by the eIDAS Regulation. For cross-border on-boarding, a fully digital process can be envisaged. This would make use of the network of eIDAS nodes which is currently being constructed.

RESUME EXECUTIF

Ce rapport est le résultat de l'étude SMART 2016/0094 concernant l'eID et l'intégration numérique².

Le Règlement eIDAS (Règlement UE No 910/2014) constitue une étape cruciale vers la mise en place du Marché Unique Numérique (MUN). En effet, elle offre la possibilité aux institutions financières de satisfaire, de manière simplifiée, aux obligations juridiques dans les domaines d'identification des clients ("connaître son client" "know-your-customer" ou "KYC"), de la lutte contre le blanchiment d'argent (Conformément à 4ème directive relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement, 4AMLD) et de l'authentification forte des parties (conformément à la directive sur les services de paiement 2, DSP2).

Les objectifs de l'étude étaient les suivants:



L'étude a été menée en quatre tâches correspondant globalement aux objectifs cités ci-dessus.

L'identification des pratiques actuelles d'intégration et des meilleures pratiques s'est reposée sur la recherche documentaire et les entretiens de onze institutions financières faisant parties des Etats Membres européens. L'échantillon sélectionné incluait aussi bien des institutions financières traditionnelles ainsi que des institutions financières ne proposant leurs services qu'exclusivement en ligne. L'analyse a permis d'identifier les processus d'intégration communs ainsi que les processus divergents comme illustré dans la figure ci-dessus. Les résultats de l'analyse ont aussi mis en lumière que le processus général d'intégration repose sur l'obtention d'un document émis par un gouvernement/une autorité officielle, et que celui-ci est généralement collecté via un entretien en face-à-face. Cependant, la situation est différente lorsque l'institution financière ne dispose pas de bureaux physiques, et que la communication est effectuée via des moyens électroniques. Pour un aperçu des processus communs

² L'intégration bancaire est un processus qui précède l'établissement d'une relation professionnelle avec un nouveau client. Si le processus d'intégration est effectué électroniquement et à distance (par exemple, en ligne), on parle d'intégration numérique.

et divergents, veuillez-vous référer au *Chapitre 3 Moyens de conformité, Figure 6*. Les principaux facteurs qui sont à l'origine des divergences concernant l'utilisation des moyens de conformité au sein des institutions financières interrogées, concernent la législation locale, la maturité quant à l'utilisation de la technologie et les solutions diverses disponibles dans les Etats Membres.

Certaines institutions interrogées utilisent déjà des technologies innovantes développées par des fournisseurs de services externes pour la vérification et la collecte d'informations sur les clients, comme des solutions eID spécifiques aux Etats Membres, des appels en vidéo, des photos en haute définition/qualité, ou encore d'autres éléments d'identification fournis par des parties tierces (third-party token). Le fait que de telles solutions techniques soient autorisées par la loi sur l'anti-blanchiment dans certains Etats Membres, augmente les possibilités de numérisation du processus d'intégration (à distance), y compris au-delà des frontières. L'utilisation d'un répertoire électronique centralisé accessible au niveau groupe (le cas échéant), c'est-à-dire par les filiales locales situées dans des pays tiers, facilite le partage ainsi que la portabilité de l'information.

Les étapes du processus d'intégration par les institutions financières interrogées, communes aux personnes physiques et aux personnes morales: Sollicitation, Vérification, Collecte d'informations, et Gestion. Elles sont résumées dans la *Tableau 1 (Table 1). Phases d'intégration identifiées pour l'étude* repris dans le *Chapitre 2. Processus d'intégration, exigences et réglementation*.

L'utilisation de solutions d'identification prévues dans le cadre des systèmes eIDAS représente un avantage en ce qui concerne les processus d'intégration des clients par les institutions financières. Pour les fins de l'étude, une classification des types de documents, basée sur la meilleure pratique, a été introduite. La classification utilisée peut être résumée comme suit:

- Type 1 Document physique sans zone de lecture automatique - "Machine Readable Zone" (MRZ) - ou puce électronique;
- Type 2 Document physique avec MRZ;
- Type 3 Document physique avec MRZ et puce électronique;
- Type 4 Document logique, implémenté dans un support numérique uniquement.

La transformation numérique des étapes du processus d'intégration permet aux institutions financières d'accroître leur portée. La numérisation des étapes (phases) de vérification et de collecte réduit les lourdes tâches liées aux étapes manuelles du processus, qui pourraient être sujettes à des erreurs. Cependant, il est primordial de garantir un degré élevé d'assurance concernant l'identité prétendue et l'authenticité des documents fournis. Plusieurs solutions digitales supportent déjà, aujourd'hui, un processus d'intégration numérique innovant. Elles permettent de simplifier les étapes de vérification et de collecte aussi bien pour l'utilisateur (c'est-à-dire un sollicitant) que pour l'institution financière. L'utilisation de solutions conformes à eIDAS permet de renforcer la portabilité des informations d'identité vérifiées à travers les Etats Membres.

L'analyse effectuée montre qu'il est justifié de conclure que les solutions conformes à eIDAS participent à faciliter les étapes de vérification des processus d'intégration pour l'identification électronique des personnes physiques et morales, avec le niveau d'assurance requis par les institutions financières selon leur gestion des risques.

Le principal apport potentiel d'eIDAS aux processus d'intégration est illustré dans la *Figure 8. Contribution d'eIDAS au processus d'intégration des clients* repris dans le *Chapitre 5. Organigramme et Commentaire de texte*. Des organigrammes ont été développés pour indiquer où et comment eIDAS peut contribuer à chaque phase d'intégration, à la fois pour les personnes physiques et les personnes morales. Ces organigrammes peuvent être utilisés afin d'évaluer à quel niveau l'intégration électronique peut bénéficier des effets juridiques induits par le règlement eIDAS. Pour une intégration au-delà des frontières (international, transfrontalière), un processus entièrement numérique peut être envisagé. Cela permettrait d'utiliser le réseau eIDAS, actuellement en cours de construction.

CHAPTER 1 INTRODUCTION

This report is prepared in the context of the SMART 2016/0094 study on "eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the European Union".

The eIDAS Regulation (EU) 910/2014³ (hereafter denoted as 'eIDAS Regulation') is a major step towards building the Digital Single Market (DSM) as it provides a predictable regulatory environment for the cross-border recognition of electronic identification (eID) and electronic trust services. eIDAS may allow to easily meet the legal obligations in the banking/financial sector, concerning security, know-your-customer, strong authentication of parties and interoperability, e.g. as provided under the Directive (EU) 2015/849⁴ (4th Anti-Money Laundering Directive, hereafter denoted as '4AMLD') and the Directive 2007/64/EC⁵ (2nd Payment Services Directive, hereafter denoted as 'PSD2').

Objectives

To further enhance the Single Market in retail financial services, providers and consumers should be able to offer/purchase retail financial products remotely and across borders in full compliance with anti-money laundering requirements. These requirements include customer due diligence (CDD) that has to be carried out by providers while entering into a business relationship with a customer as well as throughout the entire relationship.

Technological changes enable remote identification through new modalities. However, based on the recent public consultation on retail financial services, providers often reported that there are barriers caused by divergent rules or practices and that further initiatives should be taken with regards to remote identification to help them offer cross-border services. Moreover, it was noted that current supervisory and business practices greatly vary across Europe.

³ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, available at: <http://data.europa.eu/eli/reg/2014/910/oj>

⁴ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>

⁵ Directive (EU) 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, available at: <http://data.europa.eu/eli/dir/2007/64/oj>

The specific objectives of the SMART 2016/0094 study are to:

- Identify current on-boarding practices as well as best practices, including the legal requirements within the Member States, possible guidelines used and the regulatory requirements of the national regulators.
- Identify where there are common or divergent compliance means, and where digital processes might replace existing non-digital processes. Where this is considered not to be possible, the reasons why a digital process cannot be used need to be indicated.
- Map the existing physical vs digital processes and the potential digital processes against eIDAS Levels of Assurance (LoAs).
- Produce a process flow and text commentary illustrating the compliance of the potential digital processes against the sector-specific regulatory requirements.

Scope

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

Dimension	
Products and services	The study is focused on the on-boarding process at retail banks, specifically on customer due diligence and know-your-customer requirements. All eID means are in scope of the study.
Supply and demand side	The study is mainly focused on the banks and financial institutions that can benefit from the use of eID means. Solution providers have been interviewed in order to identify existing on-boarding solutions.
Time	The study covers regulations and best practices existing at the time of conducting Task 1 of the study (January – March 2017) as well as observation of the ongoing trends and envisaged changes.
Geography	The geographical scope of this study is the European Union (EU).
Stakeholders	Interviews of different stakeholders in 10 Member States: <ul style="list-style-type: none"> • 11 financial institutions; • 5 regulators and supervisors; • 6 other stakeholders (including solution providers and professional associations) The interviews were accompanied by the desk research of AML legislation in 12 Member States.

This report includes the results of the analyses conducted between the inception meeting of this project that took place in Brussels on January 16, 2017 and the date of submission of this report in November 2017.

Short summary of the methodology

The study was divided into four tasks:

Task 1 – Identifying current on-boarding practices for new customers

In this task, an inventory was created of current mandatory legal and regulatory requirements for customer on-boarding; existing guidance from national supervisors as well as an inventory of prospective amendments due to the forthcoming implementation of 4AMLD; and the Commission's proposal for a Directive amending 4AMLD (hereafter denoted as '5AMLD'⁶). Also, an inventory was created of current practices in customer on-boarding procedures, based on interviews with financial institutions, regulators and technology providers. Finally, the standard identity attributes and additional attributes (required for enhanced due diligence) were identified, including how this information is verified and goes through a validity check, and the procedure for the collection and management of evidence.

The resulting datasets were delivered to the European Commission and served as input for the subsequent tasks and their deliverables, which are summarized in this report.

Task 2 – Compliance means and digital processes

In this second task, the existing compliance means were analysed. Furthermore, an analysis of potential digital processes replacing existing non-digital processes was conducted.

Task 3 – Mapping of existing physical vs digital processes and potential digital processes against eIDAS Levels of Assurance

In this third task, the existing processes were mapped to potential fully digital processes. Additionally, potential digital processes were mapped against the different elements of the eIDAS LoA.

Task 4 – Process flow / text commentary illustrating the compliance of digital and potential digital processes against sector-specific regulatory requirements

In this final task, flowcharts and text commentary were produced for digital and potentially digital processes.

All findings which resulted from the study are covered in this report. A public validation workshop was held on 4 October 2017 at the European Commission's premises in Brussels.

⁶ Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, available at: http://eur-lex.europa.eu/procedure/EN/2016_208

Structure

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

- **Chapter 2** introduces on-boarding process phases, the concepts related to eIDAS regulation (the electronic identification process, associated levels of assurance), provides document types classification and describes the regulatory KYC/AML requirements.
- **Chapter 3** presents the common and divergent on-boarding compliance means based on the results from the surveyed financial institutions from Task 1. The analysis of the common and divergent on-boarding processes is part of Task 2 and followed the approach below:
 - Distinguish the required attributes for on-boarding in two types: identity and KYC related attributes.
 - Analyse the common and divergent identity and KYC attributes used by financial institutions for both a natural and a legal person.
 - Examine the common and divergent mechanisms used during the processes of verification, collection and management.
- **Chapter 4** consolidates the results from Task 3 by analysing the existing on-boarding processes and the potential digital processes. The existing on-boarding processes are mapped onto fully digital processes and the digital and potential digital processes mapped to the eIDAS Regulation LoAs.
- **Chapter 5** summarises the results of Task 4, providing the flowcharts describing how (future) fully digital customer on-boarding could be performed.
- **Chapter 6** concludes this report by presenting the interim conclusions of the study.

Additional and more detailed results of the different tasks are available in the Annexes. Annex I provides the eIDAS Regulation elements and describes the mapping to the on-boarding process steps and to the identity attributes. Annex II describes the AML requirements. Annex III consolidates the findings from Task 1 and Annex IV describes the common and divergent compliance means. Annex V illustrates a sample of possible emerging digital technology providers and Annex VI gives a short background on European passports. Finally, Annex VII provides an overview of opportunities for the future, which are based on the conclusions of the different break-out sessions held during the validation workshop.





CHAPTER 2 ON-BOARDING PROCESSES, REQUIREMENTS AND REGULATION

This section introduces the on-boarding process phases, the eIDAS Regulation along with the levels of assurance and electronic identification means, classification of identification document types in use, and AML regulatory requirements.

On-boarding phases

The on-boarding process implements the requirements and procedures used by financial institutions for the enrolment of potential clients. For the purpose of the study, the on-boarding process was divided into the following four process phases: application, verification, collection and management, described in more detail in the table below.

Table 1. The phases of on-boarding identified for the study

Phase	Description
	Pre-on-boarding phase, addressing the act of applying to become a client. In this phase, the applicant provides the required identity and KYC attributes for later verification and collection.
	The verification phase determines whether the expected requirements and mechanisms used to perform verification of attributes are met. It can be divided into 3 steps: <ol style="list-style-type: none"> Authenticity check of documents (to determine that the document can be considered a trustworthy source of information such as for identity attributes). Identity check of the applicant (comparison of the bearer of the document against the owner of the document). Anti-fraud check (to determine the document is not used in fraud-related activities and it belongs to a living person; and that the applicant is not involved in fraud activities, not under sanctions or considered a PEP).
	During this phase the attributes are collected and documented.
	In this phase the collected attributes are managed. This phase may be recurring.

It is important to note that the collection and verification can be performed as a single phase, denoted as 'verify while collect'. However, in this document the two process phases are examined separately.

eIDAS Regulation

The eIDAS Regulation ensures the cross-border recognition of electronic identification means of natural and legal persons within the EU, as well as the trust services⁷ for electronic transactions. The present document focuses on the electronic identification process.

Member States or Member States' mandated or recognised authorities are the entities responsible for issuing the electronic identification. The electronic identification means are issued via an electronic identification scheme and can later be used for electronic identification processes allowing the authentication of natural or legal persons. The electronic identification scheme according to the eIDAS Regulation is summarised in the figure below.

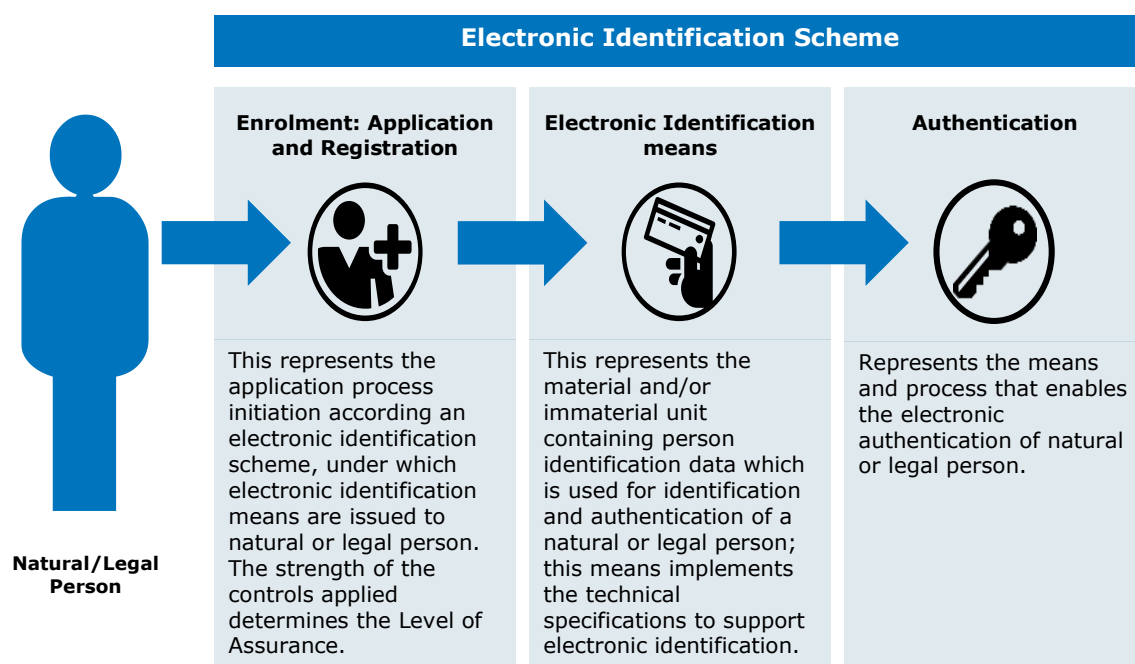


Figure 1. eIDAS electronic identification scheme process to obtain an electronic identification means to be used for authentication





To determine the quality of the personal identification data represented in the electronic identification means, the eIDAS Regulation distinguishes three different levels of assurance (LoAs) defined by the electronic identification scheme. The LoAs depend on the degree of confidence that electronic identification means provide in the claimed identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. The accompanying Implementing Regulation defining the LoAs for electronic identification means (Regulation

⁷ Trust services, according to the Regulation (EU) 910/2014, are: electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication

2015/1502⁸) provides an overview of the minimum technical specifications and procedures for the different levels along with the different key elements (Annex I). The different LoAs provide a low, substantial or high degree of confidence in the claimed or asserted identity of a person. They are characterised with reference to technical specifications, standards and procedures, including technical controls. The purpose of these controls is to decrease the risk of misuse or alteration of identity.

The table below summarises the key characteristics for the different LoAs⁹.

Table 2. eIDAS LoAs in the context of an electronic identification scheme

 eIDAS LOAs	Description
Low 	Low provides a limited degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by assuming the following: <ul style="list-style-type: none"> • Possession of an evidence recognised by a Member State, • The evidence is genuine, • Existence of the identity claimed.
Substantial 	Substantial provides a substantial degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by the level Low plus the verification of the following: <ul style="list-style-type: none"> • Possession of an evidence recognised by a Member State and check of the attributes representing the claimed identity, • Check if the evidence is genuine
High 	High provides a higher degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by the level Substantial plus at least one of the following: <ul style="list-style-type: none"> • Possession of a photo or biometric identification evidence recognised by a Member State and the claimed identity is checked through a comparison with one or more physical characteristics. • Checked by procedures employed by a public or private entity in the same Member state that provide an equivalent level, • The electronic identification means is issued on the basis of a notified electronic identification means with a High LoA.

According eIDAS' Article 6, Member States will have to recognise other notified Member States' means that are qualified 'High' or 'Substantial' by September 2018.

The mapping between the eIDAS elements and the on-boarding process steps as well as a more in-depth description of the LoAs requirements is available in Annex I.

We observed there can be a technical overlap between electronic identification and electronic signatures and trust services. In order to participate in an electronic identification, natural and legal persons are required to hold an electronic identification means (e.g. identification token) containing the electronic representation of the person identification data (i.e. the data set representing the identity of a

⁸ Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

⁹ For an overview of all the characteristics required for each of the three LoAs, please consult the Commission Implementing Regulation (EU) 2015/1502. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

natural or legal person). Technical overlaps include, among others, those cases where Member States combine an eID token with a Signature Creation Device, where the two functions might even share the same PIN. Another technical overlap is the common use of trust services to contribute in guaranteeing a LoA by using an electronic signature or seal over the file system where the identity attributes are stored; as well as the use of trust services during the execution of a challenge response protocol resulting in convincing a verifier of the authenticity of a claimant's identity.

Document classification types

For the purpose of the study and based on best practice, the present report considers four types of documents in use, from a physical only version (type 1) to a digital only version (type 4). The present study report only addresses and considers identification/authentication and does not address any signature and other trust services aspects. These types are:

- **Type 1** – A physical document that is not machine readable (i.e. does not have a Machine Readable Zone, MRZ), nor electronically readable (i.e. does not have a chip). This type represents physical only documents that can be digitalised through scanning or photographing. Since it is not possible to interact in an electronic way with such a document, it is considered outside the scope of eIDAS. However, it can be used in KYC and AML procedures. Within the EU, at the time of performing the present study, such documents were the exception rather than the rule.
- **Type 2** – A physical document that is machine readable. This MRZ can be read using Optical Character Recognition (OCR) technology. The document contains a picture of the holder. Such documents are in use today in Member States. Strictly speaking they do not fall within the scope of eIDAS since they are not electronically readable. However, similar to type 1 documents, they are in use in current KYC and AML procedures.
- **Type 3** – A physical document which is both machine-readable and electronically readable. This includes the most recent passports and eID cards which have both a MRZ and a chip. The chip can be interacted with either contact-based or contactless. Such documents fall within the scope of eIDAS, and it is up to the issuing Member State to notify (or not). For usage in KYC and AML procedures, the decision to take reliance on such a document is a discretionary decision of the financial institution performing the on-boarding. The general expectation is that in this case, the document is qualified by an eIDAS LoA of Substantial or High.
- **Type 4** – A 'logical document', implemented in digital media only. Such an electronic identification means consists of personal identification data attributes stored within a secured enclave implemented in digital media (e.g. an app on a mobile device). These electronic identification means have no physical representation and are only electronically readable (i.e. digital only). They may rely on technology which is not yet commonplace for eID means in

the public sector today, such as mobile applications. It can be assumed such means might increasingly be used. From an eIDAS and KYC/AML perspective, they are treated on equal footing as a Type 3 document. This means it is up to the issuing Member State to notify it as an official eID means, with a specific LoA.

The electronic identification means of the document types 2 and 3 can be represented in different digital forms and information can be extracted via a digital copy, via video technology or using eID protocols. For type 4, service providers generate the electronic identification means directly in digital format. Various Member States have electronic identification schemes issuing different electronic identification means under a single denominator. For instance, Sweden admits the BankID¹⁰ solution as an electronic identification means issued with different implementation solutions options. The different implementations include soft token (i.e. a private key storage in file complemented by a digital certificate) as well as a smart card and mobile application based solutions. However, at the time of compilation of this report none of the BankID solution options were listed on the PRADO website as an official Swedish identity document. For the purpose of this report, the BankID solution is considered to be a potential type 4 document given the digital only representation. However, to the understanding of the study team, the support of the solution is limited to Sweden and not cross-border.

KYC/AML requirements

During the research part of the study (performed in a course of Task 1) the current state of legal and regulatory AML requirements applicable at national level were identified. Further in this section we provide insight into the (potential) future state of the AML legislation which proposes to include electronic identification and trust services as a relevant means to fulfil KYC/AML requirements.

By understanding the AML requirements, a link can be made where eIDAS Regulation can provide support of the KYC requirements and what levels of assurance as per eIDAS can be accepted under AML legislation.

¹⁰ Available at: <https://www.bankid.com/en/>

Current legal and regulatory requirements for on-boarding

Financial institutions apply several AML requirements identified in local AML legislations which are developed in line with the FATF Recommendations¹¹; the Directives 2005/60/EC¹² (hereafter denoted as '3AMLD'); and the Directive 2006/70/EC¹³.

Prior requirements to customer due diligence (CDD) is to establish a business relationship only with identified natural or legal persons. Strong identification as well as verification of the provided information should be performed irrespectively of the on-boarding method, namely: face-to-face or remotely. The common due diligence measures include:

- identification of the natural and legal person on the basis of documents and data submitted; and verification of the submitted information on the basis of information obtained from a reliable and independent source;
- identification and verification of the legal representative and the right of representation;
- identification of the beneficial owner, based on information provided for on-boarding or obtained from another reliable and independent source; and
- obtaining information on the purpose and nature of the business relationship or transaction.

The enforcement of the due diligence measures is required for completing the on-boarding process since the relationship with the financial institution cannot be established in the following cases:

- an anonymous or unidentified person; or
- a person that fails to submit sufficient information required for customer due diligence, e.g. identity information; or
- a failure of the veracity or authenticity of the documents or data.

¹¹ International standards on combating money laundering and the financing of terrorism and proliferation, February 2012 with the following amendments, available at: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

¹² Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:en:PDF>

¹³ Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0070>

On the subject of remote on-boarding, common AML requirements are that financial institutions shall take extra CDD steps to compensate the associated risk by applying additional due diligence measures (i.e. enhanced customer due diligence, EDD). The additional measures usually are:

- obtaining an additional supporting evidence (e.g. a certified copy of an identity document) allowing to confirm the identity of the person;
- the first payment must be from a client account in the European Union; or
- receiving a validation of the client's identity by a third party (financial institution).

Some of the surveyed Member States allow the use of electronic identification means for remote on-boarding, providing a possibility for eIDAS to be used in the future to support the on-boarding process (please refer to the examples in Annex II). However, there is no common approach applied in the surveyed Member States on which electronic identification means are accepted and what are the requirements to these. Also the process differs per Member State. For electronic verification of identity, the financial institutions can perform on-boarding themselves or use a third party provider.

In order to understand where an electronic means and a digital process can support AML requirements to collection and management of information, the current record-keeping requirements as per AML legislation were studied. The following approach is commonly required by local AML regulations within the surveyed Member States:

- At on-boarding of natural persons, an officer of the financial institution shall make a copy of the page(s) of a government issued document submitted for identification which contains the identity attributes and a photograph.
- At on-boarding of legal persons, copies of government issued documents submitted for identification and verification (including documents required for identification and verification of beneficial owners) as well as for establishment of business relationship should be collected.
- The document storage period is defined on national level, and can vary among Member States. But based on the FATF Recommendations it should not be less than 5 years after termination of a business relationship.

The usage of technologies, such as computer network access to electronic databases, video conference on-boarding or eID solutions, allowed for remote on-boarding by the AML legislation, lead to divergent cases of record-keeping observed in Member States which are presented in Annex II.

Prospective and potential amendments to AML legislations on the Member State level

Following the development of the financial service industry and technologies, a new 4AMLD has been proposed. This directive replaced 3AMLD and Directive 2006/70/EC. The 4AMLD entered into force as of June 26, 2017. Please note that at the time we conducted the inventory of current AML requirements in the selected Member States,

the 4AMLD was not yet in force and not yet (fully) transported to local AML legislation at the Member State level.

Although 4AMLD does not yet introduce the possibility to employ eIDAS for customer on-boarding purposes, it proposes several amendments related to the identification of beneficial owners which can be supported by eIDAS Regulation. Specifically, the Directive suggests to create a central beneficial owner register at the national level to increase transparency across Member States (see Article 13, Article 14, Article 30 detailed in the Annex II). In respect of these amendments, eIDAS can serve as a trusted source of identification and verification of beneficial owners and therefore, help financial institutions to mitigate risk of fraud while confirming the beneficial owner's identity. Another proposition of the Directive is to set the required record-keeping period to five years after the end of the business relationship with their customer or after the date of an occasional transaction, and to delete personal data upon expiry of that retention period. If the national law determines the circumstances to further retain the data, this retention period could be exceeded to five additional years maximum (see Article 40 detailed in the Annex II).

In 2016, the Commission proposed a set of additional amendments to 4AMLD in order to enhance the measures to combat money-laundering and financial terrorism. The European Compromise text issued in October 28, 2016 (denoted as '5AMLD'¹⁴) introduces amendments related to the use of electronic identification and trust services (as per the eIDAS Regulation) for KYC on-boarding, accessing funds and/or tracing electronic transactions. This suggests an amendment to 4AMLD in line with the legal framework on mutual recognition of notified eID schemes and means.

[Recital 17:

Accurate identification and verification of data of natural and legal persons is essential for fighting money laundering or terrorist financing. Latest technical developments in the digitalisation of transactions and payments enable a secure remote or electronic identification. Those means of identification as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council should be taken into account, in particular with regard to notified electronic identification schemes and means that offer high level secure tools and provide a benchmark against which assessing the identification methods set up at national level may be checked. Therefore, it is essential to recognise secure electronic copies of original documents as well as electronic assertions, attestations or credentials as valid means of identity.]

The overview of proposed amendments to articles of 4AMLD in the relation to eIDAS is described in Annex II.

¹⁴ Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, available at: http://eur-lex.europa.eu/procedure/EN/2016_208




CHAPTER 3 COMPLIANCE MEANS

This section presents the analysis of the existing common and divergent compliance means¹⁵ used for the on-boarding process at different surveyed financial institutions, for natural and legal persons. The analysis describes the mechanisms used for the identity and KYC attributes of natural and legal persons during the on-boarding process.

Furthermore, this analysis also includes the details on dependencies from third parties (e.g. financial-institution-on-financial-institution or financial-institution-on-third-party-service-provider) and the re-use of information from other processes, such as portability of the on-boarding information.

Required attributes

For the purpose of this analysis, the different required attributes are distinguished as two types: identity and KYC related attributes, as defined below.

 Attributes	Description
<p>Identity</p> 	The identity attributes required for a natural person or for a legal person are defined by Member State legislation. For natural persons it includes, among others: Name, Address, Date of Birth, Nationality, and Occupation. For legal persons it includes, for instance: Legal name, Address, Unique Identifier.
<p>KYC</p> 	KYC attributes are required for risk, anti-fraud or suitability evaluations for natural or legal persons. This includes politically exposed person (PEP) status, Source of funds, Tax and Fiscal residence for natural person; and Beneficial Owner Identity, Source of funds and Brand name for legal person.

The consolidated view of the attributes used by the surveyed institutions is available in Annex III.

Identity attributes

Financial institutions follow different procedures and definitions of identity based on local Member State legislations. The figure below shows the identity attributes considered for both a natural and a legal person, in line with the eIDAS classification and the mandatory and additional set of identity attributes aligned with the Regulation 2015/1501. The complete mapping of these attributes is provided in Annex I.

¹⁵ Compliance means refers to the common and divergent mechanisms and techniques (e.g. credentials and tokens) used for the on-boarding process at financial institutions in the selected Member States.

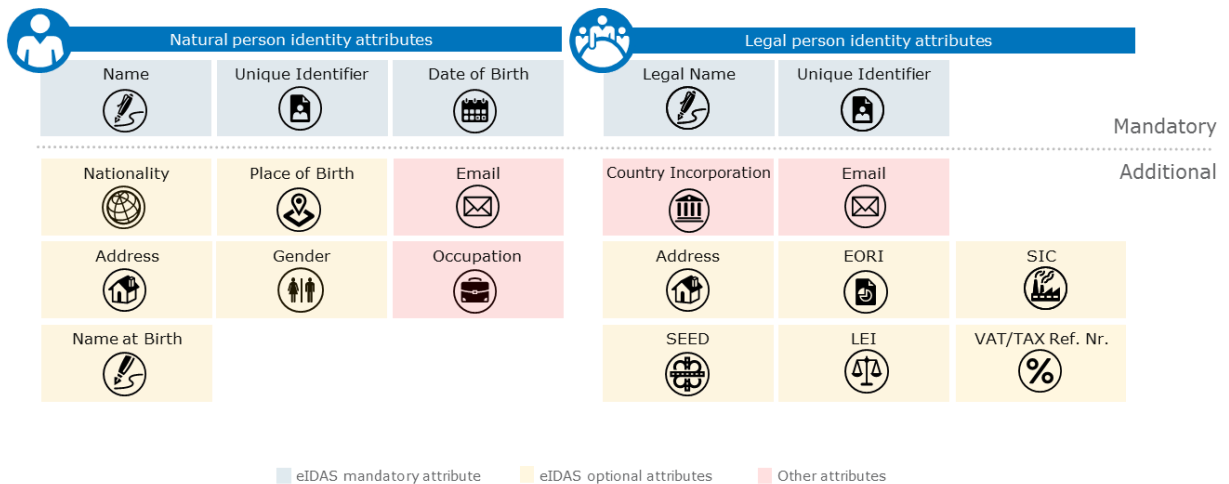


Figure 2. Natural and legal person identity attributes

Note that for a natural person the Name and Name at Birth attributes include both first and family name, whereas the address combines current address with country of residence. For a legal person the VAT/TAX Ref. Nr. attribute includes both VAT and TAX reference numbers.

There are also several abbreviations used for Optional attributes for legal persons according to eIDAS attribute profile¹⁶: Legal Entity Identifier (LEI) – an identifier which is used for identification of counterparties engaged in financial transactions (e.g. OTC trading); Economic Operator Registration and Identification (EORI) – a unique number assigned by a customs authority in a Member State to economic operators involved in customs activities; System for Exchange and Exercise Data (SEED) or an excise number which is an identification number assigned by Member States for excise purposes to records of the economic operators and premises; and Standard Industrial Classification (SIC) – a number used for an industry classification.

¹⁶ eIDAS SAML Attribute Profile, available at: https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf

The common and divergent identity attributes required for a natural and a legal person are summarised in Figure 3.

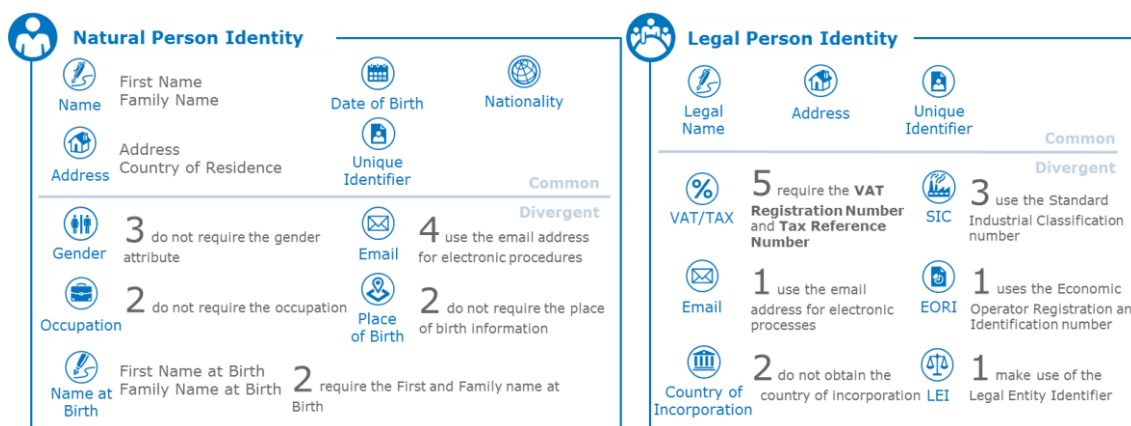


Figure 3. Overview of the common and divergent identity attributes used for a natural and a legal person at the surveyed financial institutions

Furthermore, the outcome of the analysis demonstrated that the identity of a **natural person** is commonly based on the following attributes: Name (First and Family Name), Address (Current Address and Country of Residence), Date of Birth, Nationality and Unique Identifier.

It is important to emphasise that the unique identifier used by the financial institutions for natural persons is represented by a number of government issued documents, such as a national identity card (NID) or a passport. In contrast, for cross-border electronic transaction purposes following the eIDAS attribute profile, the unique identifier for a natural person is provided by a combination of attributes, such as the national country code and government document issued number along with the country code of the trust service provider.

Different identity attributes are used for residents and non-residents. The Unique Identifier attribute is not always required for non-residents while it is required for residents. The Address attribute is also not required for non-residents by two of the surveyed financial institutions. The same applies for the Gender, where one of the financial institutions makes use of the gender for residents but not for non-residents, mainly due to ease of collection linked to other attributes (e.g. as a derivate from unique identifier).

For a **legal person** the surveyed institutions commonly require the Legal Name, Address, and the Unique Identifier attributes. It is important to note that one of the surveyed institutions does not perform on-boarding of legal persons, keeping focus on natural persons.

The Unique Identifier required for the on-boarding of a legal person is defined by the surveyed institutions according to the Directive 2012/17/EU¹⁷. In contrast, the eIDAS attribute profile separates the notions of the Unique Identifier and Directive 2012/17/EU attribute. Furthermore, only one surveyed financial institution collects Legal Entity Identifier (LEI). This can be explained by a specific purpose of the LEI number which is used for identification of counterparties that engage in financial transactions.

Comparable to natural persons, the used identity attributes differ for resident and non-resident legal persons. While one financial institution does not allow on-boarding of non-resident legal persons, one of those allowing does not require the address.

KYC Attributes

In addition to the identity attributes for a natural and a legal person, financial institutions require extra attributes to evaluate the risk and suitability associated with a prospective client. The KYC attributes group the risk, legal and regulatory attributes along with other attributes specific to the financial institution. The KYC attributes are depicted in the figure below and are not considered by the eIDAS classification (Annex I).

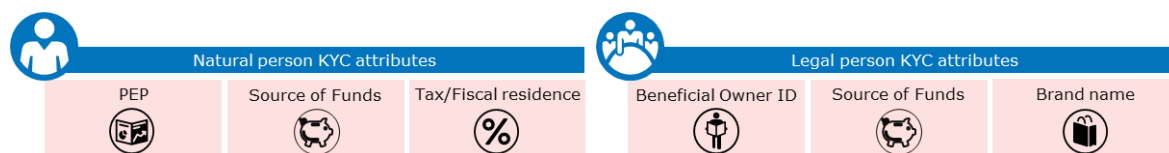


Figure 4. Natural and legal person KYC attributes

The PEP attribute for a natural person indicates the politically exposed person status describing the connection of a natural person with a government authority, and a possible higher risk for corruption due to the occupied position at the government authority. The Tax/Fiscal residence defines the mandatory Tax or Fiscal address of the natural person. The Source of Funds information shows how a natural person receives wealth, and from which activities a legal person obtains cash flows.

For a legal person the Beneficial Owner Identity attribute combines both a declaration of beneficial owners (including an ultimate beneficial owner, a person who exercises ultimate effective control over a legal person) of the legal entity and identification of these defined owners. The Brand name attribute is required to check additional available information regarding the legal person as well as compare the brand name and legal name.

¹⁷ Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies register, available at: https://joinup.ec.europa.eu/sites/default/files/eidas_saml_attribute_profile_v1.0_2.pdf

The outcome of the analysis on the surveyed financial institutions regarding the common and divergent KYC attributes used for a natural and a legal person is summarised in Figure 5.

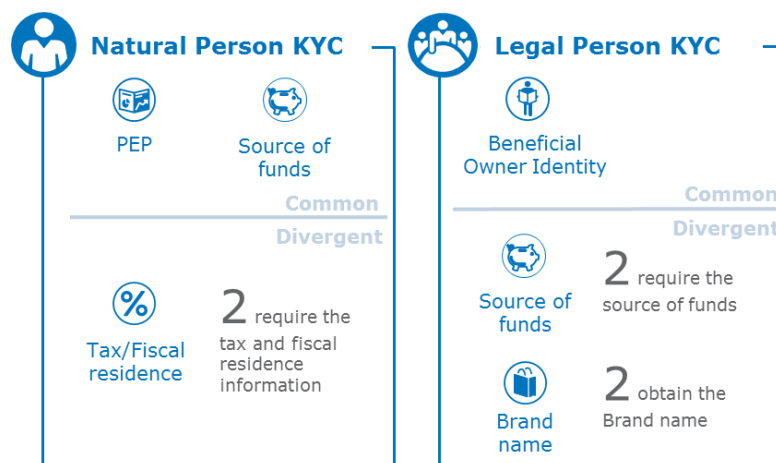


Figure 5. Overview of the common and divergent KYC attributes for a natural and legal person

The analysis of the collected data shows that the PEP status and Source of Funds attributes are commonly required for assessing the risk of a **natural person**. Eight surveyed financial institutions used the Source of Funds information only if an on-boarding of the natural person requires to follow an enhanced due diligence procedure, meaning that more detailed information should be collected, and more frequently updated during the business relationship. The Tax/Fiscal residence information is required only by two of the surveyed financial institutions. There are no different requirements for a resident and a non-resident natural person.

As aforementioned one of the surveyed institutions does not conduct **legal person** on-boarding while one does not allow on-boarding of a legal person based in a different country. The financial institutions, allowing a legal person on-boarding, commonly require the Beneficial Owner Identity information. In contrast, the Source of Funds and Brand Name are only required by two financial institutions in scope. A legal person based in another country should follow the same on-boarding requirements as a resident legal person, if not subject of an enhanced due diligence procedure due to the additional risk imposed by a specific foreign country.

On-boarding Process Requirements

This section analyses the common and divergent mechanisms used for the on-boarding process steps of verification, collection and management for the identity and KYC attributes. It is important to note that in some cases (e.g. face-to-face on-boarding) the on-boarding process of a legal person could be performed by a legal representative acting on behalf of a legal person. The legal representative definition is based on local Member State legislations, therefore the conditions may differ regarding the required attributes, roles and responsibilities.

Verification

The verification step implements the requirements and mechanisms used to perform verification of identity and KYC attributes during the on-boarding process.

The differences in the verification mechanisms used are derived from both diverse AML rules applied at Member State level and deployed technologies. Although traditional face-to-face verification using a government issued document is still the most common verification mechanism, other divergent and more innovative mechanisms are available due to different technologies and legislation across Member States. For example, in Germany the verification of a natural person identity could be done by a post office, or, in the United Kingdom the verification of identity could be checked by credit agencies. Another example is Belgium, which has mandatory national eID cards (NeID) which could support remote verification using eID software¹⁸. Estonia established a regulation¹⁹ defining the required digital provisions on how to use the mandatory NeID for the identification and verification of a person's identity. In Sweden financial institutions can issue eID for their customers (i.e. BankID) which can be used as an eID solution for on-boarding into other financial institutions or to perform other online activities, such as online shopping and eGovernment services.

The common and divergent verification mechanisms used for the identity and KYC attributes of natural and legal persons are summarised in Annex IV.

Collection

The collection process step indicates how the identity attributes are collected and documented for storage. The collection of the identity attributes can be performed via a face-to-face meeting or via a remote procedure like remote attestation with the presentation of a verification mechanism allowed as described in the previous section. The collection of the attributes is required for future verification and storage to comply with legislative regulations at the Member State and European levels.

The copy of a government issued document, such as NID, passport, resident Card (for non-citizens), and birth certificate (for minors), is the most common used collection mechanism for the identity attributes of a natural person. The collection of the copy depends on the type of the surveyed financial institution. For instance, financial institutions only available online (i.e. "neobanks") allow the collection of the copy of the government issued document remotely through a digital process, such as a digital copy. While other institutions with physical offices are favouring a face-to-face collection following local AML legislations requiring that if a customer is not physically present at on-boarding, enhanced due diligence measures should be applied.

The divergent cases are generally bound to Member State specific legislation and regulation or extra financial institution requirements allowing different mechanisms. For example, in Germany, Luxembourg, and Spain collection via a high quality video

¹⁸ Belgian [eID Software](#) allows the use of the eID for: natural person identification, electronic document signing and secure logging on to online services (e.g. [My Belgium](#) government system).

¹⁹ Regulation issued by Minister of Finance in force from 31.10.2016: Requirements and procedure for identification of persons and verification of persons' identity with information technology means, available at: <https://www.riigiteataja.ee/en/eli/504112016001/>

call is supported by the local AML regulation²⁰. Additionally, Belgium and Sweden provide eID solutions that extract the identity information through the use of the eID card for Belgium; or the financial institution issued eID for Sweden.

The collection of a legal person’s identity attributes requires a copy of a government issued document, such as a certificate of incorporation.

The common and divergent collection mechanisms used for a natural and legal person are summarised in Annex IV.




Management

The management process step describes how the identity and KYC attributes are stored and managed. This step describes the general provisions, technical controls and information management procedures followed by financial institutions to record and manage the collected attributes.

All surveyed financial institutions manage the collected attributes and documents in a similar manner for both natural and legal persons.

However, as an illustration of divergence, two of the surveyed financial institutions store the collected data in a central company-wide repository which is accessible by all the offices in different countries. Apart for general attributes availability, this allows the support for portability and re-use of the services and processes during the cross-border on-boarding process. Table 3 summarises the common and divergent management mechanisms used for both identity and KYC attributes of a natural and a legal person.

Table 3. Overview of the management mechanisms for both identity and KYC attributes of natural and legal persons

 Attributes		Management	
		Common	Divergent
 Identity	Collected attributes are electronically stored in an internal local repository (i.e. a local electronic system). Electronic copies of the documents are uploaded to the same repository and filed in the client electronic folder.		Attributes are electronically stored in an internal central repository (i.e. a central electronic system) available and accessible at a financial institution on a company-wide level.
	 KYC	It is also possible that paper copies of documents are taken and then stored in cabinets dedicated to the specific natural or legal person.	

²⁰ Germany: Geldwäschegesetz (Anti-money laundering act), available at:

<https://dejure.org/gesetze/GwG/4.html>

Luxembourg: CSSF Q&A: Identification/Verification of Identity through video chat, available at:

http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080416.pdf

Spain: Autorización de procedimientos de identificación no presencial mediante videoconferencia (Authorization of remote identification procedures by videoconference), available at:

http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf

Summary

Based on the findings, we can group and consolidate the common and divergent mechanisms used by the different surveyed financial institutions during the on-boarding process.

The consolidation of the common and divergent on-boarding mechanisms used is summarised in the figure below, and demonstrates that the copy of a government issued document represents the common mechanism used by the surveyed financial institutions during verification and collection. Also, the collection is generally performed via a face-to-face meeting at the physical office of the financial institution. Divergent situations occur when the financial institution is a “neobank” with no physical office, and thus verification and collection are performed remotely.













	Attributes	Common	Divergent				
Identity 		Government issued document 	Digital copies 	Local eID solutions 	HQ Video and photo 	Third-party token 	
KYC 		Face to Face*	Remotely				
		Collected copy is managed in an internal local electronic repository	Collected digital copy is managed in a central electronic repository accessed at company-wide level				
*For financial institutions with no physical office collection, via remote connection applies.							

Figure 6. Overview of common and divergent mechanisms used for on-boarding

CHAPTER 4 KYC PROCESSES AND LOAs OF eIDAS

The purpose of this section is to analyse how existing on-boarding processes are mapped onto digital processes based on the compliance means; as well as to map the fully digital and potential processes to the eIDAS LoAs.

The eIDAS Regulation provides a legal framework for cross-border mutual recognition of secure and trustworthy electronic identification and authentication, with credentials issued or recognised by national public authorities. As a consequence, natural and legal persons are able to prove their identity using their national electronic identification means when accessing public and potentially private services online throughout the EU. The existing on-boarding processes employed by financial institutions require natural and legal persons to follow process steps in which the verification of the claimed identity is required.

The on-boarding process steps of natural and legal persons can be distinguished as follows:

- **Non-digital:** The process is required to be performed physically and executed manually. For instance, the natural or legal person should perform the process locally and face-to-face at the financial branch.
- **Digital:** The on-boarding processes steps are performed fully electronically, not requiring any physical action.
- **Mixed:** The process step is achieved by a combination of physical and digital electronic activity.

This section starts to map the existing processes (mainly mixed processes) onto digital processes and the fully digital and potential digital processes to the eIDAS LoAs.

Non-digital and mixed processes

Most of the on-boarding process steps used by the surveyed financial institutions are mixed as they contain both digital and non-digital steps. This section demonstrates how these existing mixed processes can be mapped onto a fully digital process for local or remote on-boarding.

The fully digital processes can be supported by emerging technologies with the application of the eIDAS Regulation for electronic identification. The use of an electronic seal (eSeal) presents an emerging digital step as part of the on-boarding process for a legal person. The eSeal as defined by Article 3(25) of the eIDAS regulation can be used during the verification and collection step for the authentication of legal persons. The authentication process enables electronic identification of natural and legal persons by asserting their personal identification data in electronic format.

The eSeal is an advanced electronic signature that is issued by the creator of a seal (Article 3(24) of the eIDAS regulation) which is a legal person to ensure the origin and integrity of information. The eSeal is validated based on the electronic signature using

the eSeal certificate issued by a trust provider. The eSeal contains identification data identifying the legal person attached to the applied electronic signature.

In the case where a natural person represents the legal person, a power/mandate is required. The natural person is denoted as a legal representative. To verify the legal power/mandate of the presented legal person, the information should be signed with the legal representative's electronic signature and the legal person's eSeal.

The combination of the electronic signature and the electronic seal confirms the ability of the representative to act on behalf of the legal person. Collection of identity attributes from an eSeal can be facilitated very similarly to the ways described for documents type 3 and 4.

The tables below provide the mapping for both natural and legal persons.

Table 4. Mapping of mixed process steps in on-boarding of a natural person to digital process

Existing local on-boarding	Existing remote on-boarding	Digital process
Application		
An application is done by either filling out a paper application form, or an electronic form at the office.		<p style="text-align: center;">YES (conditionally)</p> <p>An electronic form needs to be completed, and the information can be transferred automatically from the electronic ID means onto the form.</p>
	An application is done online by filling out an electronic form via a website.	<p style="text-align: center;">YES (conditionally)</p> <p>Same as above.</p>
Verification: a. Authenticity check of documents		
The applicant provides government issued documents face-to-face. Document authentication is performed by an officer of the financial institution via visual observation and physical inspection of the provided documents.		<p style="text-align: center;">YES (conditionally)</p> <p>The eID means is integrated in the physical document and the hardware required to read and verify the electronic document aspects of the means is locally present.</p>
	The applicant sends a scanned/photo copy of the government issued documents via the financial institution's website/email. An officer of the financial institution conducts a visual observation and physical inspection of the provided copy.	<p style="text-align: center;">YES (conditionally)</p> <p>The eID means is integrated in the physical document, the hardware required to read the electronic document aspects of the means is present on the side of the applicant, and the verification can be done on the side of the financial institution.</p>
	The applicant uses video technology to show the government issued documents. The document observation is performed by an officer of the financial institution who conducts a video interview. Additionally, the officer observes the video screenshots.	<p style="text-align: center;">YES (conditionally)</p> <p>The document has an MRZ which can be interpreted by OCR. This information can be used to check e.g. against blacklists of stolen or misused documents (for a background of European passports refer to Annex VI).</p> <p>Where personal identification data is provided by an electronic ID means, such data can benefit from the presumption that its quality is guaranteed by its issuer.</p>

Existing local on-boarding	Existing remote on-boarding	Digital process
----------------------------	-----------------------------	-----------------

Verification: b. Identity check of the applicant

<p>An officer of the financial institution conducts a face-to-face verification of the identity attributes and comparison of a picture on the government issued document of the natural person.</p>		<p align="center">YES (conditionally)</p> <p>When the picture can be read and displayed from the electronic ID means in a reliable way, it can be used as a complement to the picture printed on the means.</p>
	<p>An officer of the financial institution performs a manual check of the identity attributes on the scanned/copy of the government issued document. No visual comparison of a person with the picture on the document is performed. In this case, a financial institution usually employs additional measures to mitigate risk of fraud, which can include, e.g. a request of an additional (identity) document.</p>	<p align="center">YES</p> <p>An electronic ID means can help by providing an extra electronic identification means as an additional measure.</p>
	<p>An officer of the financial institution performs identity attributes verification and visual comparison of the picture on the government issued document during a video interview.</p>	<p align="center">YES (conditionally)</p> <p>When the picture can be read and displayed from the electronic ID means in a reliable way, it can be used as a complement to the picture printed on the means.</p>
	<p>The financial institution receives a confirmation of the applicant identity in a form of a digital token provided by the third party provider (e.g. the third party creates a digital ID credential for the applicant). Third party providers include credit agencies, post offices, government authorities (e.g. tax authority, national population registration authority and embassies), notaries, etc.</p>	<p align="center">YES (conditionally)</p> <p>An electronic ID means can provide such confirmation in electronic format.</p>

Existing local on-boarding	Existing remote on-boarding	Digital process
	The identity attributes are checked by using the token material of the digital eID.	YES (conditionally) Where the eID means is capable of creating a token.

Verification: c. Anti-fraud check

An officer of the financial institution inputs the identity attributes in a proprietary or vendor database in order to perform an anti-fraud check of the presented document as well as an anti-fraud/PEP/sanction check of the applicant (i.e. screening).		YES (conditionally) Depending on the means and on the technology available to the officer, the attributes from the electronic ID means may be transferred automatically to the input of the transaction.
	The financial institution receives confirmation of the anti-fraud check in a form of a digital token provided by the third party provider (e.g. the third party creates a digital ID of the applicant).	YES An electronic ID means can provide such confirmation in electronic format.

Collection

Collection of a hard copy of the government issued document.		YES (conditionally) When an electronic form needs to be completed, and the information can be transferred automatically from an electronic ID means into the form, with guarantees of integrity.
	Collection of a scanned/photo copy or video screenshots (and video itself) of the government issued documents.	YES (conditionally) When the document has an MRZ which can be interpreted by OCR, the information from the government issued documents can be collected automatically. In case personal identification data is provided by an electronic ID means, such data can benefit from the presumption that its quality is guaranteed by its issuer.
	Collection of the attributes is done by the	YES

Existing local on-boarding	Existing remote on-boarding	Digital process
	third party provider.	An electronic ID means can support the collection of the identity attributes via the personal identity information available in the electronic identification means.
	Collection of identity attributes from the eID can be facilitated through various digital means, e.g. a card reader device.	YES An electronic ID means can support the collection of the identity attributes via the personal identity information available in the electronic identification means.

Management

Hard copies of the documents are stored in cabinets dedicated to a specific natural person.		N/A
	Scanned/photo copies or video screenshots are electronically stored in a repository (i.e. an electronic system).	N/A

Table 5. Mapping of mixed process steps in on-boarding of a legal person to digital process

Existing local on-boarding	Existing remote on-boarding	Digital process
Application		
An application is done by either filling out a paper application form or completing an electronic form at the office.		YES (conditionally) When an electronic form needs to be completed by one or more representatives, and the information can be transferred automatically from an electronic ID means into the form, with guarantees of integrity.
	An application is done online by filling out an electronic form via the financial institution's	YES (conditionally) Same as above.

Existing local on-boarding	Existing remote on-boarding	Digital process
	website.	

Verification: a. Authenticity check of document

<p>The applicant provides government issued documents face-to-face at an office of the financial institution. In this option a legal representative acts on behalf of the legal person. Where the legal representative is involved, documents confirming his or her rights to act on behalf of the legal person as well as identity documents of the legal representative are also provided. Authentication is performed by an officer via visual observation and physical inspection of the provided documents. Additionally, the applicant provides government issued documents for identification and verification of its beneficial owners.</p>		<p>YES (conditionally) When a legal representative uses an eID means, and this eID means is integrated in a physical document and the hardware required to read and verify the electronic document aspects of the means is locally present.</p>
	<p>The applicant sends a scanned/photocopy of the government issued documents via the financial institution's website/email. An officer of the financial institution conducts a visual observation and physical inspection of the provided copy. Additionally, the applicant provides a scanned/photocopy of government issued documents for identification and verification of its beneficial owners.</p>	<p>YES (conditionally) When a legal representative uses an eID means, and this eID means is integrated in the physical document, the hardware required to read the electronic document aspects of the means is present on the side of the applicant, and the verification can be done on the side of the financial institution.</p>

Verification: b. Identity check of the applicant

Existing local on-boarding	Existing remote on-boarding	Digital process
<p>An officer of the financial institution conducts verification of the identity of the legal person and its beneficial owners (as well as a legal representative, where applicable) by a manual check of the identity attributes in the provided government issued documents.</p> <p><i>*When the legal representative of the applicant is a natural person, the identity check is conducted in line with the procedure applied for a natural person.</i></p>		<p>YES (conditionally)</p> <p>When the picture can be read and displayed from the electronic ID means in a reliable way, it can be used as a complement to the picture printed on the means.</p>
	<p>An officer of the financial institution performs a manual check of the identity attributes of the legal person as well as its beneficial owners in the scanned/photocopy of the government issued document. In this case, as the applicant is not physically present, a financial institution usually employs additional measures to mitigate risk of fraud, which can include, e.g. a request of an additional (identity) document.</p>	<p>YES</p> <p>An electronic ID means can help by providing the electronic identification means for the authentication of the application and its beneficial owners.</p>
	<p>The financial institution receives confirmation of the applicant identity and identity of its beneficial owners in a form of a digital token provided by the third party provider (e.g. the third party creates a digital ID of the applicant). Third party providers include credit agencies, government authorities (e.g. tax authority, national companies' registration authority), etc.</p>	<p>YES</p> <p>An electronic ID means can provide or help to provide such confirmation in electronic format.</p>

Existing local on-boarding	Existing remote on-boarding	Digital process
----------------------------	-----------------------------	-----------------

Verification c. Anti-fraud check

<p>An officer of the financial institution inputs the identity attributes manually in the proprietary or vendor database and performs the anti-fraud check of the provided government issued documents and anti-fraud/PEP/sanction check (i.e. screening) of the applicant, its beneficial owners and a legal representative.</p>		<p>YES (conditionally) When this information needs to be entered in a computer application, and the information can be transferred automatically from an electronic ID means into the application, potentially with guarantees about integrity.</p>
	<p>The third party inputs manually the attributes in the proprietary or vendor database and performs the check. Based on the results of the check, the third party adds the information to the applicant’s digital token (e.g. a digital ID). The financial institution receives confirmation of the anti-fraud check in a form of a digital token provided by the third party provider (e.g. the third party creates a digital ID of the applicant).</p>	<p>YES An electronic ID means can provide or help to provide such confirmation in electronic format.</p>

Collection

<p>Collection of a hard copy of the government issued documents.</p>		<p>YES (conditionally) When a legal representative uses an eID means to prove his identity, and this eID means is integrated in a physical document, the hardware required to read the electronic document aspects of the means is present on the side of the applicant, and the verification can be done on the side of the financial institution. Corroborating evidence that this person is indeed appointed to represent a legal entity can potentially be supported by electronic documents created and signed/sealed by the appropriate business register.</p>
	<p>Collection of a scanned/photocopy of the</p>	<p>YES (conditionally)</p>

Existing local on-boarding	Existing remote on-boarding	Digital process
	government issued documents.	Same as above, limited to identity aspects of legal representative(s). Optionally, signed assertions can be used to provide additional assurance regarding the provided documents.
	Collection of the attributes is done electronically by the third party provider.	<p style="text-align: center;">YES</p> An electronic ID means can support the collection of the identity attributes via the personal identity information available in the electronic identification means. For other attributes, signed assertions may provide additional assurance.

Management

Hard copies of the documents are stored in cabinets dedicated to a specific legal person.		N/A
	Scanned/photocopies are electronically stored in a repository (i.e. an electronic system).	N/A

Digital and potential digital

The mapping between digital and potential digital processes with eIDAS considers the following two perspectives:

- A given electronic scheme which is in place is eIDAS compliant and can be used to base KYC/AML processes on; and
- A given KYC scheme may allow to place an eIDAS compliant scheme on top of it. This means that after the on-boarding, the financial institution may decide to issue their own electronic identification means to the customer (e.g. bank cards). This means may or may not be eIDAS compliant.

The mapping presented here addresses the first perspective, which is the one relevant for the current study.

There are parallels that can be drawn between the specified KYC/AML requirements for customer on-boarding, including the identified on-boarding process flow, and the eIDAS LoAs. It is important to note that financial institutions should define the LoAs according to a risk-based approach. The electronic identification means should provide at least a substantial LoA for electronic identification. The LoAs provided by the electronic identification means depend on the issuer, process and technical controls implemented. For instance, electronic identification means such as government issued eID (type 3) provide a high level of assurance. For digital-only documents (type 4) the identity proofing relies on qualified certificates for a level of assurance high.

Table 6 and Table 7 below provide an overview of which of the potential fully digital on-boarding process steps could be facilitated through the use of eIDAS for the different document types aforementioned. The overview of proposed amendments to articles of 4AMLD in the relation to eIDAS is described in Annex II. Type 1 documents have no electronic support as they are physical only and cannot be considered. Type 2 and 3 documents may be used to generate the electronic identification means following the eIDAS Regulation guidelines. Type 4 documents are digital only and require a qualified status or accepted and approved by the financial institution.

Table 6. Description of potential fully digital process steps in on-boarding of a natural person²¹

Local/remote on-boarding ²²	eIDAS Support
Application	
The document is read electronically (e.g. through OCR technology or eID reading, contact-based or contactless) at	YES Electronic identification means contain personal identification data in electronic

²¹ The requirements of the levels of assurance for a natural person expected by the on-boarding process steps are described in Table 12 of Annex I.

²² The local and remote on-boarding have similar process steps, as both require the use of a web or mobile application provided to the applicant by financial institution, government or a third-party provider. The application can be then accessed by an officer of the financial institution or directly by the applicant remotely.

Local/remote on-boarding ²²	eIDAS Support
the financial institution or remotely (via the financial institution or third-party application), and the digital application form is filled out automatically.	form which uniquely represents a natural person.

Verification: a. Authenticity check of documents

<p>Type 2. The applicant uses the built-in digital camera of a device (e.g. mobile phone) to read the MRZ using OCR.</p>	<p>NO</p> <p>As type 2 documents cannot provide electronic evidence, they cannot contribute to the on-boarding process by invoking eIDAS effects.</p>
<p>Type 3. The authenticity of the eID means is verified via a cryptographic protocol. This may, for instance, be based on the validation of the electronic signature over the data stored in the chip. This signature is generated by the Document Issuer, i.e. a government entity of a Member State, or on its behalf.</p>	<p>YES</p> <p>The electronic signature over the identity information provides evidence and guarantees authenticity of its origin, i.e. that the document was issued by a Member State authority.</p>
<p>Type 4. This type of document (e.g. based on an app or a mobile application) does not correspond to a physical document. They are currently not accepted in KYC on-boarding processes.</p> <p>They can potentially be used in the future as the electronic identification means once KYC regulation allows this type of document. The authenticity of the electronic identification means (containing the identity attributes and token material) is confirmed by using the authentication protocol between the user and the financial institution.</p>	<p>YES (conditionally)</p> <p>While a type 4 document may not be eIDAS compliant, it may benefit from being bootstrapped from an eIDAS eID means at the moment it was created²³.</p>

Verification: b. Identity check of the applicant

<p>Type 2. The applicant uses the application provided by the financial institution (or the third party provider, where applicable) using HQ video technology that captures the personal identification data using OCR and a copy of the facial features. Then the OCR-extracted information is compared against the identity attributes, while the facial features are verified via pattern verification techniques to compare the 'owner of the document' versus the 'bearer of the document'.</p>	<p>NO</p> <p>There is no digital evidence provided by type 2 documents.</p>
<p>Type 3. The identity of the application can be verified as follows:</p> <ul style="list-style-type: none"> If the passport or eID contains biometric information, this can potentially be compared to the features of the person in front of the camera. This can be done by a person or it can be automated. 	<p>YES</p> <p>The eIDAS Regulation can support the verification of the identity attributes via the personal identity information available in the electronic identification means. The electronic signature applied by the document issuer confirms the authenticity of the applicant's attributes.</p>

²³ For an example refer to the Belgian www.itsme.be service, which does exactly this.

Local/remote on-boarding ²²	eIDAS Support
<ul style="list-style-type: none"> In case of an eID card supporting electronic authentication, the applicant can be asked to authenticate (e.g. by entering the pin code, or using an authenticator such as from FIDO alliance²⁴). The identity attributes can be signed by the authority that issued the document. This signature can be verified. <p>In both cases an authentication process confirms the claimed identity. The identity attributes and biometric data contained in the electronic chip can be compared to both the applicant and the document being presented. The authentication is done via an electronic signature applied to the personal identification data guarantees extracted from the eID chip via an eID reader (either locally at the financial institution or remotely). The electronic signature guarantees the integrity and authenticity of the data of the applicant and its origin. The personal identification data is unlocked via a pin code through the use of an eID reader. The electronic signature is issued by a Member State authority to the applicant.</p>	
<p>Type 4. Once the digital eID, containing the person's identification data, is found genuine, the applicant will be requested to authenticate him- or herself. The current technology market provides a range of authentication means or factors such as these created by members of the FIDO alliance. These can be part of the mobile device (e.g. camera, fingerprint reader) or can be provided "out of band" such as a one-time password provided via SMS. The applicant authenticates himself/herself by e.g. using the camera or fingerprint reader of the mobile device bound to the digital eID. This process can be performed locally or remotely via a web or mobile application.</p>	<p>YES (conditionally)</p> <p>While such a type 4 document may not be eIDAS compliant, it may benefit from being bootstrapped from an eIDAS eID means at the moment it was created</p>

Verification: c. Anti-fraud check

<p>Type 2. The MRZ contains the applicant identity attributes (e.g. first and last name, date of birth; etc.) and the information on the presented document (e.g. issuer, document number, etc.). This information can be automatically collected via OCR, entered in the system and be used to perform anti-fraud checks against fraud document listings, e.g. stolen passport database, criminal database, PEP/sanction screenings.</p>	<p>NO</p> <p>There is no digital evidence provided by type 2 documents.</p>
<p>Type 3. The information in the electronic passport or eID card provides details on the identity which can be automatically uploaded to the system and be used to perform anti-fraud checks.</p>	<p>YES</p> <p>The eIDAS Regulation can support the fraud-check using the identity attributes via the personal identity information available in the electronic identification means. The electronic signature applied by the document issuer confirms the</p>

²⁴ Available at: <https://fidoalliance.org>

Local/remote on-boarding ²²	eIDAS Support
	authenticity of the applicant's attributes.
<p>Type 4. The attributes on digital eID are automatically uploaded in the system and can be checked against fraud document listings, such as a database of stolen passports.</p>	<p>YES (conditionally) While such a type 4 document may not be eIDAS compliant, it may benefit from being bootstrapped from an eIDAS eID means at the moment it was created.</p>

Collection

<p>Type 2. Once the MRZ zone is read, the information can be stored as a digital picture or in an electronic document format of choice depending on the solution used.</p>	<p>NO There is no digital evidence provided by type 2 documents.</p>
<p>Type 3. Collection of identity attributes from the electronic passport and eID can be facilitated through various digital means depending on the backend technologies used by the financial institution. Generally, identity attributes are obtained directly from the electronic passport or the eID chip.</p>	<p>YES The eIDAS Regulation can support the collection of the identity attributes via the personal identity information available in the electronic identification means. The electronic signature applied by the document issuer confirms the authenticity of the applicant's attributes.</p>
<p>Type 4. Collection of identity attributes required by the financial institution from the digital eID can be facilitated through various digital means depending on the technology ecosystem that comes with the digital eID. In the case of an eID or a passport, the read-out attributes can be stored in a file or database. In the case of an eID app, the application (or its backend services) may provide an Application Programming Interface (API) for interaction.</p>	<p>YES While such a type 4 document may not be eIDAS compliant, it may benefit from being bootstrapped from an eIDAS eID means at the moment it was created.</p>

Management

<p>The digital copies of the presented documents are stored depending on their type:</p> <p>Type 2. The digital copy provided (e.g. email, web platform, and mobile application).</p> <p>Type 3. The identity attributes that are obtained directly from the electronic passport or the eID chip are digitally stored at the financial institution.</p> <p>Type 4. The identity attributes are provided via the digital eID and are automatically stored by the financial institution.</p>	<p>N/A</p>
---	-------------------

Table 7. Description of potential fully digital process steps in on-boarding of a legal person²⁵

Local/remote on-boarding ²⁶	eIDAS Support
Application	
<p>The legal person or the legal representative of the legal person's documents are read electronically (e.g. through OCR technology or eID reading, contact-based or contactless) and the digital application form is filled out automatically.</p>	<p style="text-align: center;">YES</p> <p>Electronic identification means contain personal identification data in electronic form which uniquely represents a natural person.</p>
Verification: a. Authenticity check of documents	
<p>Verification of the authenticity of the documents of a legal representative (if natural person) and beneficial owner(s) is done according to the listed procedures for on-boarding of a natural person.</p>	<p style="text-align: center;">YES</p> <p>The eIDAS Regulation supports with the use of evidence represented by an electronic signature/seal available in the chip, allowing to verify the origin of the document, i.e. Member State authority.</p>
Verification: b. Identity check of the applicant	
<p>The verification of the identity of the legal person is performed against the trusted third party who issued the electronic identification means (or Identity Provider – e.g. the government, a financial institution, a credit agency and national population register). Verification of the identity of a legal representative and beneficial owner(s) if natural persons is done according to the listed procedures for on-boarding of a natural person.</p>	<p style="text-align: center;">YES</p> <p>In case of a natural person representing a legal person, or of a legal person directly, eIDAS identification can confirm the authenticity of the applicant. A document signed by the natural person, or sealed by a legal person with appropriate authority, can provide corroborating evidence.</p>
Verification: c. Anti-fraud check	
<p>The anti-fraud check is performed by extracting the personal identification data from the electronic identification means and checked through a blacklist anti-fraud database, such as company registers, PEP/sanctions databases.</p>	<p style="text-align: center;">YES</p> <p>When the personal identification data is provided by an eIDAS means, such data can benefit from the presumption that its quality is guaranteed by its issuer.</p>
Collection	
<p>The collection of identity attributes from the electronic identification means can be facilitated through various digital means depending on the backend technologies used by the financial institution. Generally, the identity attributes are obtained directly from the electronic identification means during the verification process. This can be from the eID chip or the mobile identity application.</p>	<p style="text-align: center;">YES</p> <p>The eIDAS Regulation can support the collection of the identity attributes via the available personal identity information available in the electronic identification means.</p>

²⁵ The requirements of the levels of assurance for a natural person expected by the on-boarding process steps are described in Table 13 of Annex I.

²⁶ The local and remote on-boarding have similar process steps, as both require the use of a web or mobile application provided to the applicant by financial institution, government or a third-party provider. The application can be then accessed by an officer of the financial institution or directly by the applicant remotely.

Local/remote on-boarding²⁶

eIDAS Support

Management

The collected identity attributes are stored at the financial institution.

N/A

CHAPTER 5 FLOWCHART AND TEXT COMMENTARY

This chapter presents flowcharts accompanied by text commentary on how eIDAS notified eIDs (as per eIDAS Regulation) could facilitate the financial institutions' customer on-boarding process in a way that helps them to comply with (European and Member State) KYC and AML requirements. It is assumed such processes will increasingly become more digital. Additionally, we looked beyond the requirements currently allowed by AML regulation and proposed a fully digital cross-border on-boarding process flow improved by the eIDAS uptake.

As a basis for the creation of the flowcharts we made use of the workflow described at the eIDAS Observatory. For convenience of the reader this workflow is copied in Figure 7 below:

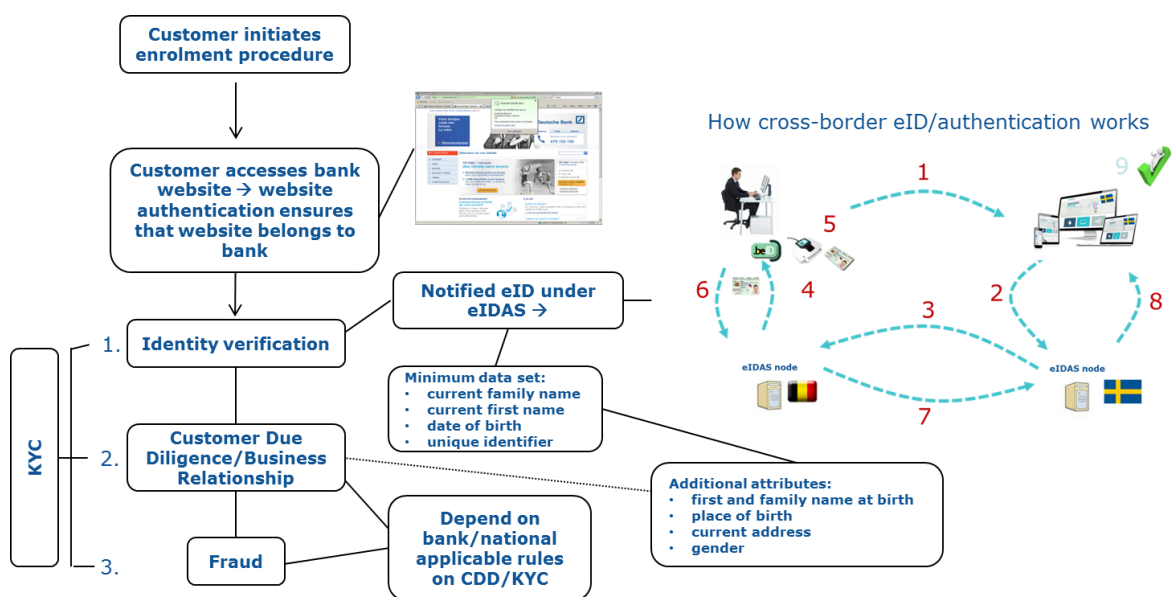


Figure 7. Sample workflow²⁷ for establishing a relationship with a customer online

²⁷ eIDAS Observatory, available at: <https://ec.europa.eu/futurium/en/content/graphic-customer-digital-onboarding>

Figure 8 describes the relationship between the workflow proposed by the eIDAS Observatory, the potential contribution of eIDAS and the structure of the flowcharts presented in this chapter:

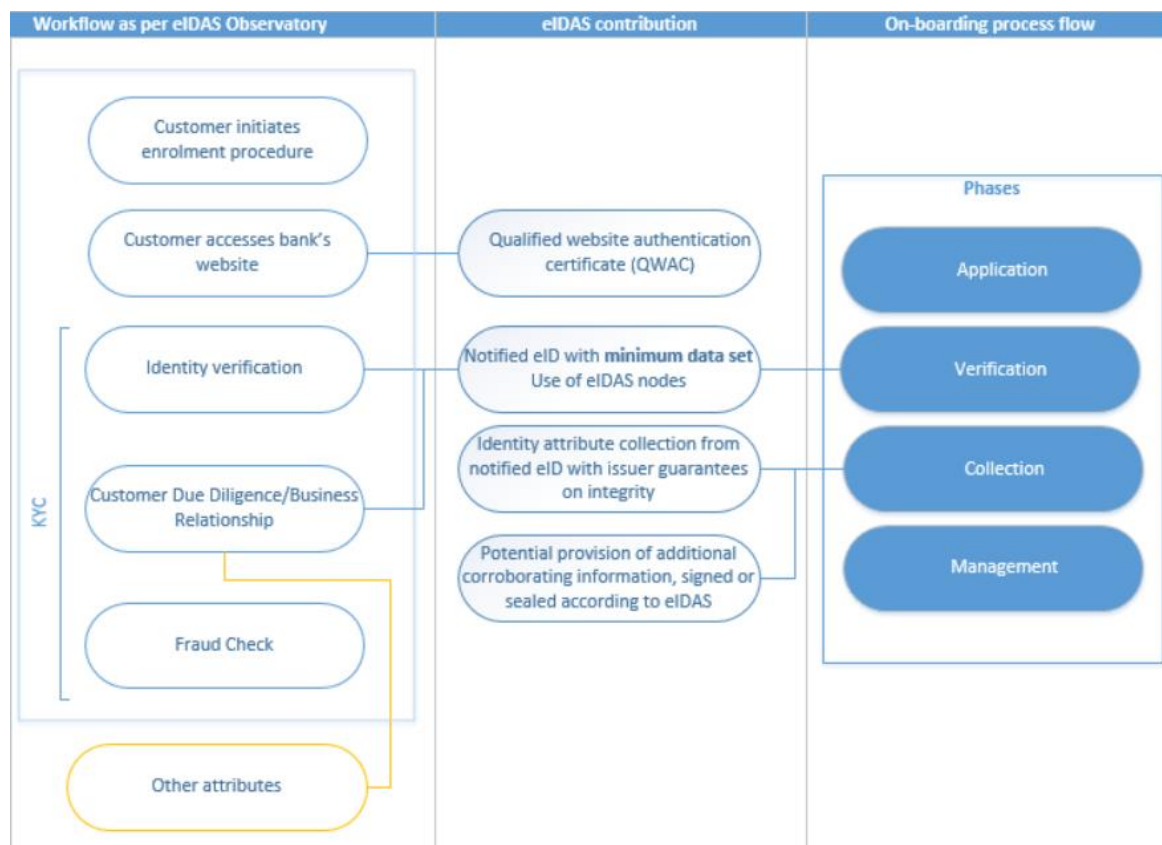


Figure 8. eIDAS contribution to customer on-boarding process

Figure 8 uses the terms of Regulation 2015/1501 which provide requirements concerning the minimum set of a natural and a legal person identification data. As per this Regulation the **minimum data set** consists of:

- mandatory attributes, which are obligatory and must be included in the minimum data set, and
- additional (optional) attributes, from which one or more attributes could be included in the minimum data set, depending if the attribute is available and acceptable to national law.

It is important to note that on-boarding of a new customer is a commercial decision taken by a financial institution. It means that even if an applicant has successfully undergone all the on-boarding phases, the financial institution can still reject the application for a business reason. In this chapter, we focused solely on the completion of the on-boarding process phases and did not conclude whether an applicant, who




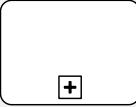


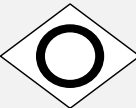
finished all the phases successfully, becomes a customer or does not. Furthermore, as already introduced in Chapter 4 KYC processes and LoAs of eIDAS, we did not take into account ID means issued by a financial institution to its customers, such as bank cards, userIDs and login passwords, or other types of bank IDs²⁸.

Structure and notation

For the graphical representation of the on-boarding process the Business Process Model and Notation (BPMN) de-facto standard²⁹ is used.

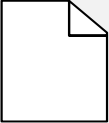


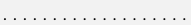

We make use of the following BPMN symbols in the flowcharts (refer to the table below):

Table 8. Flowchart symbols

Symbol	Meaning
	Start event: Start of the process
	End event: End of the process
	Task: An activity which describes a single unit of work which cannot be broken down to a further level of business process detail.
	Sub-process: An activity which shows that there are additional levels of business process details in this unit of work. A "+" sign indicates that the sub-process is collapsed. It has its own self-contained start and end events and one or more activities.
	Exclusive gateway: Exclusive decision is used to create alternative flows in a process. Only one of the paths can be taken.
	Parallel gateway: Parallel decision is used to create parallel paths without evaluating any conditions.
	Inclusive gateway: Inclusive decision is used to create alternative paths in a process when at least one of them are evaluated.

²⁸ Financial institutions may discretionary decide to allocate credentials and/or tokens they consider fit to interact with their customers. Such credentials/tokens may or may not be eIDAS compliant/notified.

²⁹ Available at: <http://www.bpmn.org/>

	<p>Data object: Is an artefact which shows which data is required or produced in an activity.</p>
	<p>Data store: Is an artefact used to store, update or retrieve information which persists after the process is completed.</p>
	<p>Sequence flow: Is a connection which shows in which order the activities are performed.</p>
	<p>Association: Is a connection which is used to link an artefact or a text to an activity.</p>
	<p>Applicant: This symbol indicates additional involvement of the Applicant in the activity.</p>

Additionally we recognise the following elements for the text commentary:

- **Process** – describes a high level flow of the on-boarding process. It may be further structured into one or more sub-processes.
- **Phase** - presents a delimited phase of the on-boarding process, specifically: application, verification, collection and management.
- **Activity** – shows actions which are performed in a process by an actor(s). The activities, depending on their complexity, are classified as:
 - Sub-process (SP)
 - Task

The following actors are participating in the on-boarding process:

- **Applicant** – a natural or a legal person applying to become a customer of a financial institution.
- **Verifier** – a party which performs, on a contractual basis, (part of) the on-boarding process. This actor could be the financial institution itself, another financial institution, an agent, an outsourcing service provider, etc.
- **Financial Institution** – an organisation which provides retail banking services in the European Union.

In this document we make the following simplifications in support of readability for a broad (non-technical) audience,

- Unless it clarifies the text commentary, we do not document the gateway logic in the process flowcharts; and

- The process flowcharts do not reflect detailed technical aspects, hence we simplified some aspects such as authentication and/or video sessions. Any additional material, where relevant, to support these technicalities is provided in footnotes throughout this document.

On-boarding of a natural person

The following flowchart provides the main overview of the (potentially) digital on-boarding process for a natural person:

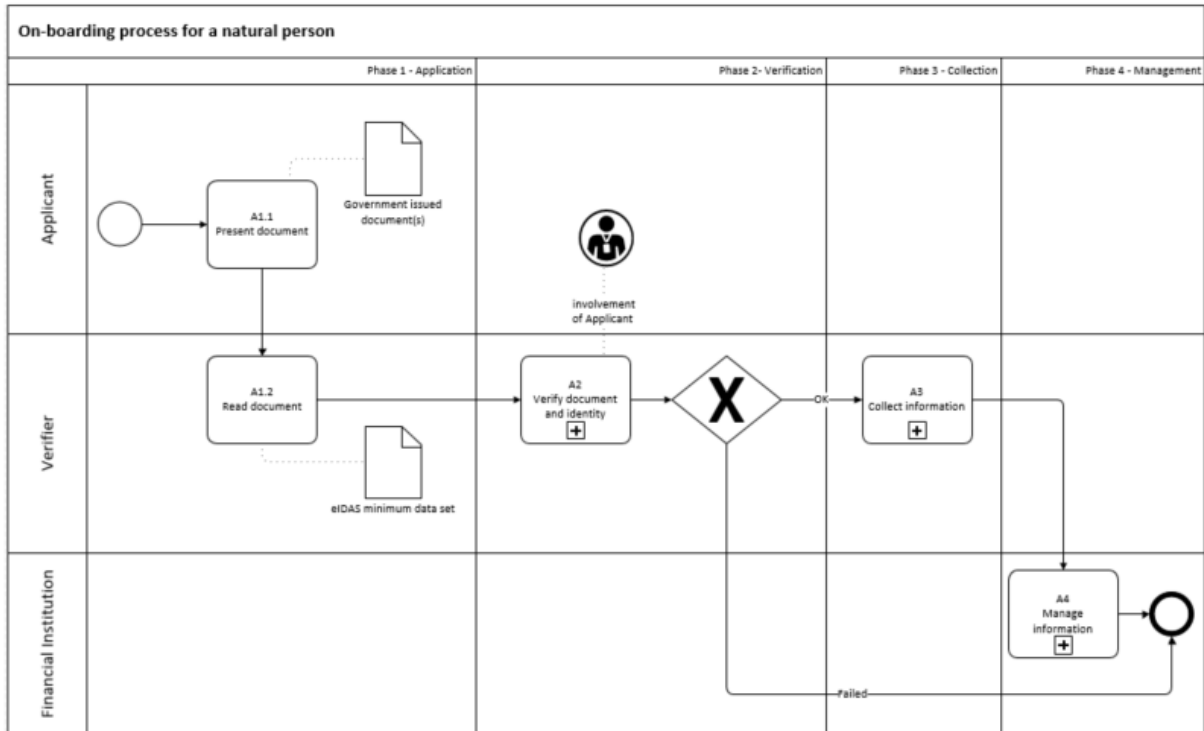


Figure 9. On-boarding process for a natural person

Process	On-boarding of a natural person
Description	The process flow in Figure 9 provides a high level description of the on-boarding of a natural person in 4 phases. It shows process steps through which a financial institution fulfils KYC and AML requirements when on-boarding a potential customer.
Input	<p>Government issued document such as:</p> <ul style="list-style-type: none"> National Identity Card (NID) Travel document Resident Card (for non-citizens) Birth certificate (for minors) <p>The electronic means (documents) are classified as per the informal classification provided in Document classification types.</p> <p>*Note that Type 1 documents do not fall within the scope of eIDAS, and, therefore, they are not discussed in the flowcharts which</p>

Process		On-boarding of a natural person	
	describe the potential digital on-boarding processes. Additionally, from an eIDAS and KYC/AML perspective, Types 3 and 4 documents are treated on equal footing and represented as a Type 3 document.		
Actors	<ul style="list-style-type: none"> • Applicant • Verifier • Financial Institution 		
Phase	Activity	Responsibilities	Actor
Phase 1 Application	A1.1 Present document	An applicant provides a verifier with the required government issued document using a technology in line with the document type. This can be done locally or remotely. The on-boarding process is initiated.	Applicant
	A1.2 Read document	The verifier digitally reads the government issued document, using technology in line with the presented document type. At this step the verifier obtains the eIDAS minimum data set as defined in the Regulation 2015/1501.	Verifier
Phase 2 Verification	A2 ³⁰ Verify the document and identity	The verifier conducts verification of the provided government issued document, identifies and authenticates the applicant (by checking the claimed identity against the identity described in the document), as well as performs a fraud check of both the document and the applicant. Note that some activities of this sub-process require involvement of the applicant. More details are provided in the following sections.	Applicant/ Verifier
Phase 3 Collection	A3 Collect information	The verifier collects identity attributes.	Verifier
Phase 4 Management	A4 Manage information	The financial institution stores the collected attributes in an electronic repository.	Financial Institution
Results	The applicant either: <ul style="list-style-type: none"> • successfully completes the on-boarding process, in this case 		

³⁰ Here and further in the document: as stated in the structure and notation to this document, a '+' sign indicates that the activity is a sub-process. It is collapsed, has its own self-contained start and end events and one or more activities, and which is described in the following section.

Process	On-boarding of a natural person
	<p>the required evidence is stored by the Financial Institution; or</p> <ul style="list-style-type: none"> • is rejected from on-boarding, in this case the reason for rejection is recorded.

Phase 1 - Application

Activities (A1.1 and A1.2) of the Application phase are described in the table above.

Phase 2 – Verification

A2 - VERIFY THE DOCUMENT'S AUTHENTICITY AND THE APPLICANT'S IDENTITY

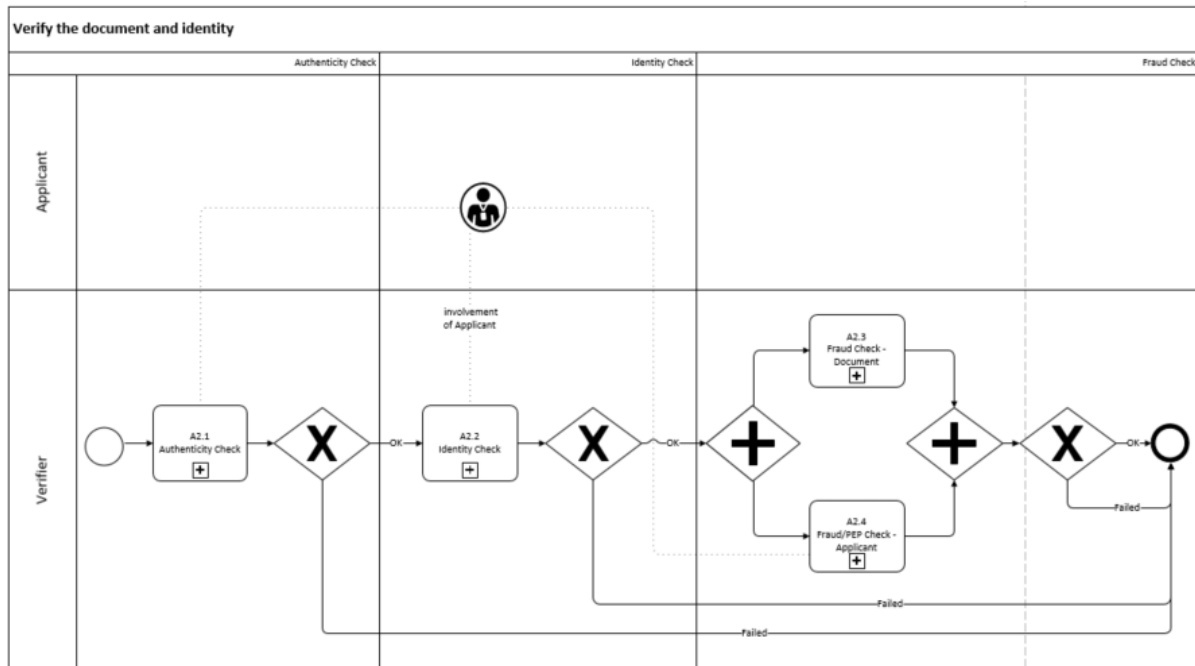


Figure 10. Verification of document's authenticity and the applicant's identity

Process	Verify the document's authenticity and the applicant's identity		
Description	A verifier conducts verification of the provided document, identifies the applicant, as well as performs a fraud check of both the document and the applicant.		
Input	Government issued document – Document type 2/3		
Actors	<ul style="list-style-type: none"> • Applicant • Verifier 		
Phase	Activity	Responsibilities	Actor
Phase 2 Verification	A2.1 Authenticity Check	Verification that the presented document is genuine.	Applicant/ Verifier
	A2.2 Identity Check	Check that the applicant is the holder of the presented document. Depending on the document type, verification of the identity of the applicant can be performed as a check of identity attributes and comparison of a picture on the government issued document or, via a validation of the token material of the digital eID.	Applicant/ Verifier

Process			
Verify the document's authenticity and the applicant's identity			
	A2.3 Fraud Check - Document	Check of the presented document against fraud database(s) (e.g. stolen passports database; population register (to confirm it belongs to a living person)).	Verifier
	A2.4 Fraud/PEP Check - Applicant	Check of the identity attributes of the applicant against fraud and PEP database(s).	(Applicant) /Verifier
Results			
	<ul style="list-style-type: none"> • If the applicant successfully completes all steps of the verification process, the applicant's data is collected and after that managed (i.e. stored in an electronic repository); or • If the applicant fails to comply with any of the verification activities, he/she is rejected and the reason for rejection is stored. 		

A2.1 - AUTHENTICITY CHECK OF THE DOCUMENT

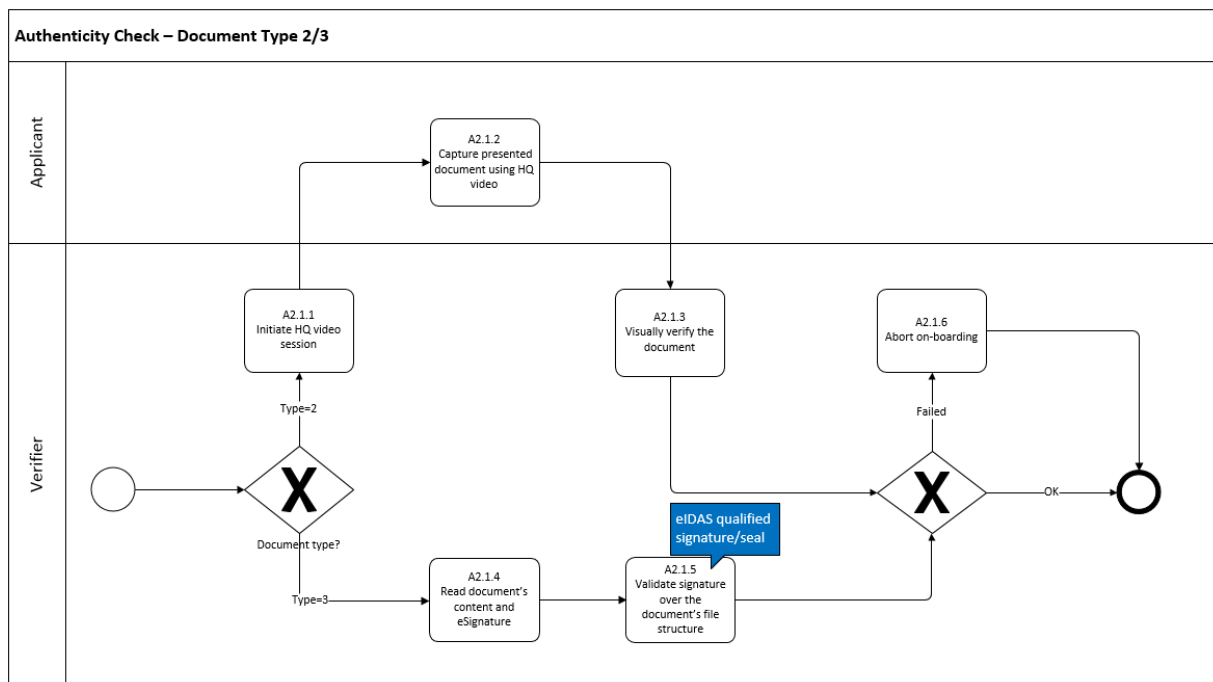


Figure 11. Authenticity Check – Document Type 2/3

Process	
Authenticity check of the document	
Description	Verification that the presented document is genuine. Depending on the document type this activity can include a visual observation and inspection of the presented document during a high quality (HQ) video session or a check by using the token material of the digital eID.

Process		Authenticity check of the document	
Input	Government issued document(s) – document type 2/3		
Actors	<ul style="list-style-type: none"> • Applicant • Verifier 		
	Activity	Responsibilities	Actor
	Document type?	The verifier checks the document type.	Verifier
	A2.1.1 Initiate HQ video session	If the applicant has a document type 2 : The verifier initiates a HQ video session with the applicant.	Verifier
	A2.1.2 Capture presented document using HQ video	Document type 2 : The applicant uses the built-in digital camera of a device (e.g. mobile phone) to read the MRZ using OCR. The applicant should show and capture the presented document.	Applicant
	A2.1.3 Visually validate the document	Document type 2 : The verifier validates that the document is genuine by utilising a trusted source for comparison, e.g. PRADO ³¹ .	Verifier
	A2.1.4 Read document's content and electronic signature	If the applicant has a document type 3 : The verifier reads the document's content and electronic signature (eSignature).	Verifier
	A2.1.5 Validate electronic signature over the document's file structure	Document type 3 : The verifier validates the signature over the document's file structure stored in the chip. This signature is generated by the Document Issuer, i.e. a government entity of a Member State, or on its behalf. eIDAS can support such signature validation using various types of eIDAS signatures and seals, including qualified signature and qualified seals. Since the Document Issuer is a legal person, the signature is technically speaking an electronic seal. Moreover, if supported by the document's chip, further cryptographic challenge/response protocols can be used to verify the authenticity of the chip, the binding of the chip to the particular document, etc.	Verifier

³¹ PRADO - Public Register of Authentic travel and identity Documents Online, available at: <http://www.consilium.europa.eu/prado/en/prado-start-page.html>

Authenticity check of the document			
	Authenticity check fails?	The verifier checks whether the document passes or fails the authenticity check.	Verifier
	A2.1.6 Abort on-boarding	In case of failure, the verifier aborts on-boarding of the applicant and informs the financial Institution and the applicant.	Verifier
Results	<ul style="list-style-type: none"> The presented document successfully passes the authenticity check; or Alternatively, if the authenticity of the document is not confirmed, the verifier aborts the on-boarding. 		

A2.2 - IDENTITY CHECK – DOCUMENT TYPE 2/3

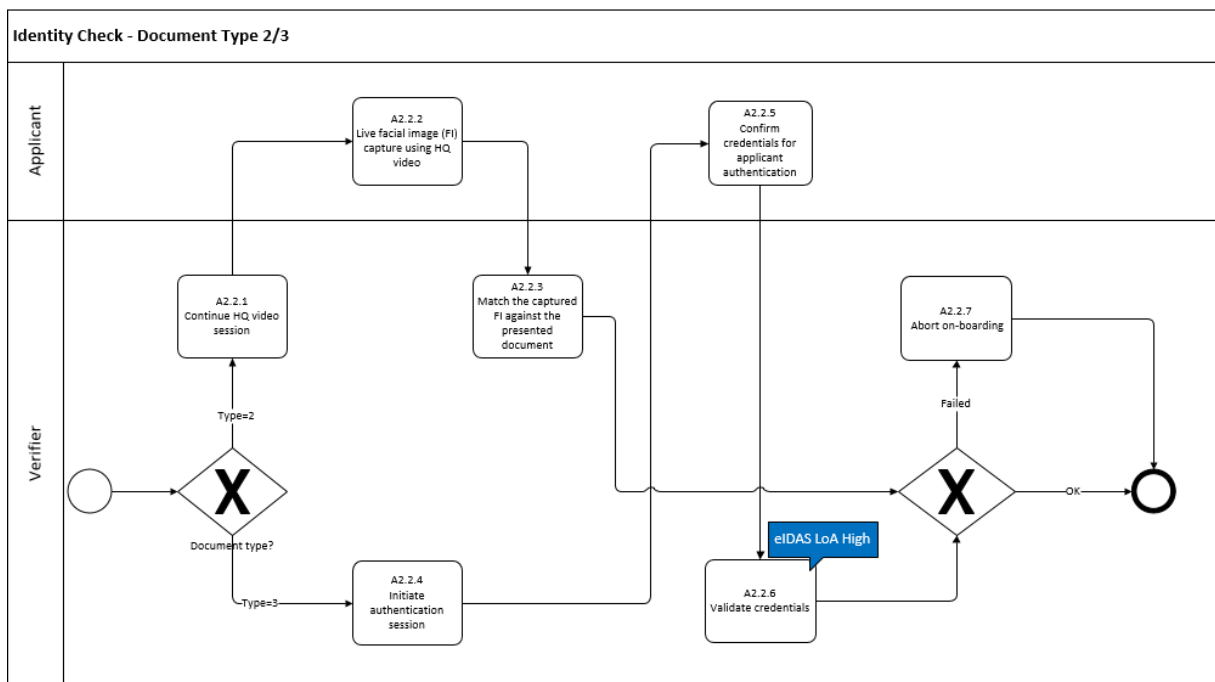


Figure 12. Identity Check – Document Type 2/3

Identity Check – Document Type 2/3			
Description	The verifier checks that the applicant is the holder of the presented document by comparing the 'owner of the document' versus the 'bearer of the document'. The owner is the person whose name is mentioned in the document. The bearer is the applicant.		
Input	Government issued document(s) – Document type 2/3		
Actors	<ul style="list-style-type: none"> Applicant Verifier 		
	Activity	Responsibilities	Actor
	Document	The verifier checks the document type.	Verifier

Process		Identity Check – Document Type 2/3	
	type?		
A2.2.1	Continue HQ video session	If the applicant has a document type 2 : The verifier continues the HQ video session with the Applicant.	Verifier
A2.2.2	Live facial image (FI) capture using HQ video	Document type 2 : During the HQ video session the applicant captures a live Facial Image (FI).	Applicant
A2.2.3	Match the captured FI against the presented document	Document type 2 : The verifier compares the captured FI to the one on the presented document.	Verifier
A2.2.4	Initiate authentication session	If the applicant has a document type 3 : the verifier initiates an authentication session.	Verifier
A2.2.5	Confirm credentials for applicant authentication	Document type 3 : During the authentication session the applicant confirms her/his credentials by, for example, entering a pin code on an eID reader.	Applicant
A2.2.6	Validate credentials	Document type 3 : The verifier validates the applicant's credentials using an electronic authentication protocol. The eIDAS Level of Assurance qualifies this authentication as per Regulation 2015/1502. The network of eIDAS nodes supports cross-border authentication.	Verifier
	Identity check fails?	The verifier checks whether the applicant passes or fails the identity check.	Verifier
A2.2.7	Abort on-boarding	In case of failure, the verifier aborts on-boarding of the applicant and informs the financial institution and the applicant.	Verifier
Results	<ul style="list-style-type: none"> • The applicant successfully passes the identity check, the on-boarding process is continued; or • The verifier aborts the on-boarding process. 		

A2.3 - FRAUD CHECK OF THE DOCUMENT

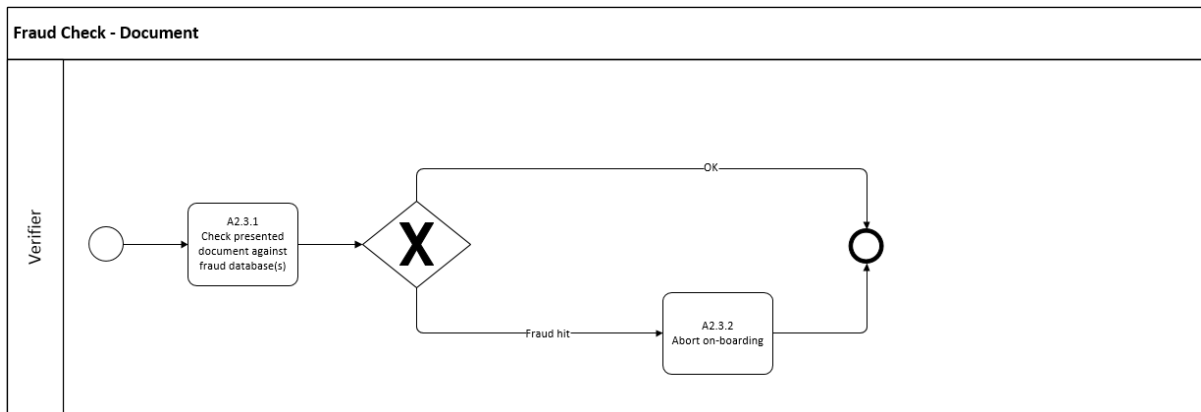


Figure 13. Fraud check of the document

Process	Fraud check of the document		
Description	The presented document(s) is (are) checked against a fraud database(s).		
Input	Government issued document(s) – Document type 2/3		
Actors	<ul style="list-style-type: none"> • Verifier 		
	Activity	Responsibilities	Actor
	A2.3.1 Check presented document against fraud database(s)	<p>The verifier checks the document's data against fraud database(s) (e.g. stolen passports database; population register (to confirm it belongs to a living person)).</p> <p>If the applicant has a document type 2: The MRZ contains the applicant's identity attributes (e.g. first and last name, date of birth, etc.) and the information on the presented document (e.g. issuer, document number, etc.). This information can be automatically collected via OCR, entered in the system and be used to perform anti-fraud checks against fraud document listings.</p> <p>If the applicant has a document type 3: The information in an eID means provides details on the identity which can be automatically uploaded in the system and be used to perform anti-fraud checks.</p>	Verifier
	A2.3.2 Abort on-boarding	In case of failure, the verifier aborts on-boarding of the applicant and informs the financial institution and the applicant.	Verifier

Process	Fraud check of the document
Results	<ul style="list-style-type: none"> If the document successfully passes the fraud check, the on-boarding is continued; or If there is a fraud hit, the verifier aborts on-boarding.

A2.4 - Fraud/PEP check of the applicant

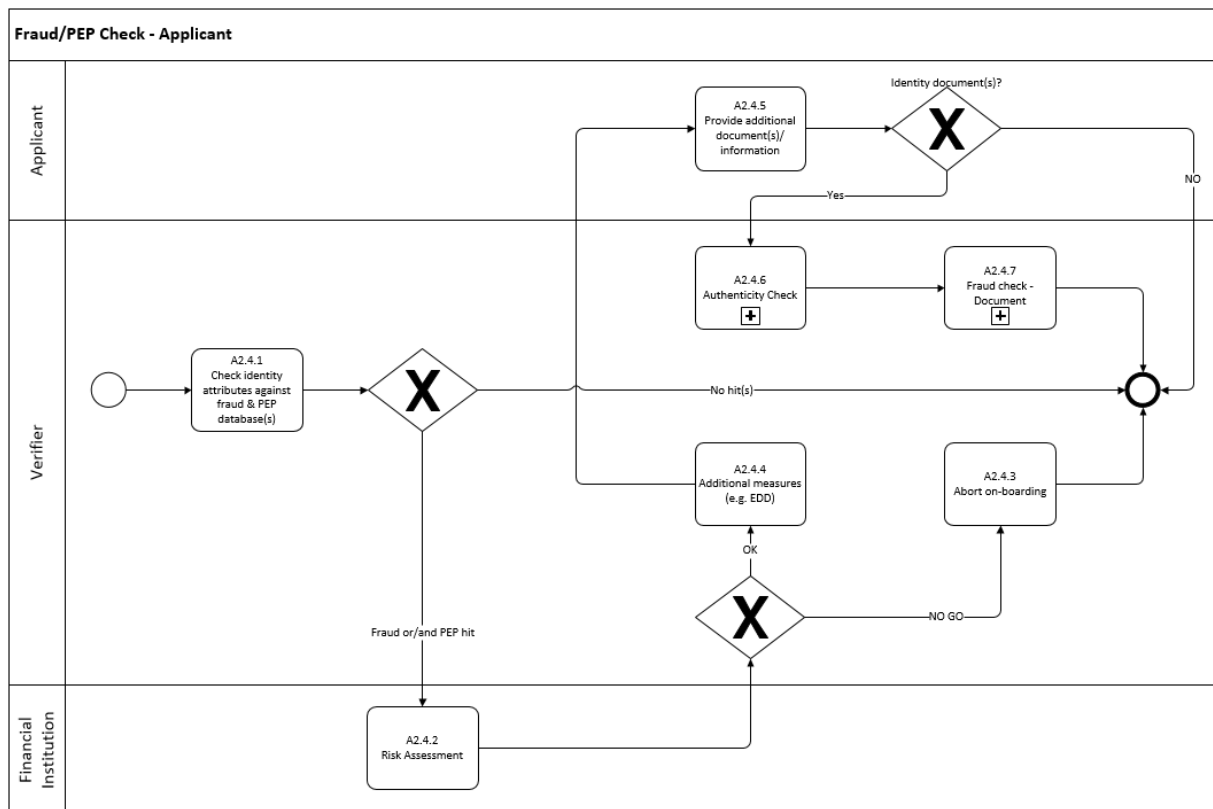


Figure 14. Fraud/PEP check of the applicant

Process	Fraud/PEP check of the applicant		
Description	Check of the identity attributes of the applicant against fraud and PEP database(s).		
Input	Government issued document(s) – Document type 2/3		
Actors	<ul style="list-style-type: none"> Applicant (if required) Verifier 		
	Activity	Responsibilities	Actor
	A2.4.1 Check identity attributes against fraud & PEP	The verifier checks the applicant’s identity attributes against a fraud database (e.g. negative media database, criminal records database, sanctions database) and a PEP database: If the applicant has a document type 2 :	Verifier

Process	Fraud/PEP check of the applicant		
	database(s)	<p>The MRZ contains the applicant identity attributes (e.g. first and last name, date of birth, etc.). This information can be automatically collected via OCR, entered in the system and be used to perform anti-fraud/PEP checks.</p> <p>If the applicant has a document type 3: The information in the eID means provides details on the identity which can potentially be automatically uploaded in the system and used to perform anti-fraud/PEP checks.</p>	
	Fraud/PEP hit?	The verifier checks if there any hits regarding the applicant.	Verifier
A2.4.2 Risk Assessment		<p>If there is a fraud and/or a PEP hit, the financial institution performs a risk assessment of the hit(s) associated with the applicant and based on the assessment decides:</p> <ul style="list-style-type: none"> to instruct the verifier to abort the on-boarding process if the risk is too high; or to instruct the verifier to apply additional or enhanced customer due diligence (EDD) measures. 	Financial Institution
A2.4.3 Abort on-boarding		In case of failure, the verifier aborts on-boarding of the applicant and informs the financial institution and the applicant.	Verifier
A2.4.4 Additional measures (EDD)		The verifier requests the applicant to provide additional (identity) documents or information (e.g. source of wealth, etc.) which can mitigate the risk associated with the hit.	Verifier
A2.4.5 Provide additional document / information		The applicant provides the document(s)/information upon request.	Applicant
Identity document(s)		If an additional identity document is provided, the verifier should perform the same activities as for other identity documents previously provided.	Verifier
A2.4.6 Authenticity check		Please refer to A2.1 - Authenticity check of the document	Verifier
A2.4.7 Fraud check		Please refer to A2.3 - Fraud check of the document	Verifier

Process	Fraud/PEP check of the applicant
Results	<ul style="list-style-type: none"> If there are no fraud/PEP hits on the applicant or the risk associated with the hit(s) is mitigated by the additional measures, the on-boarding process is continued; or If the risk associated with the fraud/PEP hit(s) remains too high, the verifier aborts the on-boarding process.

Phase 3 – Collection

A3 - Collect information

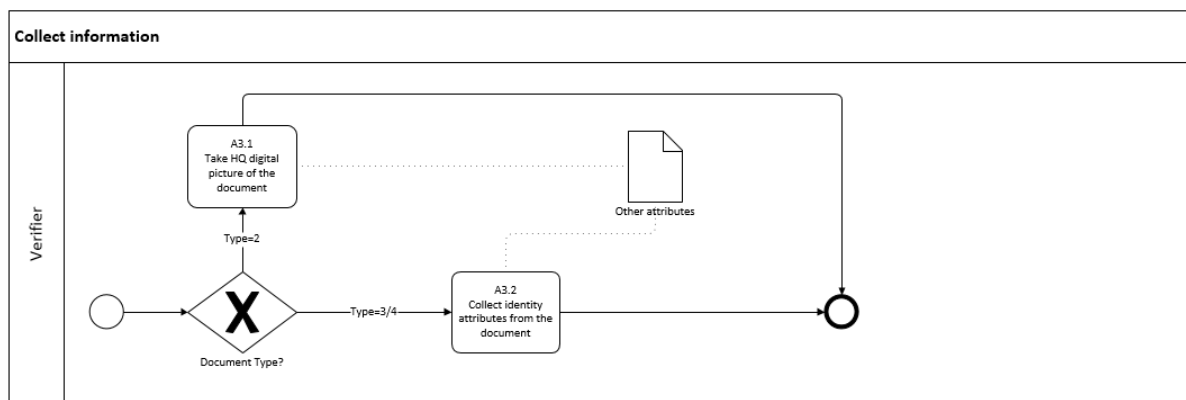


Figure 15. Collect information

Process	Collect information		
Description	The verifier collects identity attributes from the presented document.		
Input	Government issued document(s) – Document type 2/3		
Actors	<ul style="list-style-type: none"> Verifier 		
Phase	Activity	Responsibilities	Actor
Phase 3 - Collection	Document type?	The verifier checks the document type.	Verifier
	A3.1 Take HQ digital picture of the document	If the applicant has a document type 2 : Once the MRZ zone is read by the verifier, the information can be stored as a digital picture or in an electronic document format of choice depending on the solution used.	Verifier
	A3.2 Collect identity attributes from the	If the applicant has a document type 3 : Collection of identity attributes from the eID can be facilitated through various digital means depending on the back-end technologies used. Generally, identity attributes are obtained directly from an	Verifier

Process	Collect information	
	document	electronic passport or an eID chip.
Results	<p>Depending on the document type, the verifier collects a digital copy of the presented document as well as other attributes required for the on-boarding of the applicant.</p> <p><i>Remark:</i></p> <p><i>Other attributes (e.g. occupation, nationality) are commonly required by KYC procedures. The eIDAS Regulation supports the collection of the identity attributes via the minimum data set. Today only this eIDAS minimum data set is guaranteed to be available in the eIDAS means and transmitted through the eIDAS nodes. However, for on-boarding, a financial institution may need other identity attributes (e.g. nationality) and KYC attributes (e.g. occupation, source of wealth) which are obtained from different sources. Following the eIDAS interoperability framework and technical specifications, the eIDAS extended data set can support additional attributes as needed by financial institutions for on-boarding. These additional attributes may require bilateral agreements for acceptance. Alternatively, eIDAS signed or sealed assertions can be used to provide corroborating information.</i></p>	

Phase 4 – Management

A4 - Manage information

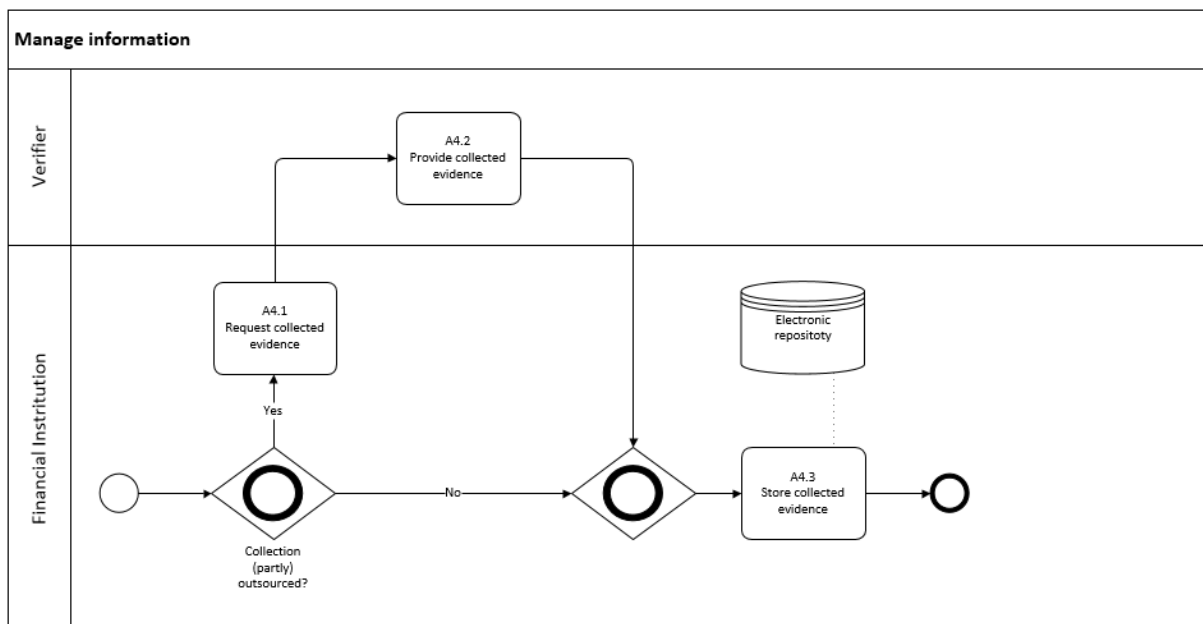


Figure 16. Manage information

Process	Manage information
Description	A financial institution stores the attributes in an electronic repository.

Process	Manage information		
Input	Government issued document(s) – Document type 2/3		
Actors	<ul style="list-style-type: none"> • Verifier • Financial Institution 		
Phase	Activity	Responsibilities	Actor
Phase 4 – Management	A4.1 Request collected evidence	When the verification and collection phases of the on-boarding process are (partly) outsourced, the financial institution requests the verifier to provide information which was collected.	Financial Institution
	A4.2 Provide collected evidence	On a contractual basis, the verifier is obliged to provide the data to the financial institution.	Verifier
	A4.3 Store collected evidence	The financial institution stores the collected evidence. The digital copy of the presented document is stored depending on their type: Document type 2 : The digital copy provided. Document type 3 : The identity attributes that are obtained directly from the eID means.	Financial Institution
Results	<ul style="list-style-type: none"> • The attributes are stored in an electronic repository at the financial institution. • The applicant successfully completes the on-boarding process. 		

On-boarding of a legal person

The following flowchart provides the main overview of the (potential) digital on-boarding process for a legal person:

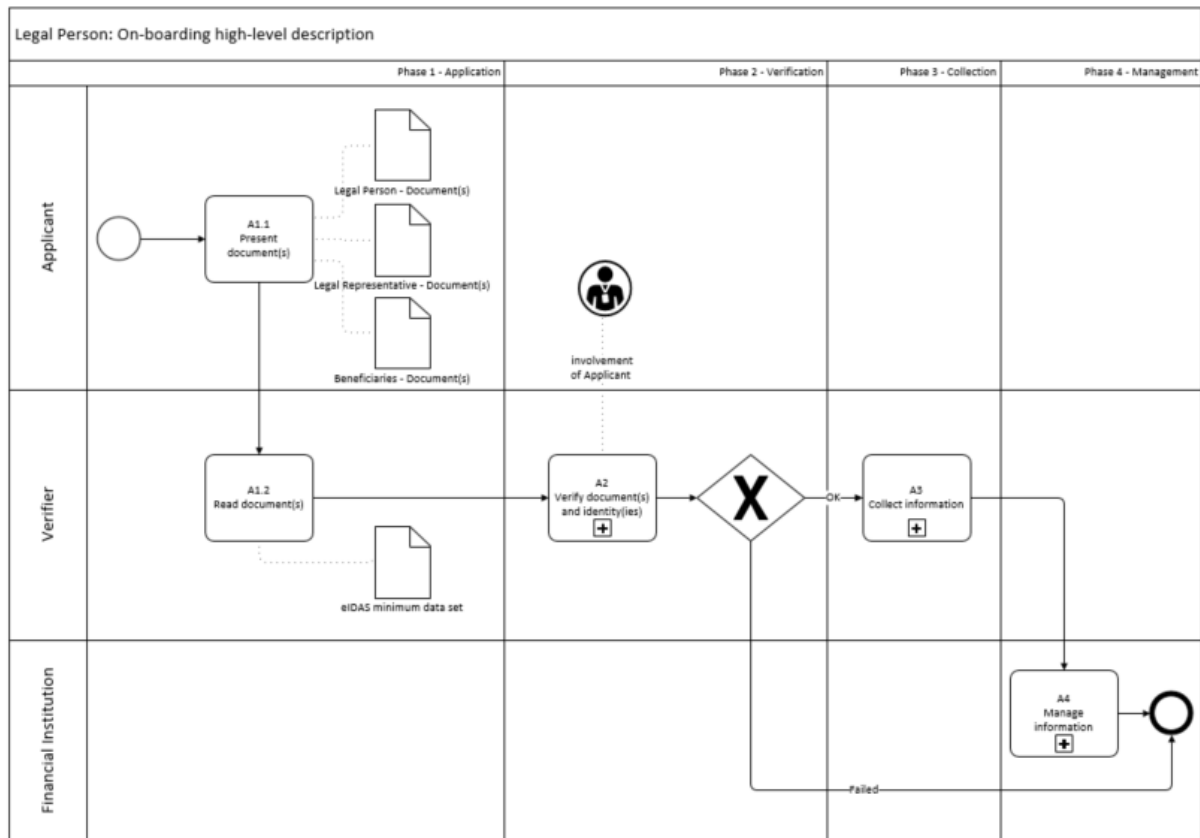


Figure 17. On-boarding process flow of a legal person

Process	On-boarding of a legal person
Description	The process flow in Figure 17 provides a high level description of the on-boarding of a legal person in four phases. It shows process activities through which a financial institution fulfils KYC and AML requirements when on-boarding a potential customer.
Input	<ul style="list-style-type: none"> For the applicant: government issued document(s) - documents confirming the identity of a legal person, which include, at least, information on a legal name, a legal address and a unique identifier as part of official registration documents (e.g. certificate of incorporation, extract from a company register, Articles of Association/ Incorporation, Legal Acts) in a machine-readable form. For beneficiaries: government issued documents confirming identity of a natural person (Document type 2/3) - see On-boarding of a natural person Phase 1 - Application. For a legal representative (where applicable and if a

Process		On-boarding of a legal person	
		<p>natural person) such as, government issued documents confirming the identity of a natural person (Document type 2/3) - see On-boarding of a natural person Phase 1 - Application; or government issued document(s) confirming legal representation rights, which are: powers (e.g. Power of Attorney), mandates - in a machine-readable format.</p>	
Actors		<ul style="list-style-type: none"> • Applicant • Verifier • Financial Institution 	
Phase	Activity	Responsibilities	Actor
Phase 1 Application	A1.1 Present document(s)	The applicant indicates its intention to become a customer of a financial institution and provides a verifier with its identity document(s) and the identity document(s) of its beneficiaries using a technology in line with the document type. If the legal representative is involved, the identity document(s) of the representative together with the legal representation rights are provided as well.	Applicant
	A1.2 Read document(s)	<p>For the applicant-related documents: the verifier digitally reads the applicant's documents using the relevant technology.</p> <p>For beneficiaries/legal representative related documents the verifier acts in line with A1.2 of the on-boarding process of a natural person (see On-boarding of a natural person - Phase 1 - Application). At this step the verifier obtains the eIDAS minimum data set as defined in the Regulation (EU) 2015/1501.</p>	Verifier
Phase 2 Verification	A2 Verify document and identity	The verifier conducts verification of the provided documents, identifies the applicant, its beneficiaries and where applicable, the legal representative, as well as performs a fraud check of the documents, the applicant/its beneficiaries and the legal representative (where applicable). Note that some activities of this sub-process require involvement of the applicant. More details are provided in the following sections.	(Applicant) /Verifier
Phase 3 Collection	A3 Collect information	The verifier collects identity attributes.	Verifier

Process		On-boarding of a legal person	
Phase 4 Management	A4 Manage information	The financial institution stores the collected attributes in an electronic repository.	Financial Institution
Results	<ul style="list-style-type: none"> The applicant successfully completes the on-boarding process, in this case the required evidence is stored by the financial institution; or The applicant is rejected from on-boarding, in this case the reason for rejection is recorded. 		

Phase 1 - Application

Activities (A1.1 and A1.2) of the Application phase are described in the table above.

Phase 2 – Verification

A2 - Verify the document’s authenticity and the applicant’s identity

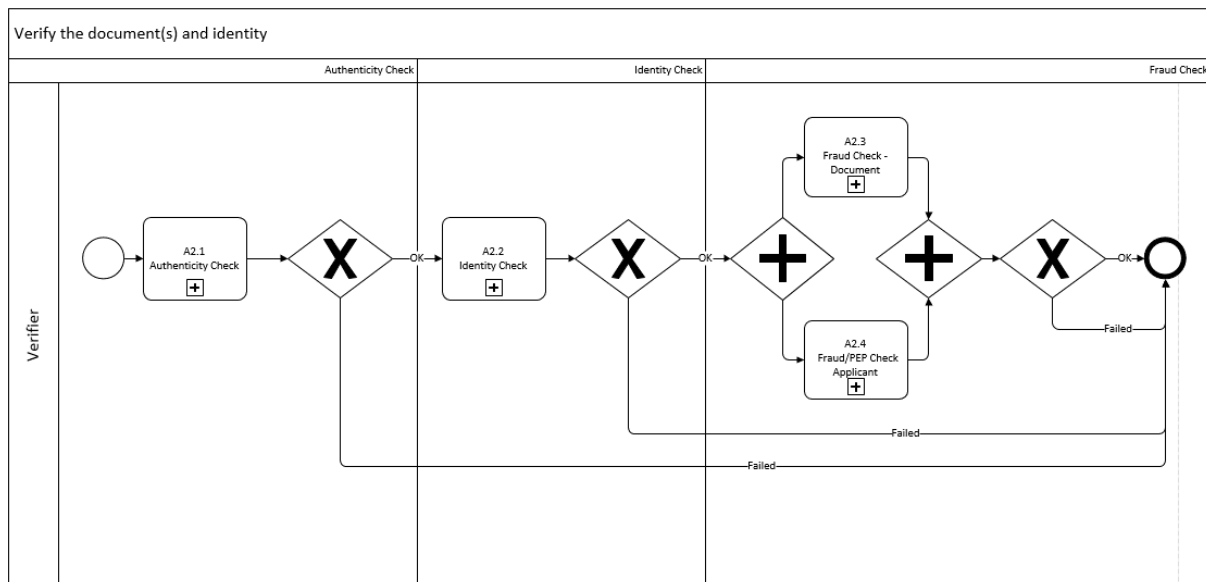


Figure 18. Verification the document’s authenticity and the applicant’s identity

Process		Verify the document’s authenticity and the applicant’s identity
Description	The verifier conducts verification of the provided government issued documents, identifies the applicant, its beneficiaries and a legal representative (where applicable), as well as performs a fraud check.	
Input	<ul style="list-style-type: none"> For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) For beneficiaries: document(s) confirming identity of a natural person For a legal representative (where applicable): 	

Process	Verify the document's authenticity and the applicant's identity		
	<ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Applicant (if required) • Verifier 		
Phase	Activity	Responsibilities	Actor
Phase 2 Verification	A2.1 Authenticity Check	Verification that the presented documents are genuine.	Verifier
	A2.2 Identity Check	Check that the applicant, its beneficiaries and a legal representative (where applicable) are the holders of the documents they presented.	Verifier
	A2.3 Fraud Check - Document	Check of the presented documents against fraud database(s).	Verifier
	A2.4 Fraud/PEP Check - Applicant	Check of the identity attributes of the applicant against fraud database(s) and PEP database.	Verifier
Results	<ul style="list-style-type: none"> • If the applicant/its beneficiaries/legal representative (where applicable) successfully complete all steps of the verification process, their data is collected and after that managed (i.e. stored in an electronic repository); or • If the applicant/its beneficiaries/legal representative (where applicable) fail to comply with any of the verification activities, the application is rejected, the reason for rejection is stored. 		

A2.1 - Authenticity check of the documents

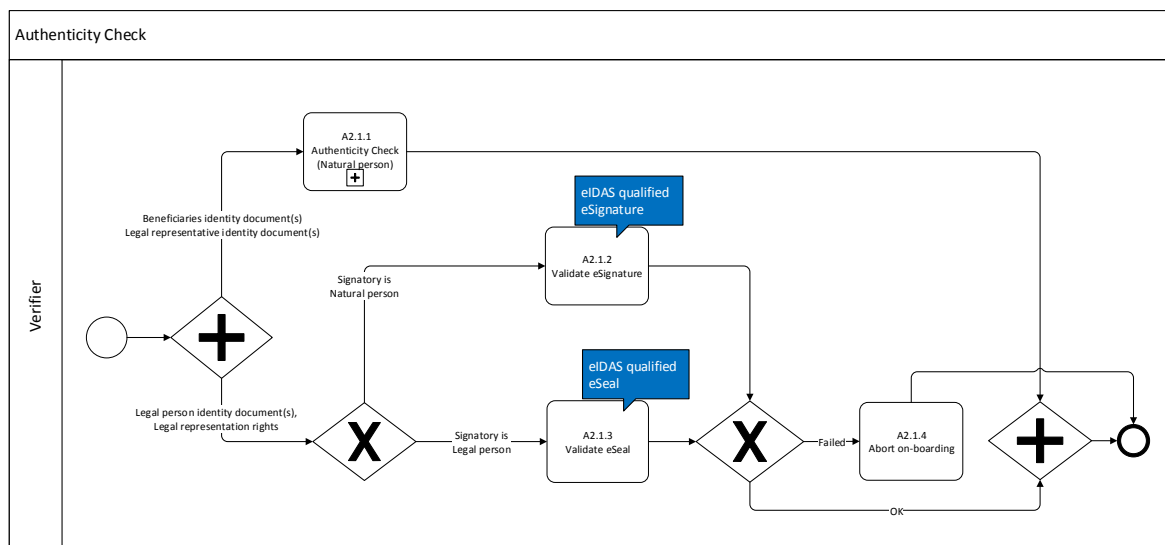


Figure 19. Authenticity checks of the documents

Process	Authenticity check of the documents		
Description	Verification that the presented documents are genuine.		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Verifier 		
	Activity	Responsibilities	Actor
	Documents of the Applicant/beneficiaries/legal representative?	The verifier checks whether the documents belong to the applicant, to its beneficiaries or to a legal representative. Following this, the verifier performs authenticity check of the documents of a natural person (for identity documents of beneficiaries and a legal representative) and of a legal person (the applicant's identity documents).	Verifier
	A2.1.1 Authenticity Check (Natural person)	Authenticity check of the presented documents of a natural person: in order to verify the authenticity of the presented identity documents of beneficiaries and a legal representative (where applicable), the verifier acts in line with the process described in A2.1 - Authenticity check of the document of a natural person's on-boarding	Verifier
	Is a signatory a natural or legal person?	Authenticity check of the presented documents of a legal person: firstly, the verifier checks who the signatory of the document was, in order to select a validation approach. After that the verifier performs the appropriate branch of the validation approach.	Verifier
	A2.1.2 Validate eSignature	If the signatory is a natural person, the verifier validates eSignature. The verifier validates the eSignature over the document's file structure stored in the chip. This eSignature is generated by the Document Issuer, i.e. a government entity of a Member State, or on its behalf. eIDAS qualified eSignature can support this task. If supported by the document's chip, further cryptographic challenge/response protocols can be used to verify the	Verifier

Process		Authenticity check of the documents	
		authenticity of the chip, the binding of the chip to the particular document etc.	
A2.1.3	Validate eSeal	If the signatory is a legal person, the verifier validates the presented eSeal. An eIDAS qualified eSeal could be used to confirm a document's authenticity. The eSeal is validated based on the electronic signature using the certificate issued by a trust service provider. The eSeal can be attached to corroborating information.	Verifier
	Authenticity check fails?	The verifier checks whether the documents pass or fail the authenticity check.	Verifier
A2.1.4	Abort on-boarding	The verifier aborts on-boarding of the applicant if one of the activities fail, and informs the financial institution and the applicant.	Verifier
Results	<ul style="list-style-type: none"> The presented documents successfully pass the different authenticity checks. On-boarding is continued; or If the authenticity of the documents is not confirmed, the verifier aborts the on-boarding. 		

A2.2 - Identity check of the applicant, beneficiaries and legal representative

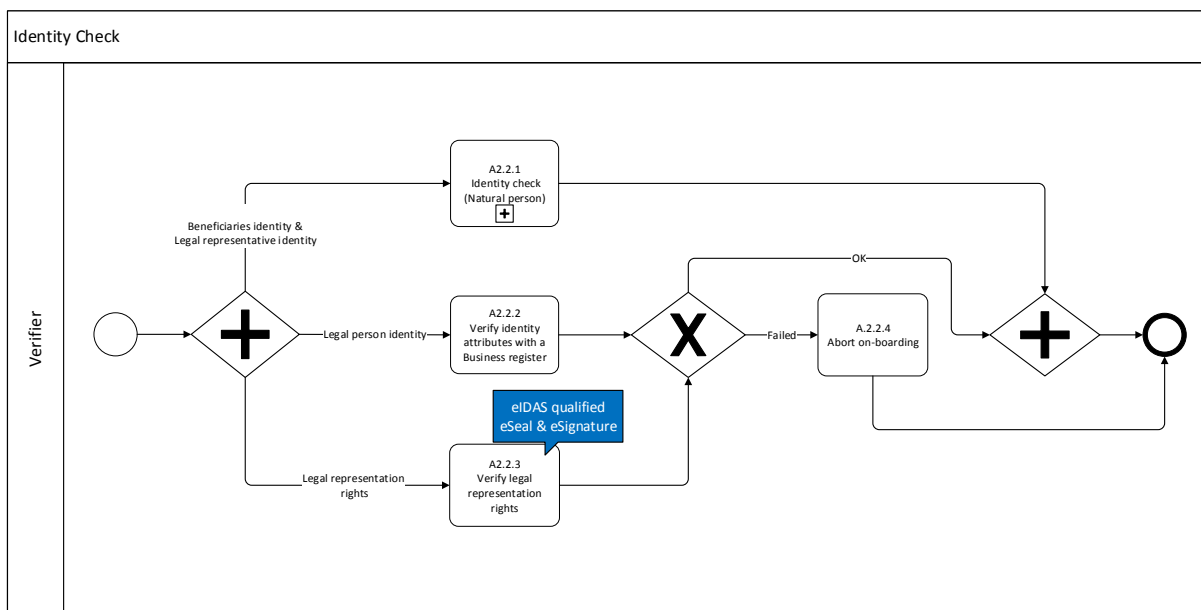


Figure 20. Identity check of the applicant, beneficiaries and legal representative

Process	Identity check of the applicant, beneficiaries and a legal representative
Description	The verifier checks that the applicant/its beneficiaries/a legal representative & legal representation rights (where applicable) are the

Process	Identity check of the applicant, beneficiaries and a legal representative		
	holders of the presented documents by comparing the 'owner of the document' versus the 'bearer of the document'. The owner is the person whose name is mentioned in the document. The bearer is the applicant.		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Verifier 		
	Activity	Responsibilities	Actor
	Documents of the Applicant/beneficiaries/legal representative?	The verifier checks whether the documents belong to the applicant, to its beneficiaries or to a legal representative. Following this, the verifier performs an identity check of the applicant, its beneficiaries and a legal representative in parallel.	Verifier
	A2.2.1 Identity Check (Natural person)	In order to verify the identity of a natural person (beneficiaries and a legal representative, where applicable), the verifier acts in line with processes of on-boarding of a natural person described in A2.2 - Identity Check – Document Type 2/3.	Verifier
	A2.2.2 Verify identity attributes with a Business register	In order to verify the identity of a legal person of the applicant, the verifier verifies identity attributes of the applicant using a business register (e.g. a company register) from the issued Member State. As the European business registers are interconnected ³² since June 2017, information can be verified through their e-Justice based search portal.	Verifier
	A2.2.3 Verify legal representation rights	In order to confirm legal representative rights when a legal representative (a natural person) acts on behalf of the applicant via a power/mandate, the verifier verifies that the legal representative has	Verifier

³² Business Registers Interconnection system (BRIS), set up in line with Directive 2012/17/EU, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:156:0001:0009:en:PDF>
And Commission Implementation Regulation (EU) 2015/884, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0884>

Process		Identity check of the applicant, beneficiaries and a legal representative	
		<p>the rights to represent the applicant.</p> <p>This can be done via verification with a business register, where there is information on appointments and terminations of a company's representatives, and the extent of their powers.</p> <p>In case that such information is provided in electronic form, eIDAS qualified eSignature and eSeal can support this task, because the verifier can validate this legal representation rights information which should be signed with the legal representative eSignature and the legal person's eSeal. The combination of the eSignature and the eSeal confirms the ability of the representative to act on behalf of the applicant.</p>	
	Identity check fails?	The verifier checks whether the applicant/its beneficiaries/legal representative pass or fail the identity check.	Verifier
	A2.2.4 Abort on-boarding	As identity check is done in parallel, all parallel processes should be completed successfully. The verifier aborts on-boarding of the applicant if one of the checks fail, and informs the financial institution and the applicant.	Verifier
Results	<ul style="list-style-type: none"> • The applicant, its beneficiaries and the legal representative (where applicable) successfully pass the identity check(s) and on-boarding is continued; or • If the identities of the applicant/beneficiaries/legal representative are not confirmed, the verifier aborts the on-boarding. 		

A2.3 - Fraud check of the documents

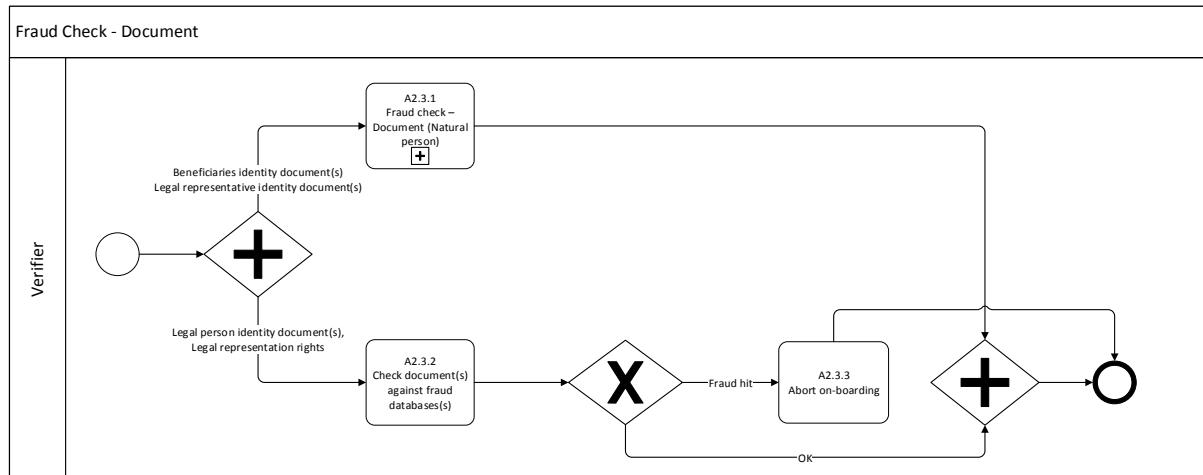


Figure 21. Fraud check of the documents

Process	Fraud check of the documents		
Description	In this activity, the presented documents are checked against a fraud database.		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Verifier 		
	Activity	Responsibilities	Actor
	Documents of the Applicant/ beneficiaries/ legal representative?	The verifier checks whether the documents belong to the applicant, to its beneficiaries or to a legal representative. Following this, the verifier performs a fraud check of the documents of the applicant, its beneficiaries and a legal representative in parallel.	Verifier
	A2.3.1 Fraud check - Document (Natural person)	In order to perform an anti-fraud check of the identity documents of a natural person (beneficiaries and a legal representative, where applicable), the verifier acts in line with A2.3 - Fraud check of the document of the on-boarding process of a natural person.	Verifier
	A2.3.2	In order to conduct an anti-fraud check of	Verifier

Process			
	Check documents against fraud database(s)	the identity documents of a legal person (the applicant), the verifier extracts the identification data of the applicant from the presented documents and checks them in a fraud database, and e.g. a business register.	
	Fraud check fails?	The verifier checks whether the documents pass or fail the fraud check.	Verifier
	A2.3.3 Abort on-boarding	All parallel processes should be completed successfully. The verifier aborts on-boarding of the applicant if one of the checks fail, and informs the financial institution and the applicant.	Verifier
Results			
	<ul style="list-style-type: none"> • If the applicant/its beneficiaries and a legal representative (where applicable) successfully pass the anti-fraud check(s) of the presented documents, the on-boarding is continued; or • If there is a fraud hit, the verifier aborts the on-boarding. 		

A2.4 - Fraud/PEP checks of the applicant, its beneficiaries and a legal representative

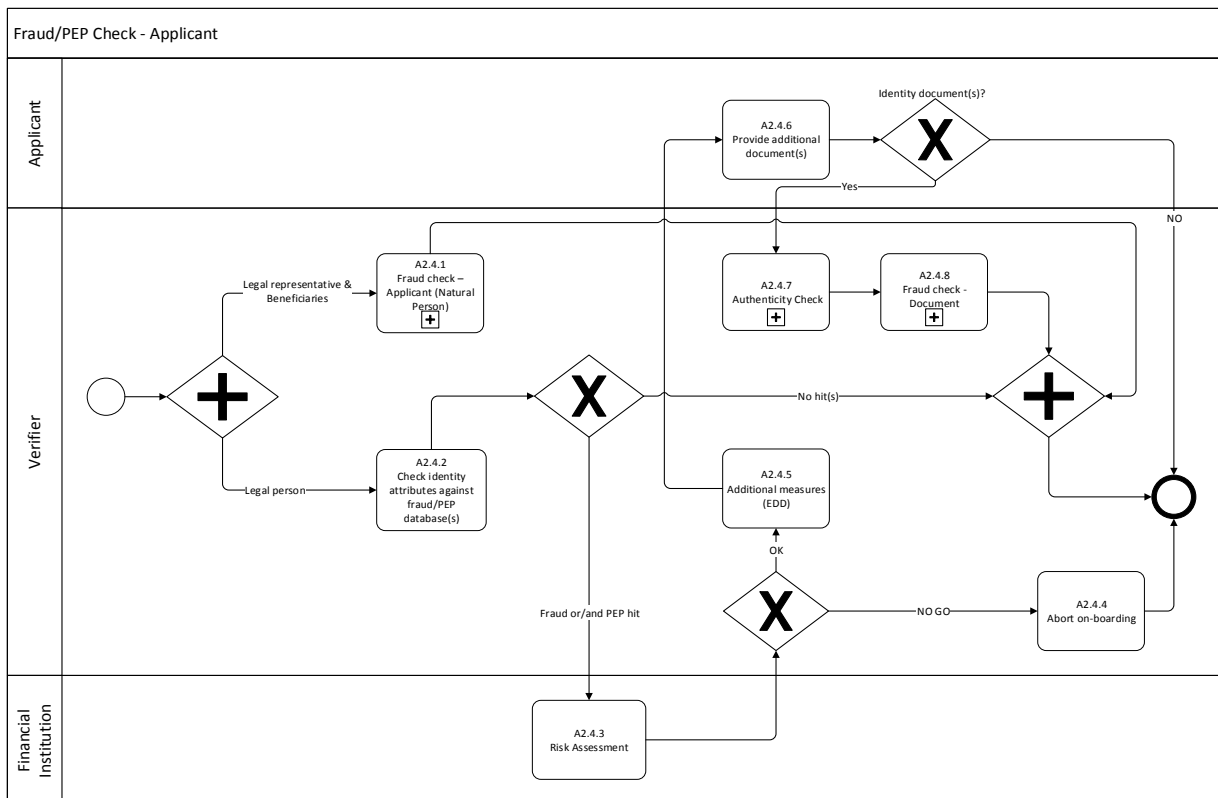


Figure 22. Fraud/PEP Checks of the applicant, beneficiaries and legal representative

Process			
Fraud checks of the applicant, beneficiaries and legal representative			
Description	Check of the identity attributes of the applicant/ its beneficiaries and a legal representative (where applicable) against fraud and PEP database(s).		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Applicant (if required) • Verifier • Financial Institution 		
	Activity	Responsibilities	Actor
	Documents of the Applicant/ beneficiaries/ legal representative ?	The verifier checks whether the documents belong to the applicant, to its beneficiaries or to a legal representative. Following this, the verifier performs fraud check(s) of the applicant, its beneficiaries and a legal representative, where applicable.	Verifier
	A2.4.1 Fraud check –Applicant (Natural person)	In order to perform a fraud/PEP check of the natural person (beneficiaries and a legal representative), the verifier performs the fraud and PEP checks in line with the A2.4 - Fraud/PEP check of the applicant of the on-boarding process of a natural person.	Verifier
	A2.4.2 Check identity attributes against fraud & PEP database(s)	When the verifier conducts a fraud/PEP check of the legal person's (the applicant's) identity attributes the verifier extracts the identification data of the applicant from the presented documents and automatically checks them against blacklisting databases (e.g. negative media database, sanctions) and a PEP database.	Verifier
	Fraud/PEP hit?	The verifier checks if there are any (fraud and/or PEP) hits regarding the applicant.	Verifier
	A2.4.3 Risk Assessment	If there is a fraud and/or a PEP hit, the financial institution performs a risk assessment of the hit associated with the applicant and based on the assessment decides:	Financial Institution

Process	Fraud checks of the applicant, beneficiaries and legal representative		
		<ul style="list-style-type: none"> to instruct the verifier to abort the on-boarding process if the risk is too high; or to instruct the verifier to apply additional measures as part of enhanced customer due diligence (EDD). 	
	A2.4.4 Abort on-boarding	The verifier aborts on-boarding of the applicant if the risk associated with the fraud/PEP check is above the risk threshold, and informs the financial institution and the applicant.	Verifier
	A2.4.5 Additional measures (EDD)	The verifier requests the applicant to provide an additional document(s), including additional identity document(s); or information (e.g. source of funds, etc.) which can mitigate the risk associated with the hit.	Verifier
	A2.4.6 Provide additional document(s)/ information	The applicant provides the document(s)/information upon request.	Applicant
	Identity document(s)	If additional identity documents are provided, the verifier should perform the same activities as for other identity documents previously provided.	Verifier
	A2.4.7 Authenticity check	Please refer to A2.1 - Authenticity check of the document of a natural person.	Verifier
	A2.4.8 Fraud check - Document	Please refer to A2.3 - Fraud check of the document of a natural person.	Verifier
Results	<ul style="list-style-type: none"> If there is no fraud/PEP hit on the applicant/its beneficiaries/a legal representative (where applicable) or the risk associated with any hits is mitigated by the EDD measures, the on-boarding is continued; or When the risk associated with the fraud/PEP hit(s) is too high, the verifier aborts the on-boarding (usually on request of the financial institution). 		

Phase 3 – Collection

A3 – Collect information

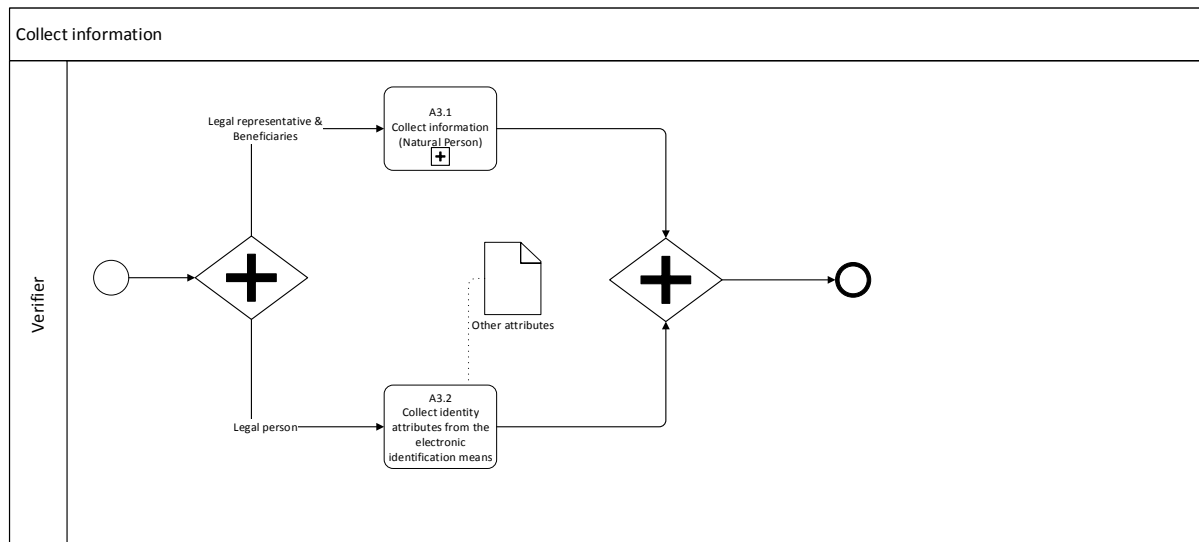


Figure 23. Collect information

Process	Collect information		
Description	The verifier collects identity attributes from the presented documents.		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Verifier 		
Phase	Activity	Responsibilities	Actor
Phase 3 - Collection	Documents of the Applicant/beneficiaries/legal representative?	<p>The verifier checks whether the documents belong to the applicant, to its beneficiaries or to a legal representative.</p> <p>Following this, the verifier in parallel performs collection of the information for a natural and for a legal person.</p>	Verifier
	A3.1 Collect information (Natural person)	In order to collect information on the beneficiaries and the legal representative (where applicable), the verifier collects identity information of natural persons in line with A3 - Collect information of the on-boarding of a natural person.	Verifier

Process		Collect information	
	A3.2 Collect identity attributes from the electronic identification means	For the legal person, the verifier collects identity attributes of the applicant from the electronic identification means which can be facilitated through various digital means depending on the back-end technologies used. Generally, the identity attributes are obtained directly from the electronic identification means during the verification process. This can be done from the eID chip or the mobile identity application.	Verifier
Results	<ul style="list-style-type: none"> The verifier collects a digital copy of the presented documents as well as other attributes required for the on-boarding of the applicant. <p><i>Remark:</i> Other attributes (e.g. country of incorporation) are commonly required by KYC procedures. The eIDAS Regulation supports the collection of the identity attributes via the minimum data set. Today only this eIDAS minimum data set is guaranteed to be available in the eIDAS means and transmitted through the eIDAS nodes. However, for on-boarding, a financial institution may need other identity attributes and KYC attributes (e.g. source of funds) which are obtained from different sources. Following the eIDAS interoperability framework and technical specifications, the eIDAS extended data set can support additional attributes as needed by financial institutions for on-boarding. These additional attributes may require bilateral agreements for acceptance. Alternatively, eIDAS signed or sealed assertions can be used to provide corroborating information.</p>		

Phase 4 - Management

A4 – Manage information

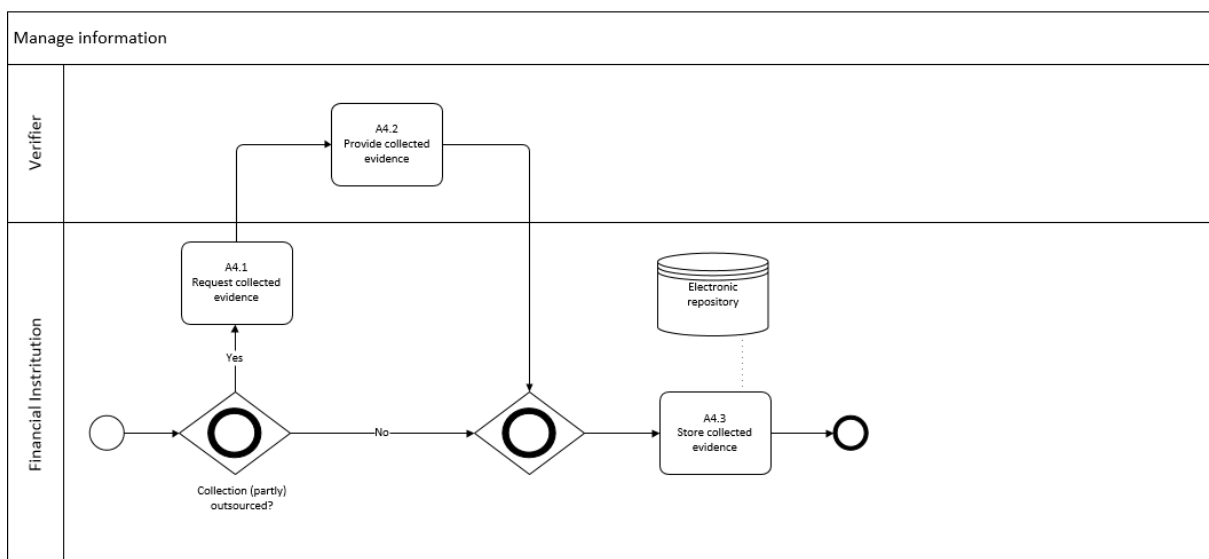


Figure 24. Manage information

Process		Manage information	
Description	A financial institution stores the attributes in an electronic repository.		
Input	<ul style="list-style-type: none"> • For the applicant: document(s) confirming identity of a legal person (e.g. extract from a company register, certificate of incorporation) • For beneficiaries: document(s) confirming identity of a natural person • For a legal representative (where applicable): <ul style="list-style-type: none"> - document(s) confirming identity of a natural person - document(s) confirming legal representation rights 		
Actors	<ul style="list-style-type: none"> • Verifier • Financial Institution 		
Phase	Activity	Responsibilities	Actor
Phase 4 – Management	A4.1 Request collected evidence	When the verification and collection phases are (partly) outsourced, the financial institution requests the verifier to provide information which was collected during the application and verification phases.	Financial Institution
	A4.2 Provide collected evidence	On a contractual basis, the verifier is obliged to provide the data to the financial institution.	Verifier
	A4.3 Store collected evidence	The financial institution stores collected evidence automatically in an electronic repository.	Financial Institution
Results	<ul style="list-style-type: none"> • The attributes are stored in an electronic repository at the financial institution. • The applicant successfully completes the on-boarding process. 		

Fully digital cross-border on-boarding process flow

Based on the findings described in previous sections eIDAS can support application, verification and collection phases of the on-boarding under the current AML regulation. Additionally, eIDAS could also help to improve the full digitalisation of the on-boarding process by relying on a notified eID. The flow chart below proposes a possible on-boarding flow for a natural person. Please note that the proposed process flow represents a potential future on-boarding process as it is not compliant with the current AML requirements because eIDAS notified eIDs are not amongst the officially accepted compliance means. Previously, 4 phases were used in our flow charts (application, verification, collection and management). These are now replaced by phases A, B and C. This demonstrates a higher degree of integration and usage of eIDAS, while achieving a similar functional outcome. It is shown how one phase can combine activities usually done in different phases.

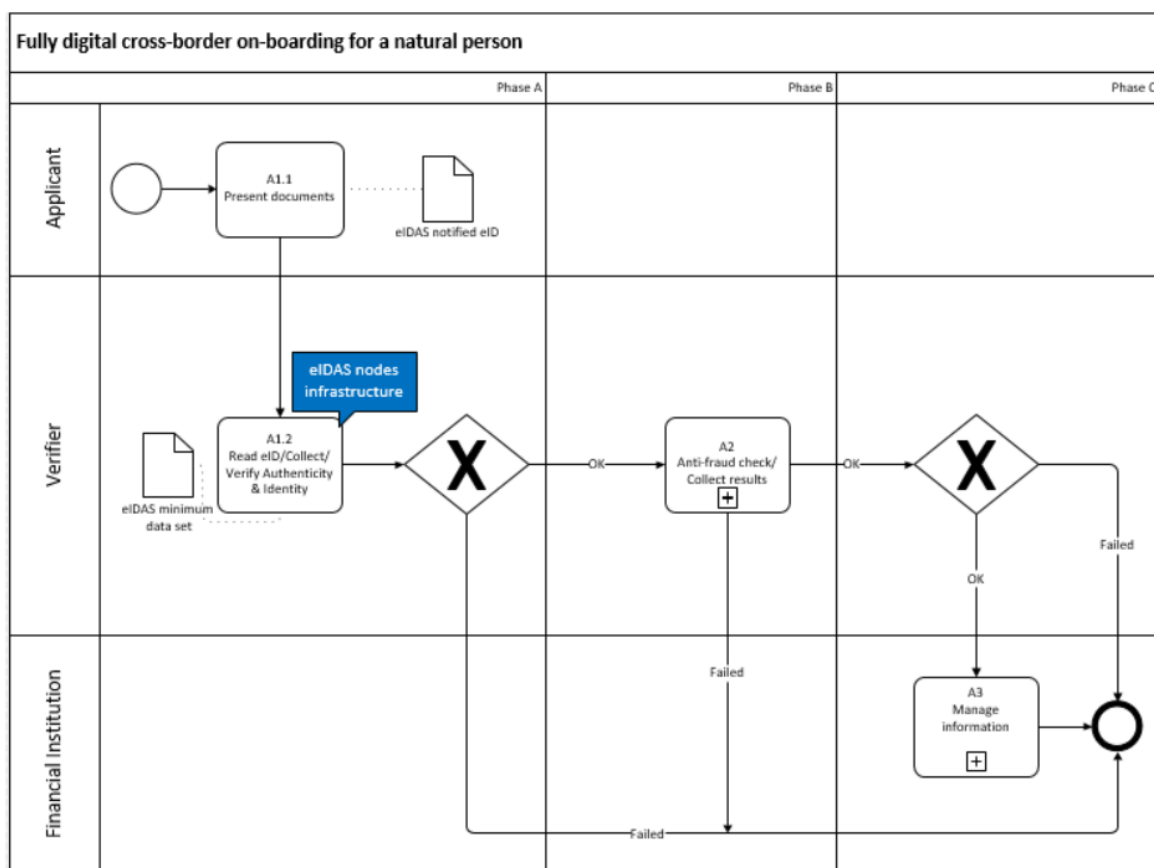


Figure 25. Online on-boarding process – Alternative process

Process	Online on-boarding for a natural person
Description	The process flow in Figure 25 provides a high level description of a fully online on-boarding process for a natural person.
Input	<ul style="list-style-type: none"> eIDAS notified eID (Document type 3)

Process			
Online on-boarding for a natural person			
Actors	<ul style="list-style-type: none"> • Applicant • Verifier • Financial Institution 		
Phase	Activity	Responsibilities	Actor
Phase A	A1.1 Present Documents	The applicant provides the eIDAS notified eID remotely to a verifier initiating the on-boarding process with a financial institution.	Applicant
Phase A	A1.2 Read/Collect /Verify Authenticity & Identity	<p>This activity includes and processes several on-boarding phases:</p> <ul style="list-style-type: none"> - The verifier digitally reads the eID from the applicant using eIDAS infrastructure. - The verifier certifies the authenticity of the eID and the identity of the applicant, through an authentication process. The use of a notified eID allows cross-board identification. The eIDAS nodes infrastructure ensures the authenticity of the electronic identification means (i.e. the notified eID) and the claimed identity of the applicant. The on-boarding process is halted if one of the verifications fails. - The verifier automatically collects the minimum data set attributes as per eIDAS. 	Verifier
Phase B	A2 Anti-fraud check /Collect results	<p>The verifier performs:</p> <ul style="list-style-type: none"> - a fraud check of the document: the document's attributes read from eID are automatically checked against fraud databases (e.g. stolen passports). The verifier acts in line with the process described in A2.1 - Authenticity check of the document of a natural person's on-boarding. - a PEP and fraud check of the applicant: the identity attributes read from eID are automatically checked against PEP/fraud/sanctions databases. The verifier performs the fraud and PEP checks in line with the A2.4 - Fraud/PEP check of the applicant of the on-boarding process of a natural person. - Automatically, the verifier collects results of the checks. In case of failure for the applicant to pass through the anti-fraud check, the 	Verifier

Process		Online on-boarding for a natural person	
		verifier aborts on-boarding.	
Phase C	A3 Manage information	The financial institution stores the collected attributes in an electronic repository.	Financial Institution
Results	<ul style="list-style-type: none"> • The applicant successfully completes the on-boarding process and the required evidence is stored by the financial institution; or • The on-boarding process is halted and the applicant is rejected. In this case, the reason and proof of rejection are recorded. 		

CHAPTER 6 CONCLUSION

The results from the interviews taken during Task 1 and the analysis in Task 2 demonstrates that a copy of a government issued document represents the common compliance means used by the surveyed financial institutions during verification and collection. Also, the collection is generally performed via a face-to-face meeting at a physical office of a financial institution. Divergent situations occur when the financial institution is a 'neobank' with no physical office, and, thus, collection and verification are performed remotely. This shows that most of the surveyed financial institutions make use of non-digital and mixed processes for on-boarding.

The analysis in Task 3 shows that digital solutions can be used for remote on-boarding in some of the surveyed institutions.

The digitalisation of the on-boarding process potentially allows a financial institution to increase its market reach and comply with (future) regulations. Depending on the type of document used, most of the non-digital process steps can potentially be replaced by a digital equivalent. The study also shows that digitalising of verification and collection steps will reduce the burden on an officer of the financial institution. However, it is important to guarantee the relevant level of assurance on the claimed identity and authenticity of the provided documents.

There already exist solution providers which implement emerging digital technologies aiming to simplify the identification, verification and collection steps for both the user (i.e. the applicant) and their clients (i.e. a financial institution or other service provider, such as a travel agency) (refer to Annex V). These solutions cover all the on-boarding phases and provide customers with self-control over their shared data, thus providing a possibility of data portability among other financial institutions and businesses, while preserving privacy rights of the applicant. Although the surveyed solutions are developed for natural persons, most of the providers are considering or are already in the process of becoming eIDAS compliant in order to provide a legal cross-border recognition for customer identification and verification service with the use of eIDAS compliant means, which will also further enhance the portability of verified identity information across Member States.

Based on the results from previous tasks, Task 4 provides a set of flowcharts that describes a potential end-to-end digital on-boarding process for both natural and legal persons underpinned by the eIDAS regulation. The use of notified eIDAS means, issued under eIDAS schemes, results in a guaranteed level of assurance of the claimed identity and the corresponding (minimum) data set. This also strengthens the different checks during the on-boarding as they are then based on information from trusted third parties (e.g., governments).

Furthermore, by leveraging the minimum data set one could expect an increase in portability of customer information and hence increase adoption of cross-border on-boarding among financial institutions and decrease the managerial burden for both the customer and the financial institutions.

Further work to standardise additional or other attributes, so that these can enrich the minimum data set, will provide additional value to the financial institution and the customer as well. Here eIDAS eSignatures and eSeals can help to guarantee the integrity of the corroborating information.

The evolving regulatory ecosystem both on the EU as well as a Member State level will further strengthen the potential of a fully digital on-boarding process by providing the necessary legal basis to support the requirements related to KYC and AML. Outside of the anti-money laundering context, there are other initiatives of the EU, such as PSD2, which provide additional possibilities for application of the eIDAS and electronic trust services.

Success of any digital process requires user or customer adoption. A clear regulatory framework supported by secure technology can surely provide this environment of trust. This implies the EU anti-money laundering directives give clear guidelines or limitations for the use of electronic identification means in order to achieve consistent levels of assurance across Member States.

GLOSSARY

The key terms used in this document are defined in the table below.

Table 9. Key terms description

Term	Description
AML	Anti-money laundering
Authentication	According to eIDAS Regulation, 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed
Beneficial owner	Beneficial owner means any natural person(s) who ultimately owns or controls the legal person(s) on whose behalf a transaction or activity is being conducted
Breeder document	A document that can serve as a basis to obtain other identification documents
CDD	Customer due diligence
EDD	Enhanced customer due diligence
eID	electronic identification
Electronic document (eDocument)	Any document in electronic format containing structured data and possibly also unstructured data
Electronic identification	'electronic identification' means the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person
Electronic Identification means	According to eIDAS Regulation, 'electronic identification means' means a material and/or immaterial unit containing personal identification data and which is used for authentication for an online service
ePassport	Electronic passport
EU	European Union
HQ	High quality
ICAO	International Civil Aviation Organization
ID	Identity
KYC	Know your customer
Legal person	A legal person may be a private (i.e., business entity or non-governmental organisation) or public (i.e., government) organisation
Legal representative	The definition of a legal representative is based on local Member State legislations, therefore the requirements may differ regarding the required attributes, roles and responsibilities. Legal representative can be a natural person as well as a legal person
MRZ	Machine readable zone available on an identity document according with ICAO 9303





Natural person	A natural person is a person (in legal meaning. i.e., one who has its own legal personality) that is an individual human being.
OCR	Optical character recognition
PEP	Politically exposed person refers to the description of a natural person entrusted to a prominent public function which presents high risk of exposure to bribery and corruption crimes due to the position.
Person identification data	`person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established
SMS	Short message service

Annex I eIDAS ELEMENTS AND MAPPING

eIDAS Elements

Table 10 summarises the eIDAS key elements of the levels of assurance defined by the Implementing Regulation for electronic identification means (as per Regulation 2015/1502).

Table 10. eIDAS key elements overview³³

Elements	Description
 <p>2.1. Enrolment</p>	<p>The element 'Enrolment' includes the following sub elements:</p> <ul style="list-style-type: none"> 2.1.1 application and registration, 2.1.2 identity proofing and verification (natural person), 2.1.3 identity proofing and verification (legal person) and 2.1.4 binding between the electronic identification means of natural and legal persons
 <p>2.2 Electronic identification means management</p>	<p>The element 'Electronic identification means management' includes the following sub elements:</p> <ul style="list-style-type: none"> 2.2.1. electronic identification means characteristics and design, 2.2.2 issuance, delivery and activation, 2.2.3 suspension, revocation and reactivation and 2.2.4 renewal and replacement
 <p>2.3 Authentication</p>	<p>The element 'Authentication' means more specifically the authentication mechanism used to perform the electronic identification;</p> <ul style="list-style-type: none"> 2.3.1 Authentication mechanism
 <p>2.4 Management and organisation</p>	<p>The element 'Management and organisation' includes the following sub elements:</p> <ul style="list-style-type: none"> 2.4.1 general provisions, 2.4.2 published notices and user information, 2.4.3 information security management, 2.4.4 record keeping, 2.4.5 facilities and staff, 2.4.6 technical controls, 2.4.7 compliance and audit.

³³ Although authentication in eIDAS Article 3(5) defines the process enabling the electronic identification of natural and legal persons. The element authentication defined by 2.3 represents the authentication mechanism used and employed, and thus does not have an equivalent among the on-boarding steps.





Mapping of eIDAS to the on-boarding process

This section maps the eIDAS key elements to the on-boarding process steps and the eIDAS LoAs requirements.

Mapping of eIDAS elements and on-boarding process steps

Table 11 maps the eIDAS key elements to the on-boarding process steps.

Table 11. Map of on-boarding process steps to the eIDAS LoAs elements

Step	eIDAS element
Application 	2.1.1 Enrolment: Application and registration
Verification 	2.1.2 Enrolment: Identity proofing and verification (natural person) 2.1.3 Enrolment: Identity proofing and verification (legal person)
Collection 	2.4.4 Management & organisation: Record keeping
Management 	2.4.4 Management & organisation: Record keeping
Out of scope	The eIDAS elements which do not have an equivalent among the on-boarding process steps are out of scope: 2.1.4 Enrolment: Binding between the electronic identification means of natural and legal person 2.2 Electronic identification means management 2.3 Authentication 2.4.1 Management and organisation: General provisions 2.4.2 Management and organisation: Publisher notices and user information 2.4.3 Management and organisation: Information Security management 2.4.5 Management and organisation: Facilities and staff 2.4.6 Management and organisation: Technical controls 2.4.7 Management and organisation: Compliance and Audit

Mapping of on-boarding process steps to requirements that might be addressed by eIDAS LOAs

Table 12. Mapping of on-boarding process steps to requirements that might be addressed by eIDAS LOAs for natural persons

Natural Person	Requirements
Application	<ol style="list-style-type: none"> 1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the use of the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.
Verification - Authenticity check of document(s)	<p>High: Requirements of either point 1 or 2 have to be met:</p> <ol style="list-style-type: none"> 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:
Verification - Identity check of the applicant	<p>(a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;</p> <p>or (b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid;</p> <p>or (c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.</p>
Verification - Anti-fraud check	<p>OR</p> <ol style="list-style-type: none"> 2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied. <p>Substantial: Level low, plus one of the alternatives listed in points 1 to 4 has to be met:</p> <ol style="list-style-type: none"> 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application 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; <p>Low:</p>

Natural Person	Requirements
	<ol style="list-style-type: none"> 1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 3. 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.
Collection Management	<ol style="list-style-type: none"> 1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention. 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

Table 13. Mapping on-boarding process steps to requirements that might be addressed by eIDAS LOAs for legal persons

Legal Person	Requirements
Application	<ol style="list-style-type: none"> 1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the use of the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.
Verification - Authenticity check of document(s)	<p>High Level substantial, plus the requirements listed below have to be met: The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context</p>
Verification - Identity check of the applicant	<p>and the evidence is checked to determine that it is valid according to an authoritative source; Substantial</p>
Verification - Anti-fraud check	<p>Level low, plus the requirements listed below have to be met: The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number and the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector</p>

Legal Person	Requirements
	<p>and steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;</p> <p><u>Low</u></p> <ol style="list-style-type: none"> 1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made. 2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source. 3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.
Collection Management	<ol style="list-style-type: none"> 1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention. 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

Mapping of identity and KYC attributes to eIDAS SAML attributes profile

This is summarised in Table 14. For alignment with the ISA Core Vocabulary definitions the Core Person Vocabulary is used for the identity of a natural person; and the Core Business Vocabulary for identity of a legal person.

Table 14. Mapping of identity attributes to eIDAS SAML attributes

Identity attributes		eIDAS categorisation	
Area	Attributes	eIDAS SAML attributes model (recorded in ISA Core Person Vocabulary)	Mandatory/Optional/Other attribute
Identity	How financial institutions establish identity, including identification of the attributes they record e.g. family name, first name, date of birth, and ensure regular updates of the client data	Natural person: cbc:FamilyName cvb:GivenName cvb:BirthDate cva:Cvidentifier cva:BirthPlaceCvlocation cva:CitizenshipJurisdiction Legal person: cvb:LegalName cva:Cvidentifier	Mandatory Mandatory Mandatory Mandatory Optional Other Mandatory Mandatory
Address	Identify what attributes are recorded around residential address and country of origin	Natural person: cva:Cvaddress Legal person: cva:Cvaddress	Optional Optional
Source of Funds / Source of Wealth	Identify what attributes are collected e.g. occupation or details of a customer's business and the differences in attributes under enhanced levels of due diligence	Natural person: cva:CvbusinessCodeType Legal person: cva:CvbusinessCode	Other Optional

The minimum data set of attributes for cross-border representing a natural and legal person is according to CIR (EU) 2015/1501 Regulation on the interoperability framework pursuant to Article 12(8) of the eIDAS regulation, and mapped in Table 14 and Table 15. The minimum data set represents the mandatory attributes required to define the identity of a natural and legal person cross border. Extra optional attributes can also be added to the minimum data set. The minimum data sets are depicted in the tables below.

Table 15. Mapping the minimum data set for a natural person identity attributes following Regulation 2015/1501 to eIDAS SAML attributes

Attributes	Natural Person	
	Identity attributes	eIDAS SAML attributes
Mandatory	Current Family Name	cbc:FamilyName
	Current First Name	cvb:GivenName
	Date of Birth	cvb:BirthDate
	Unique identifier	cva:Cvidentifier
Optional	Current Address	cva:Cvaddress
	First Name at Birth	cvb:BirthName
	Family Name at Birth	cvb:BirthName
	Place of Birth	Cva:BirthPlaceCvlocation
	Gender	Cvb:GenderCode

Table 16. Mapping the minimum data set for a legal person identity attributes following Regulation 2015/1501 to eIDAS SAML attributes

Attributes	Legal Person	
	Identity attributes	eIDAS SAML attributes
Mandatory	Current Legal Name	cvb:LegalName
	Unique identifier	cva:Cvidentifier
Optional	Current address	cva:Cvaddress
	VAT registration number	Cva:CvbusinessCode
	Tax reference number	Cva:CvbusinessCode
	Central register, commercial register or companies register file number ³⁴	cva:CvbusinessCode
	Legal Entity Identifier (LEI)	cva:CvbusinessCode
	Economic Operator Registration and Identification (EORI)	cva:CvbusinessCode
	System for Exchange of Excise Data (SEED)	cva:CvbusinessCode
	Standard Industrial Classification (SIC)	cva:CvbusinessCode

³⁴ The identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:258:0011:0019:EN:PDF>

Annex II AML REQUIREMENTS

Examples in which electronic identification means are allowed in some of the surveyed Member States include:

- possession of a digital identity, of the highest security level (Italy);
- a digital identity or certificate for the creation of a digital signature issued under an electronic identification system included in the list published by the European Commission (Italy)³⁵;
- electronic signature and certificate (national ID card) (Estonia)³⁶;
- qualified certificate as defined by Directive 1999/93/EC (replaced by EU reg. 910/2014) (Belgium)³⁷.

Examples of the divergent cases of record keeping observed in surveyed Member States:

- In countries where video technology is used for on-boarding (e.g. Spain³⁸ and Luxembourg³⁹) it is required to store at least snapshots (i.e. screenshots) of the government issued documents presented during the video call, and the audio recording of the entire conversation. The quality of the snapshots should be sufficient to use them in investigations or analysis. The storage period is aligned with requirements employed for face-to-face on-boarding in this Member State. Estonian AML legislation⁴⁰ shows an approach to record keeping where for the identification purpose of a person, a query to a database is used. First, the database should be a part of the state information system and its use should be obligatory under the legislation in force. Second, the information about making the electronic query to the corresponding register should be possible to reproduce over the same period specified for storage of the originals or copies of the government issued documents.
- Additionally, Estonian AML legislation illustrates record keeping requirements if a person is identified based on digital identification, including the user's facial image and signature image. The AML law suggests that these attributes shall be kept in

³⁵ Article 19, Decree n 231/2007, available at: <http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2007-11-21;231!vig=>

³⁶ Requirements and procedure for identification of persons and verification of persons' identity with information technology means, available at:

<https://www.riigiteataja.ee/en/eli/504112016001/consolide>

³⁷ §1 and §2 The reglement approved by Royal Decree of 16 march 2010, available at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2010031606

³⁸ Authorization of remote identification procedures by videoconference ('Autorizacion de procedimientos de identificacion no presencial mediante videoconferencia'), available at: http://www.seplac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf

³⁹ CSSF Q&A: Identification/Verification of Identity through video chat, available at: http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080416.pdf

⁴⁰ Article 26, Money Laundering and Terrorist Financing Prevention Act, available at: <https://www.riigiteataja.ee/en/eli/523122013005/consolide>

a form that can be reproduced. The period of storage is in line with requirements to record keeping of the originals or copies of the government issued documents.

Extracts from the Directive (EU) 2015/849 ('4AMLD') and proposed amendments (5AMLD) in relation to eIDAS

Customer Due Diligence

Article 13.

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

[5AMLD proposed amendment: in Article 13(1), point (a) is replaced by the following: (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 or national law]

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

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

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, obliged entities may determine the extent of such measures on a risk-sensitive basis.

Article 14.

1. Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

Performance by third parties

Article 27.

1. Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1).
2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner.

[5AMLD proposed amendment: in Article 27, paragraph 2 is replaced by the following:

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides immediately, upon request, relevant copies of identification and verification data, including, where available, data obtained through electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 or national law, and other relevant documentation on the identity of the customer or the beneficial owner.]

Beneficial ownership information

Article 30.

1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter II. [..]
3. Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State, for example a commercial register, companies register as referred to in Article 3 of Directive 2009/101/EC of the European Parliament and of the Council (1), or a public register. Member States shall notify to the Commission the characteristics of those national mechanisms. The information on beneficial ownership contained in that database may be collected in accordance with national systems. [..]
5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:
 - (a) competent authorities and FIUs, without any restriction;
 - (b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;
 - (c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to

online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

Record-keeping

Article 40.

1. Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of *five years* after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of *five years* after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.

[5AMLD proposed amendment: in Article 40, paragraph 1 (a) points (a) and (b) are replaced by the following: [(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, including, where available, information obtained through electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 or national law, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction.]

Enhanced Due Diligence and high risk factors

Annex III. The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

- (2) Product, service, transaction or delivery channel risk factors:
- (a) private banking;
 - (b) products or transactions that might favour anonymity;
 - (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

[5AMLD proposed amendment: in point (2) of Annex III where a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3) is stated, point (c) is replaced by the following:

[(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means or relevant trust services as defined in Regulation (EU) 910/2014.]

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

[..]

Annex III CONSOLIDATED FINDINGS

The geographic spread and a split depending on size and business model of the 11 financial institutions interviewed is presented on the figure below.

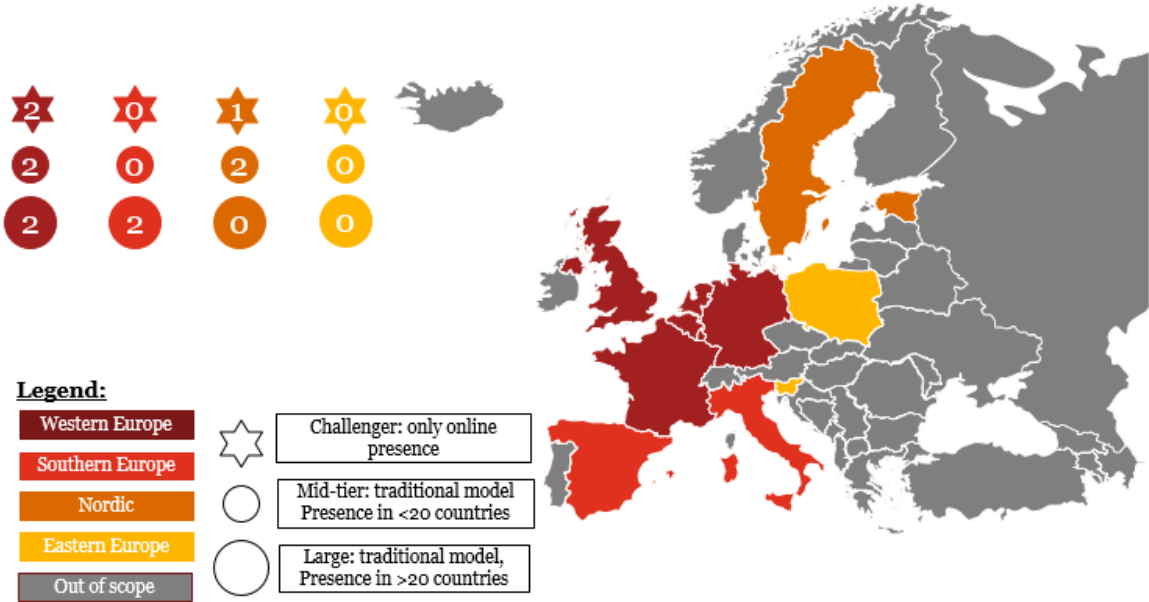


Figure 26. Geographic spread and division of financial institutions that participated in the study

The consolidated view of the identity and KYC attributes used by the different surveyed financial institutions for natural and legal persons are summarised in Table 17 and Table 18 respectively.

Table 17. Natural person attributes used by surveyed financial institutions

Natural Person Attributes	FI1	FI2	FI3	FI4	FI5	FI6	FI7	FI8	FI9	FI10	FI11
Family Name	3	3	3	3	3	3	3	3	3	3	3
First Name	3	3	3	3	3	3	3	3	3	3	3
Date of Birth	3	3	3	3	3	3	3	3	3	3	3
Unique Identifier	=	=	=	=	=	=	=	=	=	=	=
Current Address	3	3	3	7	3	3	3	3	3	=	=
Gender	3	3	7	3	7	3	3	3	3	7	=
Place of Birth	3	3	7	3	7	3	3	3	3	=	3

Country of Nationality	3	3	3	3	3	3	3	3	3	3	3
Family Name at Birth	7	7	7	7	7	7	7	7	7	=	3
First Name at Birth	7	7	7	7	7	7	7	7	7	=	3
Email	7	7	3	7	7	=	7	3	7	7	7
Country of Residence	3	3	3	3	3	3	3	3	3	3	3
Occupation	3	3	7	3	7	3	3	3	7	3	7
PEP	3	3	3	3	3	3	3	3	3	3	3
Source of Funds	3	3	3	3	3	3	3	3	3	3	3
Tax/Fiscal residence	7	7	7	7	7	7	7	7	7	7	7

Legend:

3: Attribute is used by financial institution

7 : Attribute is used by financial institution but not specified how it is collected and verified

= : Attribute is used by financial institution but not for non-residents

7 : Attribute is not used by financial institution

Table 18. Legal person attributes used by surveyed financial institutions

Legal Person Attributes	FI1	FI2	FI3	FI4	FI5	FI6	FI7	FI8	FI9	FI10	FI11
Current Legal Name	3	3	3	3	3		3	3	3	3	3
Unique Identifier (Directive 2012/17/EU)	3	3	3	3	3		3	3	3	3	=
Current Address	3	3	3	3	3		3	3	3	3	=
VAT Registration Number	7	3	7	3	7		7	7	3	=	3
TAX Reference Number	3	3	7	3	7		7	7	=	7	=
Legal Entity Identifier (LEI)	7	7	7	7	7		7	7	7	3	7
EORI	7	7	7	7	7		7	7	7	7	7

SEED	7	7	7	7	7		7	7	7	7	7
SIC	7	3	7	3	7		7	7	7	=	7
Country of Incorporation	3	3	3	3	7		7	3	3	3	3
Brand name	7	3	7	7	7		7	7	7	7	3
Email	7	7	3	7	7		7	7	7	7	7
Identification of Beneficial Owner	3	3	3	3	3		3	3	3	3	3
Source of funds	3	7	7	7	7		7	7	7	7	3

Legend:

3: Attribute is used by financial institution

= : Attribute is used by financial institution but not for a legal person from a different country

⊣ : Attribute is used by financial institution but not specified how it is collected and verified

7 : Attribute is not used by financial institution

⬜ : On-boarding is not available for a legal person by financial institution













⬜ : On-boarding of non-resident legal person is not available by financial institution

Annex IV COMMON AND DIVERGENT COMPLIANCE MEANS

Verification

The common and divergent verification mechanisms used for natural persons' identity attributes are summarised in Table 19.









Table 19. Natural person identity attributes verification mechanisms

 Natural Person Identity Attributes	Verification 			
	Common	Divergent		
Name 	Government issued document: <ul style="list-style-type: none"> • National Identity Card (NID) • Passport, travel document • Resident Card (for non-citizens) • Birth certificate (for minors) 	Government issued document: <ul style="list-style-type: none"> • Driving license Dependencies on third-parties: <ul style="list-style-type: none"> • Check with credit agencies • Lawyer/notary/embassy/police certification of an identity document (i.e. official copy of a document) • Post office certification (e.g. Post ID) • Tax database, National population register • National eID solutions (e.g. BankID) • Money wire from an EU bank account of the same customer Other: <ul style="list-style-type: none"> • (digital) copy of National Identity Card 		
Nationality 				
Date of Birth 				
Place of Birth 				
Unique Identifier 				
Name at Birth 				
Gender 			*Other: <ul style="list-style-type: none"> • Extracted from Unique Identifier^β 	
Address 			*Dependencies on third-parties: <ul style="list-style-type: none"> • Utility invoices • Tax declaration receipts 	
Occupation 			No common verification mechanism	Dependencies on third-parties: <ul style="list-style-type: none"> • Payslip • Credit agencies and Tax database checks
Email 			Verification email with one-time password and a confirmation link for online banking	Declarative by client with no further verification and confirmation

* Additionally used mechanisms to the ones listed for Name, Date of Birth, Place of Birth, Unique Identifier and Name at Birth.
^β For instance, a surveyed financial institution in Estonia mentioned that gender information is included into the Unique Identifier of the Estonian NID cards.






The common and divergent verification mechanisms used for legal persons' identity attributes are summarised in Table 20.

Table 20. Legal person identity attributes verification mechanisms

 Legal Person Identity Attributes	Verification 	
	Common	Divergent
Legal Name 	Government issued document: <ul style="list-style-type: none"> • Official registration document (e.g. certificate of incorporation, extract from a company register) • Articles of Association/ Incorporation, Legal Acts 	Government issued document: <ul style="list-style-type: none"> • Certified official registration document Dependencies on third-parties: <ul style="list-style-type: none"> • Check with credit agencies • Check with public databases (e.g. Company House) • Check with private databases • Business authorisation if the entity manages funds of third parties Other: <ul style="list-style-type: none"> • Official transaction code
Unique Identifier 		
VAT/TAX Ref. Nr. 		
Address 		
SIC 		
Country Incorporation 		

The common and divergent verification mechanisms used for natural persons' KYC attributes are summarised in Table 21.

Table 21. Natural person KYC attributes verification mechanisms




 Natural Person KYC Attributes	Verification 	
	Common	Divergent
PEP 	Screening via a PEP list	<i>No divergent verification mechanism</i>
Source of funds 	<i>No common processes[§]</i>	Dependencies from third-parties: <ul style="list-style-type: none"> • Payslip
Tax/Fiscal residence 	<i>No common processes[§]</i>	<i>No divergent verification mechanism</i>

§ No information provided by the surveyed financial institutions specifying the verification mechanism.

The common and divergent verification mechanisms used for legal persons' KYC attributes are summarised in Table 22.

Table 22. Legal person KYC attributes verification mechanisms















Legal Person KYC Attributes	Verification 	
	Common	Divergent
Beneficial Owner Identity	Beneficial owners (BO): <ul style="list-style-type: none"> Official registration document (e.g. Legal Acts, extract from the company register) Beneficial identity: <ul style="list-style-type: none"> Government issued document 	Beneficial owners (BO): <ul style="list-style-type: none"> Government issued certification Commercial register Beneficial identity: <ul style="list-style-type: none"> Copy of ID card/passport of BO Public register (or other reliable source, e.g. UBO register)
Source of funds 	<i>No common processes[§]</i>	<ul style="list-style-type: none"> Notary certification Proof from National authority Balance sheets Activity records Declarative
Brand name 	<i>No common processes[§]</i>	<ul style="list-style-type: none"> Articles of Incorporation (or an equivalent official registration document) Extract from the company register (or equivalent) Business authorisation if entity manages funds of third parties

§ No information provided by the surveyed financial institutions specifying the verification mechanism.

Collection

The common and divergent collection mechanisms used for a natural person are summarised in Table 23.









Table 23. Natural person identity attributes collection mechanisms

 Natural Person Identity Attributes	Collection 		
	Common	Divergent	
Name 	Copy of a government issued document ^x <ul style="list-style-type: none"> National Identity Card (NID) Passport, travel document Resident Card (for non-citizens) Birth certificate (for minors) 	Face-to-face: <ul style="list-style-type: none"> Official copy of a government issued document, created by a notary or other legal institution eID bank reader (at FIs office) Remotely: <ul style="list-style-type: none"> Digital copy of a government issued document, via High quality video call or Digital photo eID user software, e.g. BankID, Belgian eID Report from a credit agency Digital copy of an extract from a tax database, population register of a government issued document Post office proof of identity verification, e.g. PostID 	
Nationality 			
Date of Birth 			
Place of Birth 			
Unique Identifier 			
Name at Birth 			
Gender 			
Address 			*Face-to-face [‡] : <ul style="list-style-type: none"> Original or copy of a utility invoice Remotely [‡] : <ul style="list-style-type: none"> Digital copy of a utility invoice[‡]
Occupation 			Face-to-face [‡] : <ul style="list-style-type: none"> Original or copy of a payslip Remotely [‡] : <ul style="list-style-type: none"> Digital copy of a payslip or of an extract from the tax database
Email 			Only performed remotely by online based financial institutions [‡]

^{*} Additionally used mechanisms to the ones listed for Name, Date of Birth, Place of Birth, Unique Identifier and Name at Birth.
[‡] Declarative collection process possible.
^x For on-line based only financial institutions the collection is done at distance, otherwise the collection is Face-to-face.






The common and divergent mechanisms used for the collection of a legal person identity attributes are summarised in Table 24.

Table 24. Legal person identity attributes collection mechanisms

 Legal Person Identity Attributes	Collection 	
	Common	Divergent
Legal Name 	Copy of a government issued document: <ul style="list-style-type: none"> • Official registration document (e.g. certificate of incorporation) • Articles of Association/Incorporation 	Face-to-face: <ul style="list-style-type: none"> • Official copy of a government issued document, authenticated by a notary or other legal institution (for cross-border) • VAT/TAX reference derived from the Unique Identifier Remotely: <ul style="list-style-type: none"> • Digital copy of an extract of the company registry • Report from a credit agency
Unique Identifier 		
VAT/TAX Ref. Nr. 		
Address 		
SIC 		
Country Incorporation 		

The common and divergent collection mechanisms of the KYC attributes are depicted in Table 25 for a natural person and in Table 26 for a legal person.

Table 25. Natural person KYC attributes collection mechanisms

 Natural Person KYC Attributes	Collection 	
	Common	Divergent
PEP 	Based on results from PEP database ('PEP hits')	<i>No divergent collection process</i>
Source of funds 	<i>No common processes[§]</i>	Face-to-face [‡] : <ul style="list-style-type: none"> • An original or a copy of a payslip
Tax/Fiscal residence 	<i>No common processes[§]</i>	<i>No divergent collection process</i>

[§] No information provided by the surveyed financial institutions specifying the collection process
[‡] Declarative collection process possible.

Table 26. Legal person KYC attributes collection mechanisms



Legal Person KYC Attributes	Collection	
	Common	Divergent
Beneficial Owner Identity 	Face-to-face: <ul style="list-style-type: none"> Copy of official registration document for BO (e.g. Legal Acts, extract from the register) Copy of government issued document for BI 	Face-to-face[‡] Remotely: <ul style="list-style-type: none"> Digital copy of a document Extract from a public register
Source of funds 	<i>No common processes</i>	Face-to-face[‡]: <ul style="list-style-type: none"> Certification issued by a government body
Brand name 	<i>No common processes</i>	Face-to-face[‡]: <ul style="list-style-type: none"> Copy of Articles of Incorporation Copy of an extract of Companies Register Copy of an official registration document

[‡] Declarative collection process possible.

Annex V SAMPLE OF EMERGING DIGITAL SOLUTIONS

We have interviewed three solution providers ('SP') which are developing digital solutions that may replace the non-digital on-boarding processes in the (near) future. This could potentially facilitate the outsourcing of the on-boarding processes to (trusted) third parties and contribute to the portability of the customer identity data.

Table 27 below provides a summary of the information shared by the different solution providers during the interviews.

Table 27. Sample emerging digital solutions sample

Solution	Description
<p>SP 1</p>	<p>This solution is currently under development and will provide a mobile application, available only for a natural person on-boarding. The applicant (i.e. the prospective customer of the financial institution) will need to perform the following on-boarding steps:</p> <ul style="list-style-type: none"> • Verification: The applicant downloads the mobile application from the solution provider upon receiving an email from the financial institution. Initial verification of the applicant is performed using the email and via the mobile application by taking a picture of a government issued document (i.e. NID, passport) combined with the user's face (i.e. "a selfie"). The verification is completed by connecting to different third-parties such as a stolen passport database, PEP database, sanction lists, etc. The financial institution can decide to add and perform additional verification steps. • Collection: The verified information is automatically collected and stored in the mobile application's wallet and in a cloud-based environment. The collected information is encrypted. Sharing of the collected information with the financial institution requires the applicant's approval and consent. The data is collected based on a template profile created together with the financial institution. The information collected by the financial institution may vary, depending on different types of due diligence according to risk levels such as the residence of the applicant. • Management: The management (e.g. secure storage and maintenance) of the collected information is done by the solution provider. This results in the fact that users of the application are required to engage in the verification process only once and the collected information can be reused for future on-boarding processes. If the information is changed the financial institution is informed by the solution provider. <p>The solution is not aiming to be eIDAS compliant at the moment, however the solution provider is considering this option.</p>
<p>SP 2</p>	<p>This electronic identification solution is currently under development and is also aimed at natural persons. The applicant will need to perform the following on-boarding steps:</p> <ul style="list-style-type: none"> • Verification: The applicant should register with a valid email which is verified and confirmed with a one-time password. For remote identification, a personal device (i.e. computer or mobile phone) with an integrated camera is required. The camera is used to capture the special features of the government issued document. The solution aims to verify the visual document security elements such as an OVD, a hologram, a MRZ and printed information. In order to capture other information such as the applicant's address a commodity bill is considered. <p>In an initial release, the solution aims to perform the verification step using live interviews through high quality video technology. As part of a second release the video technology will be developed in-house. A third release will include authentication of already identified and verified customers.</p> <ul style="list-style-type: none"> • Collection: The solution aims to automatically collect identity attributes and visual security attributes from a government issued document together with the applicant's photo during the verification step. The financial institution defines which attributes must be collected. • Management: When registration and identification is completed the applicant will receive an electronic identity consisting of a digital certificate and a key pair which will be stored by the solution provider. <p>Furthermore, the solution provider is in the process of being certified by an eIDAS supervisory body, aiming to be recognised as an EU-wide Qualified Trust Service Provider delivering qualified digital certificates. Those certificates will contribute to the solution's trustworthiness. Obviously, as eID and Trust Services are inherently different, the qualification of the TSP has no immediate bearing on the eID solution.</p>

Solution	Description
SP 3	<p>This solution is provided as a mobile application and is only currently available for natural persons. The solution requires the presence of a built-in camera and RFID technology. The on-boarding process steps are as follows:</p> <ul style="list-style-type: none"> • Verification: The verification of a natural person is done by comparing the information from the electronic passport (which is securely read using RFID and the ICAO Active Authentication protocol*) and a picture (i.e. "selfie") of the applicant taken through the mobile device. This information is sent to the solution provider's system together with device information (e.g. IMEI) for verification. The device information is used as device fingerprint. To enable the use of the application, a one-time password is issued by the solution provider. • Collection: The mobile application securely captures the required identity attributes during the verification phase. The financial institution decides which exact identity attributes will be collected depending on the data available in the government issued document. This information, after successful verification, is signed by the solution provider and transmitted to the financial institution. Sensitive attributes such as biometrics are not typically required by financial institutions at the moment. • Management: The identity attributes collected are stored and managed by the financial institution. <p>Furthermore, the same solution provider also provides Trust Services, and claims to be already eIDAS compliant for electronic signatures.</p>
<p>*ICAO Active Authentication protocol enables an inspection system to verify the machine readable document chip authenticity by signing a challenge sent to the inspection system. (See ICAO Doc 9303)</p>	

During the report validation part, an additional service provider has presented an existing private eID solution. The main features of the solutions are described below.

Solution	Description
SP 4	<p>The solution is used locally in a Member State. It is provided in the form of an online Internet BankingID and is available for natural persons only. We refer to it for the purpose of this description as the Internet Banking ID (IBID).</p> <p>A user should first successfully complete on-boarding process at one of the partner local financial institutions (FI) in the Member State, become a customer and receive IBID internet banking access (i.e. login and a password).</p> <p>After that the customer is able to login in at the financial institution as well as at a number of service partner websites (e.g. insurance providers, tax authority, etc.) by using the IBID solution. It works as following:</p> <ul style="list-style-type: none"> - The customer selects the site of the service provider where (s)he wants to interact with; - (S)He checks whether IBID is support for authentication, and if so, selects this method; - (S)He then proceeds to log in, and will be authenticated by his financial institution, using IBID; this will include the use of an SMS with a security code for logging in; - (S)He is then redirected to the site he wants to visit, and will be authenticated there. <p>As the financial institution and the service provider typically use different identifiers, a linking of the identity authenticated by IBID to the identity used by the service provider needs to happen. For this purpose, at first login such a link is established, and the IBID identification is then replaced by a pseudonym. The pseudonym is derived from static data (user, IBID issuer, service provider) and is persistent. The service provider links the pseudonym to its internal identifier for the use. In subsequent logins, IBID will authenticate the pseudonym for the service provider.</p> <p>Moreover, a user can employ this solution as means for identification at the on-boarding in another local FI. However, it is a decision of the FI to accept the solution for an applicant identification or not.</p> <p>The solution has been assessed as 'Substantial' LoA as per eIDAS and is awaiting to be notified by the local authorities. At the moment the authorities are piloting this private sector's solution and also are initiating a market consultation about it.</p>

Summary of the standard ICAO PKI scheme for chip integrity through Passive Authentication

The following provides a brief summary of the ICAO PKI scheme:

- Passive Authentication (PA) consists of a two-layer certificate chain, enabling an inspection system to verify the authenticity and integrity of the data stored in the MRTD's chip.
- The root Certification Authority (CA) in this scheme is the Country Signing CA (CSCA), which authorizes Document Signers (DS) to sign the Document Security Object (SOD) on the chip.
- The CSCA certificate is distributed bilaterally by diplomatic exchange to relying States.
- DS certificate is published on the ICAO Public Key Directory (PKD) and/or stored on the MRTDs chip.
- Certificate Revocation Lists (CRLs) are published on the PKD and exchanged bilaterally.
- Passive Authentication (PA) consists of verifying the signature of the DS over the Document Security Object.
- For more information, please refer to ICAO⁴¹.

⁴¹ Available at: <https://www.icao.int/Security/>

Annex VII OPPORTUNITIES FOR THE FUTURE

The following ideas were raised by the participants of the validation workshop.

KYC portability

At the moment, regulations are different in different countries, there are various identification means and each bank has their own processes, requiring different KYC attributes, etc. Further harmonisation of the regulation is necessary to facilitate portability. Other possible enablers are i.e. a central European KYC utility or platform, managed by a supra-national authority, which would avoid unfair competition and unwillingness to cooperate. An instrument such as a charter which would clarify who remains liable for the correctness of the data could also foster the uptake of KYC portability, as well as the introduction of a unique global/EU identifier for each person. The KYC portability will reduce costs and make it more convenient for a customer to open a bank account. It is important to keep in mind to give the customer control of their data. This could possibly be solved by a fitting form of encryption (e.g. blockchain).

Cross-border opportunities and incentives

The use of eID for cross-border digital on-boarding could enable a single digital market, as geography doesn't matter anymore, with more players, more options for the customer and decreased costs related to administration for the financial sector. It could also reduce of the number of different authentication means and related costs. A similar process throughout Europe will lower the barrier and make it more convenient for customers opening a bank account in a new country. It is also an opportunity to raise security standards by requiring a substantial or high LoA, not only for banks but for all players in the market. eID could potentially bring trust and universality across both the public and private sector in the EU. With the common legal foundation set by regulations as the GDPR, the rules for sharing information are clearer, which offers possibilities. Banks can take up a role in facilitating eID understanding and digitisation. Examples are the project of Barclays and BankID, who promote the use of eID in their country but are also ambassadors of pan-EU digitisation. The use of eID facilitates SME digitisation and enables more funding for SMEs. The use of eID has the potential to bridge the gap in e.g. PEP identification and fraud prevention. eID will also be an enabler of the Internet of Things: in the near future, a customer will not only identify towards a physical person or a company but also towards a robot/machine (e.g. AirBnB: your eID as the key to your room)

eID is the future to create smooth, simple, and secure on-boarding, but right now we need Member States to create such schemes. eID will be used mainly within countries, not cross-border (there are only a limited set of use cases cross-border, e.g. Erasmus students, people moving to another country). Once an internal market is created, there is an opportunity to move forward (and outwards) from that. However, there are still uncertainties regarding the business model: it is currently free for citizens and public sector to use eIDAS nodes, but how expensive will it be for the private sector? How can we use the price element to push the creation of this market? The pricing element should be used to exploit eIDAS opportunities today to build a market for tomorrow.

KYC attributes

KYC attributes typically consist of ID attributes like name, first name, date and place of birth, etc. Additional attributes often are i.e. the tax address, jurisdiction or contact details. It is important to differentiate between the identity datasets themselves and the information which is used to verify information about oneself. Better portability of KYC attributes could be facilitated through the use of a centralised architecture. This would also fit in context of GDPR where the data subjects have more control over their data. Access to the data in the centralised structure can only be given by the data subject him/herself.

European Commission

Study on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU

Luxembourg, Publications Office of the European Union

2018 – 117 pages

ISBN 978-92-79-77867-4

doi:10.2759/94773



Publications Office

doi:10.2759/94773

ISBN 978-92-79-77867-4