



**The case for an attribute-based & LoA-rated KYC
framework for the digital age**

***ASSESSING PORTABLE
KYC/CDD SOLUTIONS
IN THE BANKING SECTOR***

December 2019

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

PDF format at:

<https://europa.eu/!GU86Qy>



scan QR code to download

Assessing portable KYC/CDD solutions in the banking sector:

The case for an attribute-based & LoA-rated KYC framework

for the digital age - *December 2019*

European Commission

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

European Commission

1049 Bruxelles/Brussel

Belgium

© European Union, 2019

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

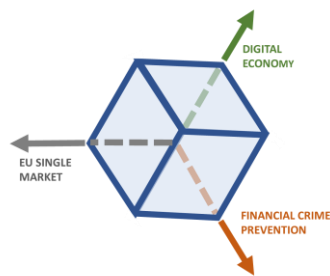
CREDITS

All images © European Union, except:

cover: © ipopba - stock.adobe.com

ASSESSING PORTABLE KYC/CDD SOLUTIONS IN THE BANKING SECTOR

THE CASE FOR AN ATTRIBUTE-BASED & LoA-RATED KYC FRAMEWORK FOR THE DIGITAL AGE



FOREWORD

This document presents ‘work in progress’ in relation to the subject matters and topics contemplated by Priority Group 2 and should therefore not be viewed as a complete and definitive proposal in respect thereof. We are aware that some of the matters presented in the Report are subject to ongoing discussions, and at times differing views amongst Expert Group members, and it is acknowledged that a number of matters require further investigations/clarifications. However, as the Expert Group mandate is now drawing to a close, we believe it can be presented to a wider audience in order to contribute to a debate on the ways and means of a robust and efficient CI/CDD attribute-based LoA-rated framework opening-up mutualisation opportunities and fostering a digital economy within EU member States.

As discussions are continuing on certain topics considered by the Report, we have moved to the Appendix a number of proposals in respect of which a consensus amongst members of the Expert Group was less likely to emerge or that need further work, hopefully leaving the main part of the document on a more stable footing.

We do nevertheless suggest that more discussions should take place on the following matters :

- Eligibility criteria for Trusted sources and RITPs;
- Connected individuals representing legal entities (or individuals) ;
- Deployment with IT and data standards.

We also suggest engaging with the eIDAS cooperation network, especially when it comes to clarifying the LoA attribute requirements for core identity attributes presented remotely, where a close alignment of solutions is needed to avoid regulatory arbitrage. In addition to the eIDAS cooperation network, we are also suggesting liaising with the Bits AS in Norway and BIS in Germany so as to capitalize on the important work undertaken by both institutions on the topic of secure digital verification of identity.

December 2019

Stéphane MOUY – Priority Group 2 Team Leader
Eric WAGNER – Priority Group 2 Rapporteur

This report has been prepared by the project team in the context of the work of the European Commission’s Expert Group on eID and remote KYC processes for the sole purpose of providing to the European Commission proposals for remote on-boarding processes in the banking sector, including the identification and assessment of the risks and how these can be mitigated as well as interoperability and overall functionality perspectives.

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

TABLE OF CONTENT

INTRODUCTION

- **FOREWORD**
- **EXECUTIVE SUMMARY**

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

PRIORITY GROUP 2 MANDATE

As per the Terms of Reference for two Sub-Groups of the Expert Group on Electronic Identification and Remote Know-Your-Customer Processes date July 20, 2018, Priority Group 2 was instructed to:

1. [Prepare] *an opinion on the need for, and the scope of, a framework for portable CI/CDD¹ solutions in particular in the banking sector. The opinion should consider key challenges/obstacles (e.g. liability framework) building on the eID interoperability framework with additional sets of attributes in order to enhance the usability of portable remote CI/CDD¹ solutions;*
2. *Assess the necessary minimum set of attributes necessary for CDD purposes in the banking sector and the appropriate level of assurance as per eIDAS (high, substantial and low) vis-à-vis various sets/types of attributes relevant for the CI/CDD¹ processes.*

The work undertaken by Priority Group 2 is also taking place within the wider mandate of the Expert Group as set out in Commission Decision of 14 December 2017, which was instructed to consider solutions that:

- are safe and secure;
- do not introduce new risks to public order, consumers or to the financial system;
- comply with Union data protection laws; and
- are in line with the Union anti-money laundering Directive (EU) 2015/849²

Priority Group 2 has therefore focused on the following three broad topics:

- **How CI and CDD attributes can meaningfully be related to defined Levels of Assurance ('LoAs') in general and eIDAS LoAs in particular;**
- **What benefits the introduction of an attribute-based LoA-rated framework can bring to the financial sector, as well as what challenges would be faced,** including that AML-CFT processes should not be weakened as a result;
- **How the transferability of KYC attributes could be implemented,** so that a relying party could safely make use of KYC attributes generated by third parties, including KYC utilities, as part of its own onboarding processes.

This implies that, in contrast to Report 1 primarily considering existing onboarding processes and therefore having a more descriptive outlook, Report 2 is prospective in nature, makes proposals and advocates a number of changes in the way KYC processes are implemented within the EU.

In this document:

- **'Report 1'** refers to the Priority Group 1 report and **'Report 2'** or **'the Report'** refers to this document;
- **'KYC'** refers to both **Customer Identification ('CI')**, i.e. the process of identifying the customer, and **Customer Due Diligence ('CDD')**, i.e. the process of determining the customer's status in relation to a number of factors, such as its politically-exposed person (PEP) status, source of funds, sanction list status, ultimate beneficial owner, etc;
- the Customer identification and due diligence framework proposals and recommendations outlined in Report 2 are referred to as the **'KYC Framework'** or the **'Proposal'** as the case may be;
- the EU Commission Expert Group on Electronic Identification and Remote Know-Your-Customer processes is referred to as the **'Expert Group'**.

The Report also noted that a number of regulatory developments are under way :

- the digital identity guidance currently under preparation by the Financial Action Task Force – **FATF**;
- The 5 December 2019 ECOFIN decision instructing the Commission, inter alia, to *'consider whether some AML/CFT aspects could be better addressed through a regulation and by exploring the opportunities and challenges in using technological innovation in combatting money laundering and countering the financing of terrorism.'*

These two developments are viewed as timely and meaningful contributions to the debate involving digital identities and the EU regulatory environment and Report 2 therefore attempts to integrate them into its developments.

1. The Terms of Reference refer to the 'KYC/CDD' term, but since KYC is often construed as including CDD, it has been replaced by 'CI/CDD' for consistency purposes
2. As confirmed by the EU Commission, the wording *'in line with Directive 2015/849'* is also to reflect more recent regulatory developments (including EU directives 2018/843 and 2018/1673 as well as those outlined above)

EXECUTIVE SUMMARY – 1/3

KEY MESSAGES

The Priority Group 2 acknowledges the multi-dimensional impact of KYC processes in the digital age and has been aiming at solutions that can bring improvements in three key directions:

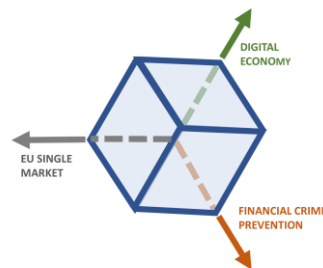
- enabling ‘full digital’ KYC processes with digital IDs and facilitating KYC-related services within the EU as well as financial inclusion (a ‘**Digital Economy**’ dimension);
- strengthening the existing ML/TF framework and adjusting it to digital/remote onboarding interaction (a ‘**Financial Crime Prevention**’ dimension);
- reducing the fragmentation of the EU KYC landscape and ensuring a level playing field for cross-border services eliminating regulatory arbitrage opportunities (a ‘**Single Market**’ dimension).

The three dimensions must not be viewed in isolation nor as intrinsically in conflict, as it is believed that progress can be achieved in all areas simultaneously.

The Report draws on the work of Report 1 showing a **high level of fragmentation of onboarding practices and sizeable differences in the way they are implemented within the EU financial sector**, a situation which can be attributed to two main factors: differences in approaches with regard to the deployment of digital ID solutions within national markets and significant discrepancies between national KYC requirements, with the latter factor now viewed as an inherent AML/CFT risk factor by EU regulatory authorities. In addition, these result in the partitioning of national banking markets and are preventing the development of competitive pan-European KYC services benefitting customers.

At the regulatory level, the Report identifies a **tension between on the one hand ‘single market’ elements** such as the banking passport, the single supervisory mechanism and the cross-border recognition of eIDAS digital identities **and on the other hand minimum harmonisation rules set out by the AML Directive** giving considerable discretion to member States for the practical deployment of KYC processes. This is a lesser concern when onboarding processes are primarily ‘on premises’ (face-to-face) as customers can only be approached by a limited pool of financial services providers but is problematic when remote onboarding becomes the norm – a situation facilitated by the deployment of readily available digital identity solutions – and is contributing to the fragmentation of the EU banking market along national borders. The Report takes the view that the tension generates regulatory arbitrage and weakens the overall effectiveness of EU AML/CFT processes.

COMMENTS/MORE INFO



The aim of the KYC Framework outlined in Report 2 is to achieve substantial progress in all three directions

[Go to page 9](#) for a **description of the current KYC landscape in Europe**
[Go to page 12](#) for a presentation of the **multi-dimensional impact of migrating from a document-based to an attribute-based environment** for KYC processes

[Go to Report 1](#) for a presentation of the **diversity of remote onboarding journeys and their reliance on ID documents presented remotely**
[Go to page 10](#) for an overview of the **current regulatory landscape and the implied risks for AML/CFT processes as considered by EU regulatory authorities**

[Go to pages 10 & 24](#) for the description of the interactions **between KYC and single market rules**

EXECUTIVE SUMMARY – 2/3

KEY MESSAGES

The Report recognises the critical role played by attributes in digital interactions and **recommends establishing a KYC framework primarily based on attributes, both for customer identification and customer due diligence matters, as a suitable approach for remote onboarding processes in the digital age.** This enables interactions that can either be document-based (i.e when attributes are remotely extracted from existing ID or CDD documents) or natively digital, where attributes are communicated through established IT protocols without supporting documents.

The Report focuses on the need to assess the reliability of KYC attributes and draws upon the recognition of eIDAS e-identity and trust services under 5AMLD as well as upon eIDAS Regulation setting Low, Substantial and High level requirements for different **‘assurance levels’ or ‘levels of assurance’**, and recommends extending the LoA notion to CI (non-eIDAS) as well as CDD and Contact attributes. However, care must be taken to ensure that the assessment methodologies are consistent for the same categories of attributes, hence the proposal to index the LoAs according to whether they related to CI or CDD matters.

The **linkage between attributes and LoAs** is either defined under or derived from the eIDAS Regulation for CI attributes or set out by reference to a number of factors for CDD attributes, with the most relevant being the status of the attribute source and the reliability of the communication channel used for the transfer of the attribute to the party relying on it. This means, for example, that a **High/ Substantial LoA will be assigned to an attribute that can be directly related to a ‘Trusted Source’/‘Recognised independent Third Party’** and is communicated to the intended recipient in a manner that cannot be easily compromised. If on the other hand the communication channel is susceptible to attacks or the document presented remotely can be edited, this will result in a lower LoA.

The Report also recognises **the importance of ensuring that the attributes used for KYC purposes are ‘reliable independent source data’** as required under the FATF Recommendation 10 and can be meaningfully used as part of a risk-based approach. This means that attributes reflect a situation that is current, but also implies that, when attributes are not directly communicated by the client, they are made available to obliged entities in a manner that ensures that they can be readily used and not just ‘confirmed’ by third party providers as tokens or hash messages.

COMMENTS/MORE INFO

[Go to page 16 & 17](#) for an overall presentation
[Go to page 22](#) for a presentation of the key core ID, Contact and Status/Good standing attributes
[Go to pages 17-18](#) for a presentation of the attributes remotely extracted from ID documents

[Go to pages 13 & 14](#) for an overall presentation of the **need to relate attributes to LoAs**

[Go to page 19](#) for a general **presentation of Trusted Sources and Recognized Independent Third Parties**

[Go to page 23](#) for a presentation of **refresh requirements for attributes**
[Go to page 24](#) for a presentation of **cross-border implications**

EXECUTIVE SUMMARY – 3/3

KEY MESSAGES

The Report outlines a **KYC framework presenting, for customary onboarding journeys, minimum attribute and LoA requirements for standard ML/TF risks** which makes room for the risk-based approach principle outlined by FATF and reflected in the AMLD. The Proposal focuses on current/payment account services but suggestions can be made for other customary onboarding journeys, including applying for loans and credit services as well as for savings or investment services. It does not attempt to address complex or specific customer relationships – large corporates and multinationals, institutionals and public sector entities as well as financial institutions are therefore out of scope of the KYC Framework.

Regulated entities using the KYC framework on an ‘as is’ basis must at all times be able to demonstrate that it can be applied to customer relationships not entailing higher ML/TF risks for them and, if that is the case, that the additional measures taken (such as requiring more attributes and/or higher attributes and/or more stringent refresh/reverify requirements) are commensurate with the higher risks involved. The Report recognises that the range of measures to be taken is highly context-specific and therefore refrains from taking a fully prescriptive approach to those risk-based situations, but offers a set of pre-defined additional attributes that can be used for such purpose on a risk-based basis. In addition, other measures (such as monitoring the behaviour of the customer or using other attributes) can also be used as well when relevant.

The Report also outlines an **outcome-based proposal for the management of KYC attributes clarifying what is expected of financial institutions using KYC attributes provided by third parties**. This is viewed as key for a proper assessment of liability implications when external CI/CDD verification providers are involved whilst maintaining the ultimate responsibility with the financial institution offering services to clients in accordance with FATF Recommendation 17. For such purpose, the Report identifies **four attribute-related tasks (Collect, Verify, Record & Process, Refresh)** serving as a basis for liability assessment and bringing visibility and predictability in this area, including critically for the **Verify task** assessing the trustworthiness of the attribute and which is LoA-dependent.

The deployment of KYC-related services by **KYC attribute custodians, i.e. banks and KYC utilities**, is facilitated by the task-related approach outlined above, bringing new opportunities for bank-based (decentralised) and KYC Utility-based (centralised) KYC services as well as significant cost reductions for the financial sector as a whole.

COMMENTS/MORE INFO

[Go to pages 25 to 27](#) for a presentation of the **KYC framework for individuals**
[Go to pages 28 & 29](#) for a presentation of the **KYC framework for legal entities**
[Go to Appendix](#) for a presentation of the **KYC framework for other services**

[Go to pages 32-36](#) for a discussion of the **risk-based approach**
[Go to page 33](#) for a presentation of the **FATF digital identity draft guidance**
[Go to page 35](#) for a presentation of **additional attributes for enhanced due diligence**

[Go to pages 38 & 39](#) for a presentation of the **key tasks to be performed by KYC relying parties**
[Go to page 40](#) for a presentation of the **implications for banking relationships**

[Go to page 41](#) for a presentation of the **centralised and decentralised KYC models**

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

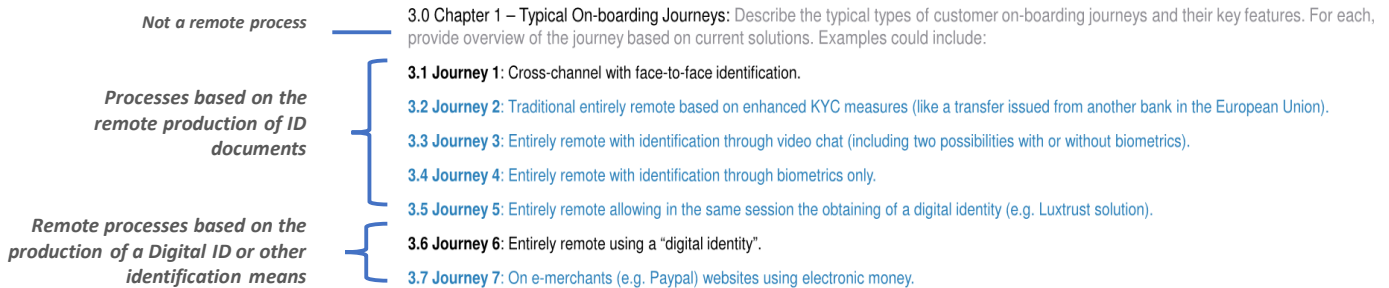
- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

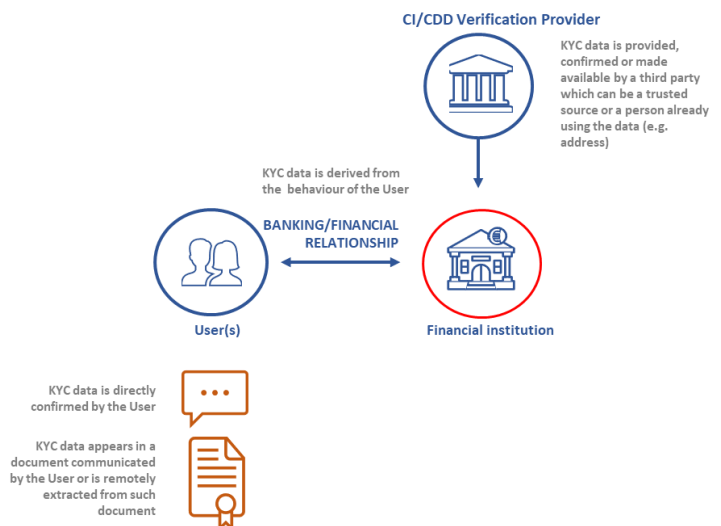
THE CONTEXT : REMOTE ONBOARDING PRACTICES ARE DIVERSE LEADING FINANCIAL INSTITUTIONS TO COLLECT KYC DATA THROUGH VARIOUS CHANNELS

- The work undertaken by Priority Group I confirms remote onboarding journeys are very diverse across the EU. In fact, only one of the contemplated remote onboarding journeys makes use of existing digital identities (with limited volumes compared to others)



- Financial institutions are ‘obliged entities’ subject to extensive KYC requirements that imply significant screening processes for new customers at the start of the business relationship, of which identity proofing is a key component (but not the only one) as well at the continuous monitoring of the transactions undertaken by customers once the relationship has been established, in accordance with the FATF guidelines. Indeed, Recommendation 10 of FATF requires inter alia FIs to :
 - Identify the customer using reliable, independent source documents (a topic now considered by the FATF draft digital identity guidance);
 - Understanding and obtaining information on the purpose and intended nature of the relationship;
 - Conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.
- We can see two important consequences deriving from this:
 - Financial institutions need to collect KYC data that extend far beyond the mere determination of the identity of the customer – although identifying the customer is of course a key component of the KYC process;
 - KYC data are collected in various ‘shapes and forms’, through three main delivery channels:
 - Information directly confirmed by the customer without supporting documents or external source confirmation (self-declaration);
 - Information provided by the customer with a supporting document or confirmed by a third party or trusted source;
 - Information derived from the behaviour of the customer, including the transactions implemented by him/her (for example account history).

- These three main channels have always existed, but the increasing availability of IT protocols facilitating data transfers as well as the development of publicly available databases (of which professional and social networks are the most obvious examples) imply a shift from customer-supplied/document-based to third-party confirmed information.
- That shift is ongoing but gradual - although real, it is subject to GDPR & data privacy as well organisational constraints limiting its development. It follows that financial institutions typically need to combine various sources of information in order to assess the AML/CFT risk profile of their customers as well as their eligibility to the financial services offered.



- We see this situation as likely to be maintained in the future, meaning that a KYC framework should accommodate and reflect the variety of channels and sources used by financial institutions to build the KYC profiles of clients.

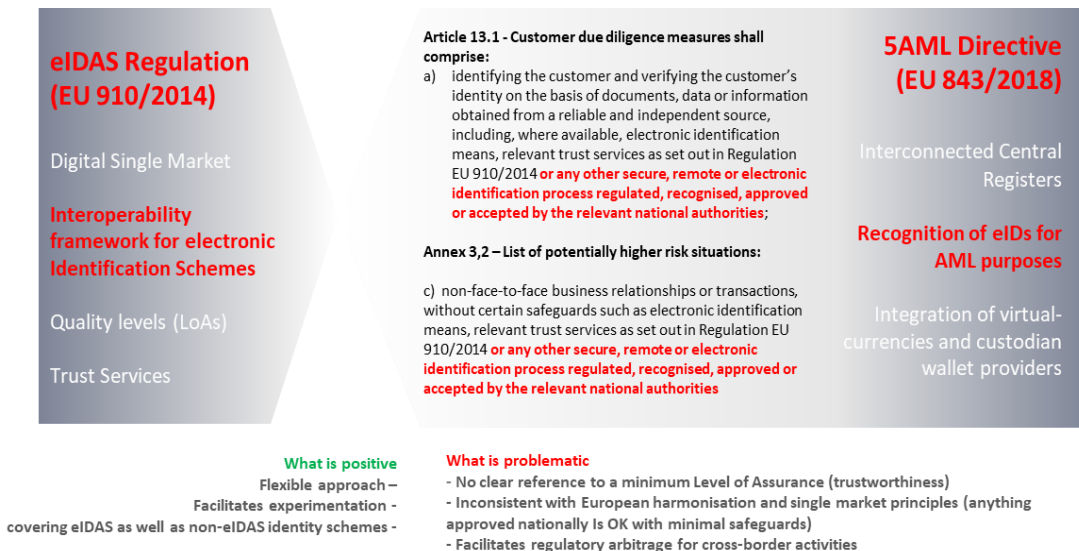
THE CONTEXT : A FRAGMENTED LANDSCAPE CREATING STRUCTURAL AML/CFT RISKS

- The Expert Group discussions as well as the work undertaken by Priority Group I confirm the fragmentation of remote onboarding practices across the EU, which can be attributed to a number of factors:
 - The **varying level of deployment of digital identity schemes** across EU member States, including for this matter eIDAS-notified schemes;
 - The **limited mutualisation of KYC processes for retail and corporate financial services**, which implies that each financial service provider has to deploy full-scale CI and CDD processes even when the necessary information can be made available from a third party in a secure and reliable format;
 - The **absence of a common regulatory approach for customer identification and due diligence processes when performed remotely**, meaning that each member State defines its own policies. This situation is increasingly acknowledged by European regulatory authorities as problematic as well as recognised as a key factor affecting the effectiveness of the European AML/CFT framework¹.
- In short, divergent national legal frameworks which are a direct consequence of the minimum harmonisation approach adopted by the EU AML directives are now recognised by the ESAs as a factor weakening the overall effectiveness of EU AML/CFT processes. This could be contained when financial services were mostly offered locally and ‘on-premises’ onboarding was the norm – meaning that financial services were not offered in a cross-border context - but becomes a critical weakness that needs addressing when remote onboarding is the new normal and consumers are routinely interacting with service providers located in different countries and subject to differing KYC regimes.
- In addition to weakening the overall AML/CFT framework, the fragmentation of KYC rules creates structural problems for the EU financial sector and brings no tangible benefits for customers:
 - KYC processes are unnecessarily replicated, with prospects and clients having to provide the same information each time they need a new service. This leads to a duplication of efforts, poor customer experience as well as higher costs for the financial sector;
 - The high cost of KYC processes and the prevalence of national barriers leads to fragmentation and prevents the deployment of a critical addressable market, a situation explaining at least in part why Europe is sidelined in the global tech race. See notably https://en.wikipedia.org/wiki/List_of_unicorn_startup_companies
- This approach appears to be in marked contrast with the one adopted for banking regulations and the deployment of financial services within the EU (or EEA) as well as the implementation of the Capital Markets Union which is a priority of the European Commission. It is also out of step with the eIDAS regulation offering a cross-border legal recognition of notified digital identities.
- Indeed, banking and financial services are in the EU covered by a banking passport set out in the single rulebook principle which is a foundational principle of the single market - Passporting enables firms that are authorised in any EU or EEA state to trade freely in any other with minimal additional authorisation.
- In this context, we believe that reconciling single market financial services with loosely coordinated or uncoordinated national KYC rules is highly problematic, and likely to be unstable in the long term, especially knowing that KYC rules are designed to ensure the integrity of financial transactions and prevent fraudulent activities. As KYC rules apply to services providers (obliged entities) and not directly to customers, it implies that customers are then able to select which KYC rules should apply to them, with an incentive given to providers based in jurisdictions with less demanding KYC requirements.

1. See for example the October 2019 edition of the *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union’s financial sector* in which the ESAs are ‘particularly concerned about ML/TF risks arising from legislative divergence in [...] four [AML/CFT] areas’. In the same vein, the September 2019 statement by the EBA Chairperson Jose Manuel Campa note that ‘divergence of national practices exposes the Union’s internal market to significant ML/TF risks’ and that ‘the current system of minimum harmonisation at national level needs to demonstrably deliver effective and comparable application of AML/CFT rules by competent authorities and consistent outcomes.’

THE CONTEXT : A FRAGMENTED LANDSCAPE PREVENTING THE DEPLOYMENT OF EU-BASED SOLUTIONS

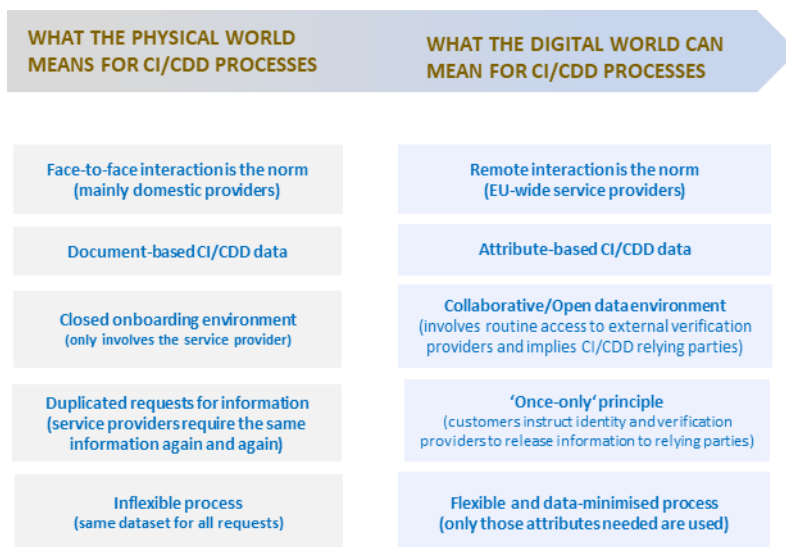
- An illustration of this trend can be seen in the treatment of digital identities within the EU AML/CFT framework. As is well known, 5AMLD recognises digital identities and confirms that remote onboarding implemented with a digital identity is not per se deemed to be higher risk - both very positive contributions. However, 5AMLD critically relies on national authorities for the treatment of digital IDs in onboarding processes within the financial sector, leaving considerable discretion to national authorities and ample room for divergence of national markets within Europe.



- The eIDAS Regulation ensures the recognition of digital identities that can be used across borders with full legal effect, but was designed to apply to public services offered to citizens, not to private sector services (B2B or B2C relationships). It incorporates the key notion of level of trustworthiness or assurance (LoAs) for digital identities but leave it to the service provider to determine which LoAs should be required. This is one of the major contribution of the eIDAS regulation but the fact that it does cover a far smaller spectrum of attributes than those needed by obliged entities and does not address status and/or good-standing aspects, which are critical for the financial sector, no doubt limits its use.
- As noted by the FATF in its draft digital identity guidance, implementing digital identities translated in ease of use for customers, combined with efficiency gains for regulated entities and can help lower on-boarding costs. *“One report¹ suggests that institutions using digital ID at high-levels of assurance could see up to 90 percent cost reduction in customer onboarding with the time taken for these interactions reduced from days or weeks to minutes. These cost savings could facilitate financial inclusion for otherwise excluded or under-served individuals by reducing onboarding costs. It can also help to redistribute savings towards other AML/CFT compliance functions.”*
1 - McKinsey Global Institute (2019) Digital Identification
- The fragmentation of KYC rules along national borders is also a major impediment to the development of KYC utilities and KYC services within Europe. The financial sector needs trusted identity and KYC attributes, is heavily investing and spending considerable amounts to implement KYC processes and, of all industries, is the most natural custodian of trust from customers. However, with a number of exceptions in Nordic countries, it has not been able to capitalize on these factors to offer efficient and robust KYC services in a mutualised way. This means that KYC processes are unnecessarily replicated across entities (and often, within entities, across business lines), with the same information requested again and again from customers. A key reason behind this situation is that, in spite of the size of the EU banking market, the addressable market for digital KYC services remains comparatively small and nationally defined, therefore limiting return on investment prospects for private sector firms and that liability implications have not been harmonised across EU member States.
- On the other hand, CI and CDD processes have historically been designed for face to face/same location interactions, but this assumption is proving increasingly ill-suited for the digital age. Indeed, digital interactions imply that the service provider and the prospect/client are based in different locations, if not countries. A number of key implications derive from this factual situation:
 - Remote onboarding and non-face-to-face interactions are the norm, not the exception;
 - With KYC rules applying to obliged entities, i.e. providers of financial (and other) services, not consumers, there is no compelling reason to have different KYC rules for domestic service providers in a given EU country and for service providers based in other EU countries but offering cross-border services to the same customers with a European banking passport under the freedom to provide services (which is what happens today).

CI/CDD IN THE DIGITAL AGE : FROM A DOCUMENT-BASED TO AN ATTRIBUTE-BASED ENVIRONMENT

- The graph below illustrates the change of paradigm resulting from the mass-market availability of remote onboarding processes, which is facilitated by the availability of digital identities recognised on a cross-border basis.



- CI & CDD processes are currently costly and cumbersome – a major pain point for customers and financial institutions alike and are ill-suited to deal with remote onboarding processes. The same information is requested again and again in order to access services and usually cannot be reused for future interactions. In addition, there is only very limited recognition of external Trusted sources of information. Lastly, the availability on the same consumer market of service providers subject to differing CI/CDD rules opens up regulatory arbitrage opportunities weakening the overall EU regulatory AML/CFT framework.
- Attributes need to be considered irrespective of the channel used for their delivery to the service provider. This implies that documents will continue to be used for onboarding processes and will coexist with digital identities and other data sharing protocols relating KYC stakeholders for the foreseeable future. This highlights the need to cover both in a neutral way.
- **There is therefore a need for an EU-wide CI/CDD standard :**
 - **applying to all financial services providers, therefore ensuring a level-playing field;**
 - **Based on attributes**, not documents, so that ID documents and digital identities are treated in a consistent basis;
 - **Structured around recognized Levels of Assurance (LoAs)** (Low, Substantial & High), so that clarity and visibility is given on the reliability and trustworthiness of the attributes so communicated. In line with the mandate of Priority Group 2, we suggest that LoAs be as closely related to eIDAS LoAs as possible for CI attributes.

- In order to foster an open data environment, the standard must facilitate a collaborative approach amongst key stakeholders involved in managing CI and CDD attributes, including national governments, public utilities, KYC utilities and digital safe service providers. It must also facilitate the use of leading open IT protocols and not require complex IT specifications – a simpler approach reusing existing IT standards is therefore preferable.

Why are standards important?

In general, technical standards contain a set of specifications and procedures with respect to the operation, maintenance, and reliability of materials, products, methods, and services used by individuals or organizations.

Standards ensure the implementation of universally understood protocols necessary for operation, compatibility, and interoperability, which are in turn necessary for product development and adoption. **While the adoption of standards has a positive impact in market penetration and international trade, a lack of standards creates issues for the effectiveness and robustness of an identity system, including problems with interoperability, interconnectivity and vendor lock-in.**

As electronic IDs have begun to replace paper-based systems, the technologies, inter-device communication and security requirements underpinning identity systems have become more complex—increasing the importance of standards for identity management. However, choosing between standards is challenging due to rapid technological innovation and disruption, product diversification, changing interoperability and interconnectivity requirements, and the need to continuously improve the implementation of standards.

ID4D – World Bank : **Technical standards for digital identity** (2018)

CI/CDD IN THE DIGITAL AGE : LINKING ATTRIBUTES AND LoAs TO SPECIFIC ONBOARDING JOURNEYS

- eIDAS-notified digital identity schemes are LoA-rated, meaning that they are meeting established reliability and trustworthiness standards (as further described in Commission Implementation Regulation 1502/2015). This is the world standard for the international recognition of digital identities, which should be preserved and enhanced. However, the eIDAS regulation was not designed to be used for the private sector or indeed financial sector, meaning that there is currently no EU guidelines as to which LoA should be recognized for onboarding in the financial sector when using eIDAS-notified digital identities. In addition, CDD processes go well beyond the mere identification of prospects, but aim to establish their due diligence profiles in line with applicable anti-money laundering and terrorism financing as well as tax avoidance requirements. This leaves every member State to define its own approach, which applies to all service providers acting from its territory, including when providing cross-border services.

Table 1 - Summary description of the customer due diligence checks in retail banking

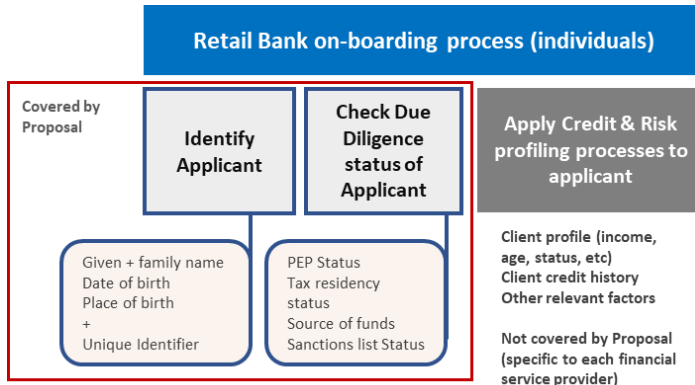
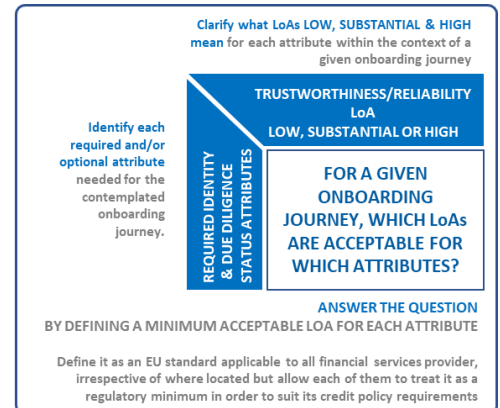


Table 2 – Summary presentation of the decision-making process linking key Identity or CDD attributes to LoAs. Attributes are LoA-rated and for a given onboarding journey, a minimum LoA for each attribute is required



- We also recognize that customer due diligence go beyond the mere identification of a prospect. Indeed, there are a number of additional checks which need to be performed for risk, anti-fraud and suitability purposes, including politically exposed person status, source of funds, tax residence, sanction list status (for individuals and legal entities) as well as ultimate beneficial owner (for legal entities).
- This implies that in the financial sector, especially for retail services, KYC and CDD processes can be broadly divided into three main categories (see Table 1):
 - **Customer identification processes** – the requirement is to identify the prospect with a sufficient degree of assurance and a close alignment with existing eIDAS rules is highly desirable, if not required;
 - **Customer due diligence processes** – the requirement is to assess the due diligence profile of the customer, a topic where a common standard are needed to facilitate an open data environment as well as limit regulatory arbitrage opportunities, but where current eIDAS rules are less relevant;
 - **Credit and risk profiling processes**, which tend to be specific to each financial institution and are often related to its business profile and risk appetite, and are viewed as beyond the scope of the Proposal.
- It is believed that a consistent approach can be used for both the CI and CDD sides of the onboarding process in the financial sector, which can be summarized in the following way:
 - Identify the key attributes required for CI or CDD processes in the financial sector ;
 - Clarify which minimum LoA is required.
- On the first aspect, work has already been done to identify the Due Diligence attributes beyond identity attributes, including notably in the ‘CEF EID BUILDING BLOCK FOR BANKING AND EDUCATIONAL DOMAINS - ARCHITECTURAL SOLUTION DOCUMENT (E-BANKING)’ as well as in the ‘STUDY ON EID AND DIGITAL ON-BOARDING’ PwC report released in 2018. We are proposing to use the key attributes so identified.
- It is recognised that the approach works best with standard use cases and is not to be applied in situations where ad-hoc investigations must be implemented. This will exclude from the scope of the Proposal the following categories of entities:
 - Large corporates/multinationals;
 - Institutionals and public entities;
 - Providers of financial services.

RATING CI & CDD ATTRIBUTES

- KYC processes broadly include **customer identification (CI)** and **customer due diligence (CDD)** processes. Both CI and CDD processes involve attributes which are collected by financial institutions in order to build and maintain KYC profiles for customers. As stated earlier, these attributes usually come from various sources and communication channels.
- As illustrated by Report 1, customer identification processes implemented by the financial sector make massive use of ID documents presented remotely, a situation for which there are no European guidelines or standards, and to a much lesser extent, eIDAS digital identities which are assigned specific levels of assurance set out in EU Regulation 2015/1502.
 - In light of the critical importance of ensuring a high level of trustworthiness for customer identification processes and in order to avoid structural differences in the way onboarding processes are implemented, therefore minimising regulatory arbitrage opportunities between eIDAS and non-eIDAS onboarding journeys, we are suggesting that non-eIDAS CI attributes be LoA-rated in a manner that is as consistent as possible with eIDAS LoAs. Pages 16 to 18 attempt to present a preliminary proposal in this respect.
- **Customer due diligence** processes are broader as they cover business relationship as well as service usage aspects and are continuing in nature but customer due diligence attributes are usually status-related, i.e. attest to the situation of an applicant with respect to a certain position or situation (politically exposed person, sanction list, country of tax residence, etc). They assume that the person has been identified in a satisfactory manner but do not, as such, give any indication as to whether this is the case. For example, establishing that a certain Mr X is a politically exposed person is a wholly distinct matter from establishing that Mr X is indeed the person initiating a relationship with the financial institution. In line with the mandate of Priority Group 2, we believe there are key merits in having CDD attributes LoA-rated, hence the fact that the Framework includes LoAs for CDD as well as contact attributes, but also take the view that LoAs should be aligned with the customary KYC practices of financial institutions and as simple as possible to understand. We note in this respect that the trustworthiness of CDD attributes is typically dependent on (i) the source of information confirming the status or position and (ii) the way the information is transferred to the service provider. However, and contrary to what happens for CI processes under eIDAS, there are no established levels of assurance currently available for Customer Due Diligence attributes.
 - We are suggesting that CDD attributes be LoA-rated but recommend adopting a simpler analytical framework specifically addressing the needs of the financial sector. Page 19 attempts to present a preliminary proposal in this respect.
- Although the mandate of Priority Group 2 is to use the Low, Substantial and High LoA definitions derived from the eIDAS framework, discussions within the Expert Group leading to the Report have stressed the need to ensure that the use of terminology is not misleading, especially when it comes to levels of assurance. In light of the fact that LoAs for CI attributes imply more factors, including critically for identity proofing purposes as well as different methodologies than those used for CDD attributes, we suggest using the same *Low*, *Substantial* and *High* LoA Terminology for CI and CDD attributes, but with an index confirming that they apply to different categories of attributes. This means that they appear as follows:

CI LoAs : _{CI}Low, _{CI}Substantial, _{CI}High
CDD LoAs : _{CDD}Low, _{CDD}Substantial, _{CDD}High

- In a wider context, the retrieval of information from submitted documents and external sources has to be made in a manner consistent with GDPR and e-privacy principles, an issue mostly falling beyond the scope of Report 2 and therefore not discussed in detail here. However, it may be worth mentioning here that :
 - KYC data are ‘personal data’ and therefore subject to GDPR and e-Privacy guidelines;
 - KYC data are either required by law applicable to the financial institution (including notably anti-money laundering laws and regulations), necessary for the performance of the service(s) offered by the financial institution or for the ‘purposes of a legitimate interest’ of the financial institution, and therefore do not usually require client consent as a basis for processing;
 - There are however three main areas where GDPR concerns must be considered and addressed:
 - When KYC data, once collected, is reused by the financial institution for a purpose other than KYC (notably marketing and profiling);
 - When KYC data is not maintained by the financial institution in accordance with GDPR guidelines; and
 - When biometric data are involved – a matter closely related to liveness detection processes for remotely presented ID documents and where consent is always required.

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

CI ATTRIBUTES : eIDAS AND NON-eIDAS PROCESSES

- The increasing deployment of digital identity schemes, especially eIDAS schemes, has and will continue to have a transformational impact on the European remote onboarding landscape but its use in the financial sector is subject to specific factors, such as the need of financial institutions to collect more attributes than those propagated by digital identity schemes as well as the availability of alternative onboarding methods, which are both well established (at times entrenched) and benefit from a steady flow of financial innovation.
- In light of this, it is believed that a significant proportion of remote onboarding journeys will in the foreseeable future continue to be based on the production of physical ID documents. This illustrates the need for a KYC framework covering all major remote onboarding processes, not just those using an existing digital identity as onboarding journeys based upon ID documents are likely to remain prevalent for years to come. A key reason is that physical ID documents are increasingly incorporating electronic functionalities designed to be used remotely and will in the future be required to comply with the minimum security standards set out by ICAO 93.03 (see European Parliament vote of 4 April 2019).
- It follows that, in view of the high substitutability of remote onboarding processes, any assessment of CI attributes ought to be made in a consistent way for those CI attributes propagated as part of eIDAS-notified identities as well as for those remotely extracted from ID documents as part of non-eIDAS onboarding processes. However the current situation in this respect is that :
 - CI attributes propagated as part of eIDAS-notified identities are assessed in a harmonised way defined by EU Regulation 2015/1502 (and related guidance);
 - CI attributes remotely extracted from ID documents (non-eIDAS processes) are assessed as part of KYC rules that are nationally defined and remain wholly uncoordinated at EU level.

The resulting gap is in our view problematic and can be exploited by bad actors, especially when banking passport rules (freedom of services) allow service providers to offer services to EU customers with Home country KYC regulations, with only limited recognition of the Host (consumer) country KYC rules.

- However, ID documents presented remotely may lead to a number of concerns :
 - Many existing ID documents are not designed to be presented remotely. They may contain useful physical security features but these often cannot be fully verified in a remote context – leaving remote presentation as a less secure alternative ;
 - the remote extraction of core ID attributes (e.g. name, first name, date & place of birth) from ID documents can be compromised if subject to attacks when unprotected and ;
 - last but certainly not least, an ID document has to be related to an individual, hence the need to verify that the person purporting to be the holder of the ID document is indeed the legitimate holder of the ID document – some visual or biometric inspection is needed which itself leads to a number of practical challenges and difficulties.
- We are aware that these matters are being currently considered by the eIDAS Cooperation Network updating the guidance for eIDAS LoAs, but work is not finalised and naturally focuses on eIDAS-notified digital identity schemes, not the remote presentation of ID documents generally. The current lack of a ‘common view’ on these practices is contributing to the fragmentation of the EU onboarding landscape for the financial sector and appears in clear need of harmonisation/standardisation. The Proposal goes some way towards that aim and makes use of the 2018 PwC Study on eID and digital onboarding, a report which contains a useful classification of ID documents which can serve as a basis for CI assessment
 - Type 1 ID documents : not machine readable not electronically readable documents
 - Type 2 ID documents : machine-readable documents (a category to which we suggest adding documents containing security features that can be used remotely)
 - Type 3 & 4 ID documents : electronically readable documents such as biometric passports (type 3 documents) and ‘logical documents’ not represented in physical format (type 4 documents). Note that Type 3 and Type 4 ID documents are deemed equivalent for CI & AML/CFT purposes pursuant to the PwC Study and correspond to the Substantial or High eIDAS LoAs. Type 4 documents which cover the necessary financial services attribute set have yet to emerge.

CI ATTRIBUTES (INDIVIDUALS) – LoAs FOR ATTRIBUTES REMOTELY EXTRACTED (1/2)

- Another dimension to be considered is the existence and increasing availability of non-eIDAS digital identity schemes (i.e. identity schemes not notified as part of the eIDAS framework) which are often promoted by private-sector entities, including GAFAs, are already widely used and may even become mainstream in the future.
- This results in three main alternatives for the remote communication of identity attributes :
 - use of an eIDAS ID;
 - use of another ID (non-eIDAS);
 - use of an ID document presented remotely.
- When core identity attributes are propagated as part of an eIDAS ID scheme, it is suggested that the relevant LoA be used without further adjustment or reconsideration – the eIDAS ID attributes are therefore fully accepted and the LoA rating not reassessed.
- Although considering other (non-eIDAS) IDs could be useful and bring benefits, we are not proposing to include these within the Proposal for two main reasons :
 - There are significant legal uncertainties involving the recognition of non-eIDAS digital identities, especially on a cross-border basis – this is one critical difference with eIDAS IDs which are given full legal recognition within the EEA;
 - At a practical level, assessing the features of non-eIDAS IDs along the Low, Substantial and High LoAs defined for eIDAS IDs should primarily be considered by the eIDAS Cooperation Network, which is better equipped to deal with these issues than the Expert Group.
- When core ID attributes are extracted from ID documents presented remotely – an extremely common situation today - we then have to deal with a number of issues:
 - Is the document a trusted document – Is it issued by a national authority ?
 - Can all necessary attributes be captured? If not, the process is very likely to fail.
 - Can it be reliably verified? This is an important aspect for ID documents that may not include all security features required for distance verification (which are in fact distinct from those applicable to face-to-face situations)
 - Is the person presenting it the legitimate holder of the ID document? The document may be confirmed as satisfactory, but has to be related to, and matched with, a physical person who is its legitimate holder.
 - Is the communication able to withstand moderate or high potential attacks?
- There is currently no commonly accepted way to treat this situation. The lack of standard in this field is a significant problem which needs addressing at EU level and we are proposing that a coordinated approach be defined to deal with ID documents presented remotely.
- The Proposal recognizes that two key dimensions stand out:
 - The **strength & quality of the attribute extraction process** from the presented ID document. This dimension primarily focuses on the ID document itself as well as the robustness and integrity of the method used to retrieve the ID information – the ‘document authentication’ dimension;
 - The **effective presence of the individual referred to in the ID document** – usually confirmed when his/her face corresponds to the ID document photo (but other biometric processes can also be contemplated) - the ‘Presence detection’ dimension.
- The Proposal therefore integrate and combine the two dimensions into a single LoA framework, where the two dimensions are treated equally and each is structured around three key levels of assurance (Low, Substantial and High) – see table 1.

CI ATTRIBUTES (INDIVIDUALS) – LoAs FOR ATTRIBUTES REMOTELY EXTRACTED (2/2)

- The document authentication dimension (table 1) sets forth a number of criteria which have to be met in order to meet the Low, Substantial or High LoA. These relate to the type of document and make use of the PwC Study on eID and digital onboarding (2018) classification of ID documents. Those criteria include basic and advanced checks, confirmation of the validity of the document as well as guidelines for the protection of the integrity of the attributes remotely captured. As a close consistency with the eIDAS requirements is needed, hence the need to coordinate efforts with the eIDAS Cooperation Network in this field.
- The presence detection dimension (Table 2) is focusing on the interaction with a human being who must be the legitimate holder of the ID document. It defines a requirement that an appropriate liveness detection process take place for the Substantial and High Levels with two major characteristics :

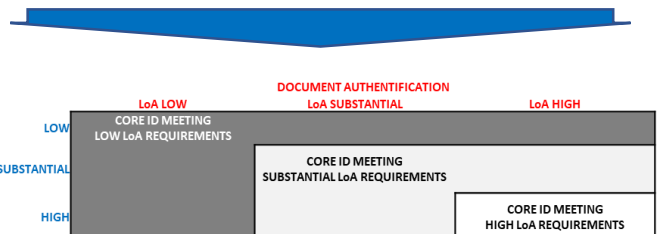
 - A minimum (Substantial LoA) and enhanced (High LoA) set of liveness detection criteria are to be defined (for example, challenge response selfie, use of colored flashlights or advanced 3D motion detection techniques could be considered here);
 - For the High LoA, we suggest benchmarking all proposed method against a maximum false acceptance score or other customarily accepted metrics.
- Certain requirements are defined in broad terms (e.g. ‘quality capture of ID photo’) or need to be further specified at a technical level (‘minimum/enhanced set of security features’, ‘maximum false-acceptance score’).
- Further discussions are needed, leading to possible additional adjustments of Tables 1 and 2, to ensure a consistent approach with the solutions arrived at for eIDAS digital identities, so that arbitrage opportunities are reduced to a minimum.
- Significant work has already been done in this respect, notably by Bits AS in Norway or BIS in Germany, leading to the recommendation that these be considered as a matter of priority.
- A proposal would be to instruct the EBA and/or eIDAS Cooperation Network to define appropriate guidelines for remote onboarding in consultation with leading European IT security agencies so that eIDAS-equivalent LoAs can be assigned to CI attributes and can be applied to a variety of communication channels.

Table 1

DOCUMENT AUTHENTICATION REQUIREMENTS		
LoA LOW	LoA SUBSTANTIAL	LoA HIGH
Document type		
Type 1, Type 2 & Equivalent, type 3 or 4 ID documents	Type 2 & Equivalent, Type 3 or 4 ID documents	Type 3 or 4 ID documents
Basic document checks		
Document is an eligible ID document Document appears genuine No obvious data inconsistency ID document within validity period	same as for LoA Low	Same as for Low LoA
Advanced document checks		
N/A	Validation of security element of the ID document (MRZ data and/or Hologram)	Electronic validation of ID attributes (implying valid e-signature or seal of issuing authority)
Validity of document		
N/A	Verification of loss/stolen document database (when available)	Same as for Substantial LoA
Data capture & transmission		
Capture of all ID attributes (other than photo) N/A	Electronic extraction of all ID attributes (photo optional)	Electronic extraction of all ID attributes (including photo)
Transmission secure against 'basic' attack potential	Transmission secure against 'moderate' attack potential	Transmission secure against 'high' attack potential
Other authentication aspects		
N/A	Other criteria consistent with eIDAS requirements 2015/1502 for Substantial LoA (including guidance document)	Other criteria consistent with eIDAS requirements 2015/1502 for High LoA (including guidance document)

Table 2

PRESENCE DETECTION REQUIREMENTS		
LoA LOW	N/A	N/A
LoA SUBSTANTIAL	Selfie screenshot + Liveness detection method with minimum set of security features	Other criteria consistent with eIDAS requirements 2015/1502 for Substantial LoA (including guidance document)
LoA HIGH	Liveness detection method with enhanced set of security features and delivering a false acceptance score lower than the maximum approved level.	Other criteria consistent with eIDAS requirements 2015/1502 for High LoA (including guidance document)



CDD ATTRIBUTES : TRUSTED SOURCES & RECOGNISED INDEPENDENT THIRD PARTIES


- As mentioned earlier, CDD attributes are often directly confirmed or submitted by applicants but increasingly collected by financial institutions by accessing external sources of information that can attest to the veracity and trustworthiness of the information submitted. We expect this trend to increase in the coming years and welcome it as a positive open data development. Any attempt to assess LoAs of CDD attributes should therefore integrate and capture this trend.
- In light of the variety of sources and communication channels used for CDD data, we advocate a somewhat simpler approach than the one contemplated for CI attributes, which focuses on two key questions for KYC data not directly self-asserted by the customer :
 - When the data is supported by a document or confirmed by a third party, how trustworthy is the source of information ? and
 - Is the process used to communicate the data to the financial institution maintaining the authenticity and integrity of the relevant data?
- for CDD attributes such as tax residency, PEP status, source of funds, there is no single Trusted source but rather a variety of sources which can be used, which have to be defined for each attribute. We therefore propose to identify two main categories of verification providers for CDD attributes :
 - **Trusted sources**, which are deemed reliable for the attribute considered (for example, the social security authority will be the Trusted source for its social security numbers), and the data of which are eligible for a HIGH LoA rating. It is expected that most Trusted sources will be public institutions or government departments;
 - **Recognized Independent Third Parties (RITPs)**, which are third parties usually using the attribute for their own activities, but acting independently from the Trusted source as well as the claimant (for example, a hospital or medical practitioner could be a RITP for the social security number or a utility for the address attribute) and which data would be eligible for a Substantial LoA rating.
- If the information is not directly transmitted by the verification provider (Trusted source or RITP) to the financial institution, but is instead channeled via the applicant, we believe that it should be assigned a Lower LoA rating, unless there is a mechanism in place ensuring the protection of the integrity of the information submitted. Table 1 summarizes the contemplated approach for Trusted sources & RITPs and table 2 outlines the way the KYC Framework could work for the address attribute and illustrates it with a Protected document example (using a digital visible seal).

Table 1 CDD LoAs	DATA AUTHENTICITY & INTEGRITY			
	UNPROTECTED during extraction and communication phase			PROTECTED during extraction and communication phase
	Attribute directly received from the Trusted source without transiting via the Prospect	Attribute received via a RITP without transiting via the Prospect	Attribute received via the Prospect or any other third party	All communication channels (including when transmitted via the Prospect or any other third party)
DATA ORIGINATOR				
TRUSTED SOURCE	CDD SUBSTANTIAL	CDD LOW	CDD LOW	CDD HIGH
RECOGNISED INDEPENDENT THIRD PARTY – RITP	N/A	CDD LOW	CDD LOW	CDD SUBSTANTIAL
PROSPECT AND OTHER THIRD PARTIES	N/A	N/A	CDD LOW	CDD LOW

Example of LoAs for the Current address attribute

Important for tax purposes (key determinant of tax residency status)

- **Low** : presentation of unprotected document showing the address
- **Substantial** : the address is securely confirmed by a public utility (RITP) or appears in a **Protected document** issued by a RITP
- **High** : the address is securely confirmed by a local authority or official post office (Trusted source) or appears in a **Protected document** issued by a Trusted source



Example of Protected document

There are several ways to create a **Protected document** – such as having the document signed or sealed electronically (Advanced or Qualified eIDAS levels) so that changes made to the document can be readily identified.

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

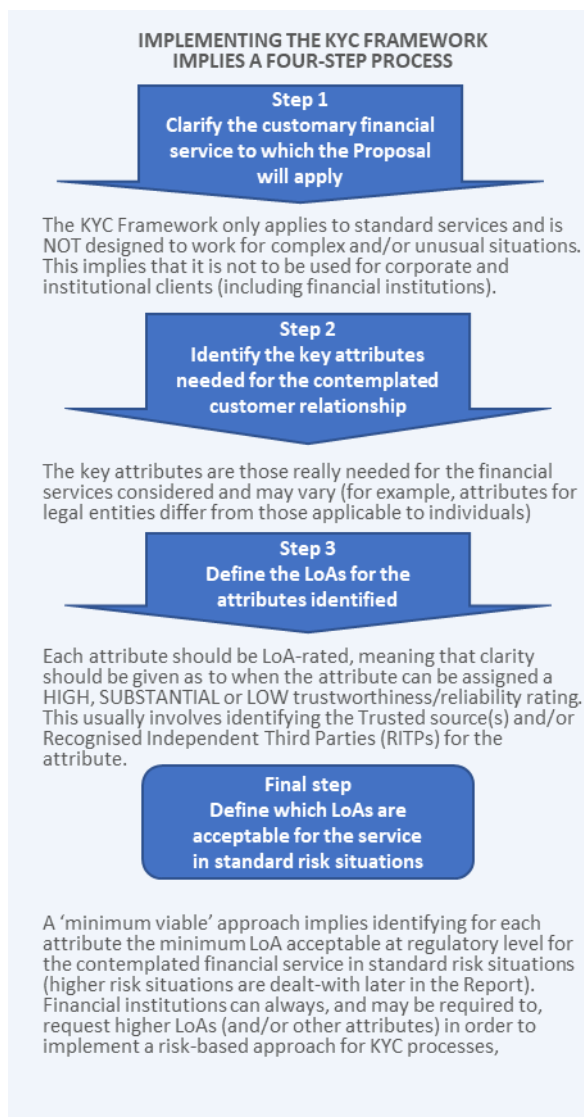
- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

A FRAMEWORK PROPOSAL FOR STANDARD RISK ONBOARDING JOURNEYS IN THE FINANCIAL SECTOR

- The Proposal is designed for remote onboarding journeys in the financial sector – i.e. when there is no face-to-face contact between the service provider and the consumer. It is based upon the key concepts of the eIDAS regulation – notably Attributes and Levels of Assurance - and is designed to work with and accommodate eIDAS-notified eID schemes.
- The Proposal is attribute-based, not document-based, but is consistent with the use of ID and other documents which will continue to be presented remotely for years to come.
- The Proposal advocates a standard for normal risks situations, which can be adjusted by regulatory authorities on a country (or even regional) basis, but recognises the critical importance of financial institution applying a risks-based approach for new client relationships based on customary factors (customer profile, country, industry, product & services, etc). Each financial institution therefore remains responsible for identifying higher risk situations, leading to additional attributes and/or higher LoAs and/or more stringent attribute refresh requirements being required.
- The Proposal applies to all financial service providers, irrespective of where located, and reduces regulatory arbitrage opportunities for KYC processes. This means that customers solicited by remote means, including by financial service providers marketing passported services, should be subject to the same KYC standard and have better opportunities to select financial services providers on their own merits.
- The Proposal is consistent with, and conducive to, an Open data environment by recognising the value of information directly obtained from external Verification Providers (notably Trusted sources and Recognised Independent Third Parties (RITPs) and assigning LoAs to such information. The Proposal is also meant to facilitate the interoperability of CI/CDD processes by facilitating interactions between CI/CDD providers and CI/CDD relying parties. This point is discussed further in the Part 3 Section.
- The attributes can be propagated from one participant to another by making use of existing IT protocols (for example OpenID Connect), opening up transferability and portability KYC opportunities in line with GDPR requirements. A standard use case is when a client has a KYC profile with a financial institution which is then instructed to transfer it to a third party in order to access new services, therefore illustrating one possibility of the ‘Once-only’ concept.
- As it is based on well-defined attributes and Levels of assurance, the Proposal offers greater clarity as to what is expected from financial services providers for CI and Customer due diligence processes, therefore offering a high quality EU standard for customary financial services. This also has positive implications for the assessment of liabilities and failures to comply.



WHICH ATTRIBUTES ARE TO BE CONSIDERED – STANDARD RISK SITUATIONS

- If the benefits of standardisation are to be achieved, it is important that a common set of attributes can be defined for customary onboarding journeys, especially with a cross-border dimension. However, the need to ensure a sound AML/CFT framework for financial services means that attributes must go beyond the simple identification of the person involved and give clarity on his/her position with respect to a number of issues (for example, the fact that he/she is a politically exposed person).
- For identity attributes, the reference is the Commission Implementation Regulation 2015/1501 which outlines the mandatory and optional attributes required for the eIDAS interoperability framework but we have also considered the ICAO standard 93.03 for travel documents (notably passports) in light of the fact that is the universal standard for the cross-border identification of individuals.

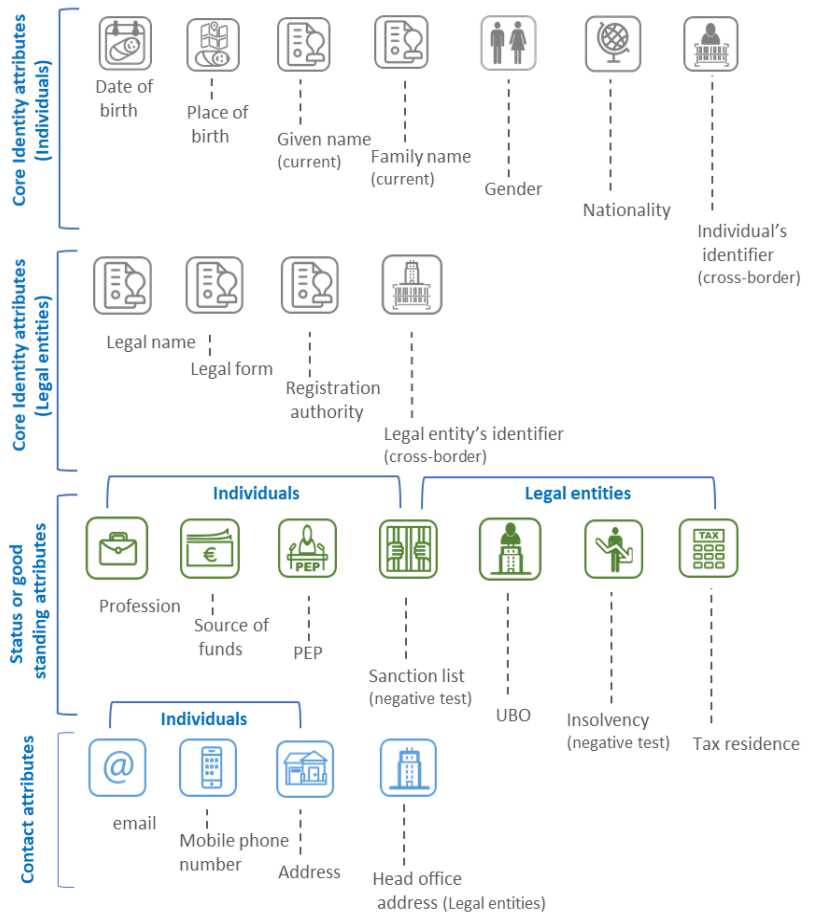
- For Customer Due diligence attributes, we have mainly looked at the eID Building block for banking and educational domains as well as the PwC Study on eID and digital on-boarding. However, the ‘No Sanction list’ attribute, assessing the non-appearance of the applicant’s name of key sanction lists, is new as it is viewed as necessary both for individuals and legal entities in order to achieve a sound AML/CFT framework.

- The attributes have been regrouped into three main categories.

➤ **Core identity attributes**: this is the set of attributes which, when combined, uniquely identify a person with an acceptable level of assurance. These are different for individuals and legal entities

➤ **Status (individuals) or good standing (legal entities) attributes**. These are attributes which are usually required for customer due diligence purposes and establish a customer service eligibility status.

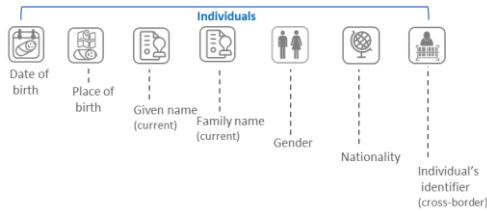
➤ **Contact attributes**. These are attributes that facilitate interactions with the person.



REVERIFYING ATTRIBUTES – HOW FREQUENTLY SHOULD THIS HAPPEN?

- A key factor ensuring the reliability and trustworthiness of the KYC Framework is that attributes reflect a situation that is current, not outdated, whilst recognising that certain attributes are inherently more stable than others, and therefore do not need to be reverified with the same frequency. In light of this fact, a gradual and risk-based approach is considered as appropriate.
- We propose, for standard risk situations, to categorise KYC attributes in three main groups with differentiated refresh requirements

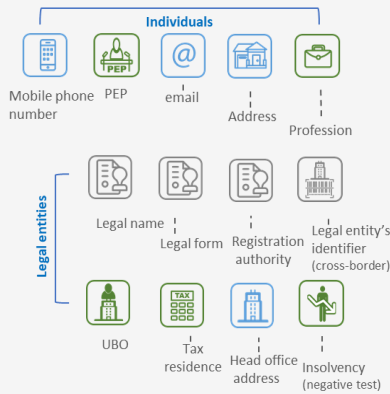
Permanent or very stable attributes



Permanent or very stable attributes do not need to be refreshed frequently. We suggest a minimum 10-year refresh frequency requirement, in line with the EU proposed requirement for Identity card – see Proposal for a Regulation strengthening the security of identity cards (April 2019).

The attribute is to be refreshed (i) when extracted from a document, certificate or token specifying an expiry date, before such date (ii) as may be needed, as part of the risk-based approach implemented by the financial institution in light of the then current circumstances of the business relationship

Variable attributes

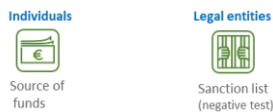


Variable attributes are attributes which are expected to change over a period of time, even though this may be infrequent. It is up to the financial institution to determine, for the considered relationship, the likelihood of change of the attributes.

Different approaches can be suggested for Variable attributes.

- One option is to require each financial institution to set its own refresh requirements as part of its risk-based approach for ML/FT processes, provided that they should always be more stringent than for Permanent or very stable attributes
- Another option is to define a common minimum refresh requirements as for Permanent attributes (5 years?). This could also allow national regulatory authorities to set more stringent refresh requirements – applying both to domestic services providers and EU services providers offering services on a cross-border basis.

Inherently unstable attributes

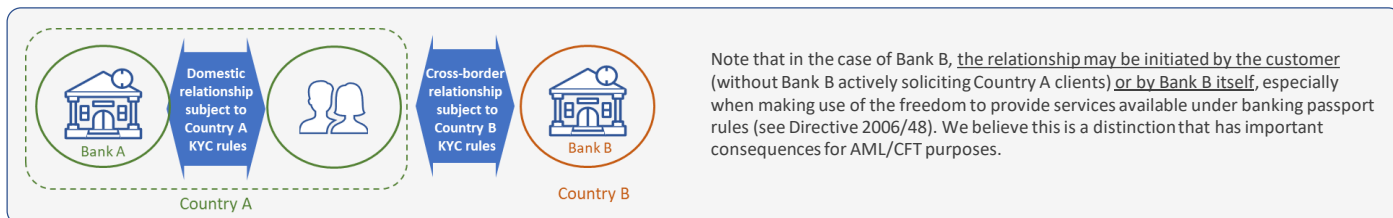


Inherently unstable attributes are attributes that cannot be assumed to be stable and have to be monitored on a permanent basis (or for each occurrence).

- The proposed categorisation of attributes for refresh purposes is designed to leave ample room for the meaningful implementation of a risk-based approach by financial institutions. However, whilst the Proposal does not advocate taking a prescriptive approach in this field, there could be merit in setting, for variable attributes, minimum common refresh requirements which could be combined with the implementation of a RBA by obliged entities. A number of alternatives are suggested which can be further discussed.

HOW SHOULD CROSS-BORDER SERVICES BE CONSIDERED

- A structural feature of AML/CFT rules is they apply to ‘obliged entities’, i.e. providers of financial (or other) services subject to the jurisdiction of regulatory entities, not directly to customers. The distinction has no impact in a domestic context – the KYC rules of the relevant country have to apply – but when the financial service provider is located in a country other than the country of residence of the customer, i.e. when a cross-border business relationship is involved, this leads to different KYC rules applying to the same customer depending on the country in which the service provider is located – see graph below.



- We view this as potentially problematic for two reasons : (i) it opens up regulatory arbitrage opportunities for bad actors (acting as consumers) and creates an uneven level playing field for service providers and (ii) it is out of step with consumer protection principles giving priority to the law of the country where the consumer has its habitual residence (see EU Regulation 593/2008).
- However, we recognise that this situation can be considered less important in situations where face to face (non-digital) interactions are common and for institutions for which the key markets are local. It nevertheless becomes an issue in environments where remote interactions are the norm – a situation clearly facilitated by digital identity schemes. For this reason, we see it as a matter needing increasingly attention in a single digital market context, especially for financial institutions making use of the freedom to provide cross-border services under banking passport rules.
- In relation to freedom to provide services, the banking passport rules set out in Directive 2006/48 give clear prominence to the ‘Home State’ (Country B in relation to Bank B) when it comes to defining the scope of the regulatory supervision of financial institutions, with the Host State (Country A in relation to Bank B) having more limited authority to take action, but nevertheless having access to information in a manner regulated by the EBA. We believe that this framework is a factor that mitigates the risks involved
- This leads us to suggest the following distinction:
 - When financial services are offered on a cross-border basis without the bank having obtained a banking passport, which is typically the case when the bank has not previously solicited the customer, the situation may be viewed as higher risk, especially when the purpose and intended nature of the business relationship seems unclear. In any event, a case by case analysis appears warranted;
 - When financial services are offered on a cross-border basis with the bank making use of the rules regarding freedom to provide services, i.e. when customers are responding to general solicitations made by the bank, there is no compelling reason to consider that, from an AML/CFT point of view, cross-border services will be inherently riskier than domestic financial services.

MINIMUM KYC FRAMEWORK FOR CURRENT/PAYMENT ACCOUNT OPENING – INDIVIDUALS

- The following table gives an overview of the KYC Framework for account opening purposes by an individual (payment/current account). As stated earlier, this applies in standard – not higher – risk situations. Note in this respect that:
 - the obliged entity bears the responsibility of determining whether the contemplated customer relationship implies normal or higher ML/TF risks based on all pertinent circumstances – the KYC Framework is not prescriptive in this respect;
 - In the event that the customer relationship implies higher risks, the obliged entity is responsible for taking all appropriate mitigating measures, such as inter alia requiring more attributes and/or higher LoAs and/or more stringent refresh requirements.

Table 1

INDIVIDUALS OR PROFESSIONALS - PAYMENT/CURRENT ACCOUNT OPENING		REQUIRED?	LEVEL OF ASSURANCE		
			c ₁ LOW	c ₂ SUBSTANTIAL	c ₃ HIGH
CORE ID	IDENTITY	Current family name			
		Current first name	REQUIRED		
		Date of birth		NOT ACCEPTED	ACCEPTED
		Place of birth			ACCEPTED
		Gender ¹			ACCEPTED
		Country of nationality	OPTIONAL		
	Individual's Identifier	Unique Identifier (eIDAS) or ID card number or Passport number	REQUIRED	NOT ACCEPTED	ACCEPTED
				ACCEPTED	ACCEPTED
	STATUS	NO SANCTION LISTS		NOT ACCEPTED	
		PEP STATUS		NOT ACCEPTED	
		TAX RESIDENCE	REQUIRED	ACCEPTED	ACCEPTED
		OCCUPATION		ACCEPTED EXCEPT WHEN ACTING AS PROFESSIONAL	ACCEPTED
	CONTACT	Current address			
		Mobile phone number	REQUIRED	NOT ACCEPTED	ACCEPTED
		email address			ACCEPTED

- Each attribute is defined as required or optional and the tables show for each attribute which LoA is acceptable for onboarding purposes.
- As can be expected, the HIGH LoA is always acceptable but achieving a HIGH LoA can be technically or operationally challenging - more so than what is required for a Low or Substantial LoA. Conversely, the LOW LoA is often deemed below the minimum acceptable reliability level, except for specific situations (e.g. the occupation attribute for a non-professional account). As illustrated by Report 1, the Substantial LoA is in line with the current practices of the financial sector in Europe and therefore viewed as acceptable.
- As stated earlier, the Framework could be adjusted by national regulatory authorities in order to reflect environment differences. Variations should be (i) justified by objective factors (ii) limited in scope and (iii) applicable both to domestic financial services providers and EU financial services providers offering cross-border services to customers located in the relevant country (especially when making use of the freedom to provide services available under EU banking passport rules)

The following pages give more indication as to how the LoAs of each attribute are determined.

1. We are aware that the **gender attribute** is subject to differing implementation practices in EU member States. We suggest using the solution outlined in the ICAO 93.03 standard for travel documents, itself reflected in EU Regulation 2019/1157 on ID documents. This means that the gender field can be populated by a **M**, **F** or **X** sign.

2. Note that the ‘Source of fund’ attribute is not listed here as we are considering normal risk situations and standard, not enhanced, CDD. In the event that, say, a substantial transfer or payment were to be made into the account, this should reveal a higher risk situation and trigger a source of funds query as part of the risk-based approach implemented by the financial institution.

OTHER ATTRIBUTES FOR INDIVIDUALS – LoAs FOR STATUS ATTRIBUTES

- The table gives an overview of the Status attributes required for account opening purposes (payment or current account) by an individual.
- As can be seen from the table, and in line with table 1 of page 19 :
 - ^{CDD}High LoA attributes are related to Trusted sources whereas ^{CDD}Substantial LoA attributes are related to RITPs;
 - ^{CDD}Low LoA attributes are also related to Trusted sources or RITPs but are evidenced by messages or documents which are not protected. Note however that financial institutions are expected to perform basic checks in relation to ^{CDD}Low LoA attributes, meaning that a *prima facie* verification check must not lead to any suspicion of an invalid or fraudulent message or document (for example, the document appears genuine, has not expired or the attributes shown in the document match those already available to the financial institution).
- It follows that the simple indication of an attribute by the customer, without any supporting document or message, will fail to attract a low LoA. The same result will occur when the attribute is supported by a document or message originating from or related to a third party that is not a Trusted source or RITPs.

		^{CDD} LOW	^{CDD} SUBSTANTIAL	^{CDD} HIGH	RELEVANT CONFIRMATION	ELIGIBLE RITPs	ELIGIBLE TRUSTED SOURCES
STATUS ATTRIBUTES	OCCUPATION		The Relevant Confirmation directly originates from a RITP and is protected during its extraction and communication to the recipient or directly originates from a Trusted Source but is not protected during its extraction and communication to the recipient	The Relevant Confirmation directly originates from a Trusted source and is protected during its extraction and communication to the recipient	Official occupation or profession	[DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY] [SOCIAL SECURITY AUTHORITY]	[EMPLOYER] [PROFESSIONAL BODY] [TAX AUTHORITY]
	PEP STATUS	The Relevant Confirmation appears to originate from a Trusted source or RITP but is not protected during its extraction and communication to the recipient			Official status	[THIRD PARTY PEP SERVICE PROVIDER] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[PUBLIC AUTHORITY ISSUING PEP LIST]
	SANCTION LISTS STATUS				Negative result for leading sanction lists	[SANCTION LISTS SERVICE PROVIDER] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[PUBLIC AUTHORITY ISSUING SANCTION LIST]
	TAX RESIDENCE				Tax residence	[BANK or FINANCIAL INSTITUTION] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[TAX AUTHORITY]

- The table identifies the RITPs and Trusted sources contemplated for the relevant attributes as well as the type of confirmation which is requested from them. Further work is needed to specify how these should be defined – hence the fact that they are currently presented in broad or generic terms only.
 - Trusted sources are expected to be recognised public authorities in most cases, and therefore could be identified as part of an EU-wide approved list.
 - RITPs are expected to be identified as recognised categories of entities or persons.
- Both Trusted sources and RITPs are defined for each attribute – the fact that a Trusted source/RITP is recognised for a given attribute gives no indication as to whether it should be accepted as such for other attributes.
- The type of confirmation expected for each attribute is also broadly defined and may have to be further adjusted to reflect the specifics of each attribute. We expect that in some cases the confirmation will consist in a message confirming one set of data, whereas in other instances the confirmation would result in the production of one or more documents.

OTHER ATTRIBUTES FOR INDIVIDUALS – LoAs FOR IDENTIFIER & CONTACT ATTRIBUTES

- The table gives an overview of the Identifier and Contact attributes required for opening purposes (payment or current account) by an individual. The type of confirmation expected for each attribute is also broadly defined and may have to be further adjusted to reflect the specifics of each attribute. We expect that in some cases the confirmation will consist in a message confirming one set of data, whereas in other instances the confirmation would result in the production of one or more documents.
- As can be seen from the tables below, and in line with table 1 of page 19 :
 - High LoA attributes are related to Trusted sources whereas Substantial LoA attributes are related to RITPs;
 - Low LoA attributes are also related to Trusted sources or RITPs but are evidenced by messages or documents which are not protected. Note however that financial institutions are expected to perform basic checks in relation to Low LoA attributes, meaning that a *prima facie* verification check must not lead to any suspicion of an invalid or fraudulent message or document (for example, the document appears genuine, has not expired or the attributes shown in the document match those already available to the financial institution).
- It follows that the simple indication of an attribute by the customer, without any supporting document or message, will fail to attract a low LoA. The same result will occur when the attribute is supported by a document or message originating from or related to a third party that is not a Trusted source or RITPs.
- The table identifies on a preliminary basis the RITPs and Trusted sources contemplated for the relevant attributes. Further work is needed to clarify how these should be defined. For example, Trusted sources can in some cases be readily identified for a number of attributes (sanction list, tax residence, etc) but may have to be generically defined for others.

		c_iLOW	c_iSUBSTANTIAL	c_iHIGH	RELEVANT CONFIRMATION	ELIGIBLE RITPs	ELIGIBLE Trusted sources
IDENTIFIER ATTRIBUTES	Unique Identifier (eIDAS)		The Relevant Confirmation is communicated as part of a	The Relevant Confirmation is	eIDAS Unique Identifier of the applicant	[BANK or FINANCIAL INSTITUTION] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[ISSUER OF eID]
	ID Card number	The Relevant Confirmation is communicated as part of a Low LoA eIDAS eID, or appears to originate from a RITP or Trusted source but fails to meet the	Substantial LoA Eidas eID, directly originates from a RITP and is protected during its extraction and communication to the recipient or directly originates from a Trusted Source but is not protected during its extraction and communication to the recipient	as part of a High LoA eIDAS eID or directly originates from a Trusted source and is protected during its extraction and communication to the recipient	ID Card	[BANK or FINANCIAL INSTITUTION] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[ISSUING STATE]
	Passport number	Substantial and High LoA requirements			Passport	[BANK or FINANCIAL INSTITUTION] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[ISSUING STATE]
	Existing Bank Account Code				applicant is the sole account holder and the Bank Account Code is:	[TAX AUTHORITY] [PUBLIC UTILITY] [BANK or FINANCIAL INSTITUTION other than the account bank] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[ACCOUNT BANK]

		c_oDLOW	c_oD SUBSTANTIAL	c_oD HIGH	RELEVANT CONFIRMATION	ELIGIBLE RITPs	ELIGIBLE Trusted sources
CONTACT ATTRIBUTES	Current Address	The Relevant Confirmation appears to originate from a Trusted source or RITP but is not protected during its extraction and communication to the recipient	The Relevant Confirmation directly originates from a RITP and is protected during its extraction and communication to the recipient or directly originates from a Trusted Source but is not protected during its extraction and communication to the recipient	The Relevant Confirmation originates from a Trusted source and is protected during its extraction and communication to the recipient	Address of the applicant	[PUBLIC UTILITY] [DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY]	[LOCAL AUTHORITY] [POSTAL SERVICE]
	Mobile Phone Number				Mobile phone number of the applicant	[DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY] [TELCO]	[CONSIDER WHETHER A Trusted source IS POSSIBLE]
	Email Address				Email address of the applicant	[DIGITAL SAFE SERVICES PROVIDER] [KYC UTILITY] [ISP]	[CONSIDER WHETHER A Trusted source IS POSSIBLE]

MINIMUM KYC FRAMEWORK FOR CURRENT/PAYMENT ACCOUNT OPENING – LEGAL ENTITIES

- The following table gives an overview of the KYC Framework for account opening purposes by a legal entity (payment/current account). As stated earlier, this applies in standard – not higher – risk situations. Note in this respect that:
 - the obliged entity bears the responsibility of determining whether the contemplated customer relationship implies normal or higher ML/TF risks based on all pertinent circumstances – the KYC Framework is not prescriptive in this respect
 - In the event that the customer relationship implies higher risks, the obliged entity is responsible for taking all appropriate mitigating measures, such as inter alia requiring more attributes and/or higher LoAs and/or more stringent refresh requirements.

LEGAL ENTITY / PAYMENT/CURRENT ACCOUNT OPENING		REQUIRED OR RISK-BASED?	LEVEL OF ASSURANCE			
			c _i LOW	c _i SUBSTANTIAL	c _i HIGH	
CORE ID	IDENTITY	Legal Name Legal form/structure Registration authority Registration number Main address (Head office)	REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED
	Company's Identifier	eIDAS Unique Identifier or Tax reference number or Legal Entity Identifier	REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED
			c _{DD} LOW	c _{DD} SUBSTANTIAL	c _{DD} HIGH	
GOOD STANDING		NO SANCTION LISTS	REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED
		NO BANKRUPTCY/INSOLVENCY	RISK-BASED			
			c _{DD} LOW	c _{DD} SUBSTANTIAL	c _{DD} HIGH	
CONNECTED INDIVIDUALS	ULTIMATE BENEFICIAL OWNER		REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED
	INDIVIDUAL ACTING ON BEHALF OF LEGAL ENTITY	Legal representative Director Empowered Employee Empowered third party Ad-hoc attorney	One position category REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED
	INDIVIDUAL'S IDENTITY ATTRIBUTES	First Name, Name, Date & Place of Birth	REQUIRED	NOT ACCEPTED	ACCEPTED	ACCEPTED

- Legal identity attributes are grouped into three main categories, Core ID, Good Standing and Connected Individual
- As for individuals, the Framework could be adjusted by national regulatory authorities in order to reflect environment differences. Variations should be (i) justified by objective factors (ii) limited in scope and (iii) applicable both to domestic financial services providers and EU financial services providers offering cross-border services to customers located in the relevant country (especially when making use of the freedom to provide services available under EU banking passport rules)
- Core ID attributes include the identity attributes viewed as necessary for a proper identification of the entity and derived from eIDAS implementation regulation 2015/1501. We also provide for a Company's identifier, leaving a variety of options for its determination.
- Good standing attributes refer to two main confirmations : the absence of any official sanction affecting the company as well as of any bankruptcy/insolvency proceedings affecting the company; These two tests are fairly straightforward and usually complied with by accessing public databases.
- Connected individuals attributes refer to two distinct situations where individuals are 'linked' to a legal entity. The first one is the UBO – Ultimate Beneficial Owner where an individual has ultimate corporate control over the legal entity and the second one refers to the fact that legal entities are in fact managed by individuals who need to be identified as well for day to day financial services. Note that there are two aspects to be considered here :
 - The identification of the individual acting on behalf of the legal entity;
 - The linkage between the individual and the legal entity (i.e. the position and status of the individual vis a vis the entity)
- As is the case for individuals and for the same reasons, the High and Substantial LoAs are accepted without restriction.

ID & GOOD STANDING ATTRIBUTES FOR LEGAL ENTITIES

- The table gives an overview of the Core ID and Good standing attributes required for opening purposes (payment or current account) by a legal entity.
- As can be seen from the table, and in line with table 1 of page 19 :
 - High LoA attributes are related to Trusted sources whereas Substantial LoA attributes are related to RITPs;
 - Low LoA attributes are also related to Trusted sources or RITPs but are evidenced by messages or documents which are not protected. Note however that financial institutions are expected to perform basic checks in relation to Low LoA attributes, meaning that a *prima facie* verification check must not lead to any suspicion of an invalid or fraudulent message or document (for example, the document appears genuine, has not expired or the attributes shown in the document match those already available to the financial institution).
- The table identifies on a preliminary basis the RITPs and Trusted sources contemplated for the relevant attributes. Further work is needed to clarify how these should be defined. For example, Trusted sources can in some cases be readily identified for a number of attributes (sanction list, tax residence, etc) but may have to be generically defined for others.
- The type of confirmation expected for each attribute is also broadly defined and may have to be further adjusted to reflect the specifics of each attribute. We expect that in some cases the confirmation will consist in a message confirming one set of data, whereas in other instances the confirmation would result in the production of one or more documents.

		ciLOW	ciSUBSTANTIAL	ciHIGH	RELEVANT CONFIRMATION	ELIGIBLE RITPs	ELIGIBLE TRUSTED SOURCES
CORE ID	Company's Identity Legal Name Legal form Registration authority Registration number Main address (Head office)	The Relevant Confirmation is communicated as part of a Low LoA eIDAS eID, or appears to originate from a RITP or Trusted source but fails to meet the Substantial and High LoA requirements	The Relevant Confirmation is communicated as part of a Substantial LoA Eidas eID, directly originates from a RITP and is protected during its extraction and communication to the recipient or directly originates from a Trusted Source but is not protected during its extraction and communication to the recipient	The Relevant Confirmation is communicated as part of a High LoA eIDAS eID or directly originates from a Trusted source and is protected during its extraction and communication to the recipient	[BUSINESS REGISTRATION]	[BANK or FINANCIAL INSTITUTION] [TAX AUTHORITY] [KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	[BUSINESS REGISTRATION AUTHORITY]
	Company's Identifier eIDAS Unique Identifier or Tax reference number or Legal entity Identifier				[TAX DOCUMENT] [BUSINESS REGISTRATION]	[BANK or FINANCIAL INSTITUTION] [KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	[ISSUER OF eID] [TAX AUTHORITY] [ISSUER OF LEGAL ENTITY IDENTIFIER]
GOOD STANDING	NO SANCTION LISTS	The Relevant Confirmation appears to originate from a Trusted source or RITP but is not protected during its extraction and communication to the recipient	The Relevant Confirmation originates from a RITP and is protected during its extraction and communication to the recipient	The Relevant Confirmation originates from a Trusted source and is protected during its extraction and communication to the recipient	'Fail' confirmation of a search of Legal entity, UBO or key executive on leading Sanction Lists	[SANCTION LIST SERVICE PROVIDER] [KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	[SANCTION LIST ISSUER]
	NO BANKRUPTCY/INSOLVENCY				'Fail' confirmation search of Legal entity, UBO or key executive on any bankruptcy/insolvency proceedings	[INSOLVENCY LIST SERVICE PROVIDER] [KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	[INSOLVENCY AUTHORITY]

CONNECTED INDIVIDUAL ATTRIBUTES FOR LEGAL ENTITIES

- Legal entities are connected to individuals in two key respects. First, a legal entity is connected to its Ultimate Beneficial Owner (UBO) who needs to be identified as part of standard CDD requirements. In addition, legal entities are represented for account opening and management purposes by individuals, but the relationship between the individual acting on behalf of the legal entity is not uniform and can be identified by 5 key relationships covering most typical situations – see table below
- The table gives an overview of the Connected Individual’s attributes required for UBOs as well as for account opening purposes (payment or current account) by a legal entity.
- As can be seen from the table, and in line with table 1 of page 19 :
 - High LoA attributes are related to Trusted sources whereas Substantial LoA attributes are related to RITPs;
 - Low LoA attributes are also related to Trusted sources or RITPs but are evidenced by messages or documents which are not protected. Note however that financial institutions are expected to perform basic checks in relation to Low LoA attributes, meaning that a *prima facie* verification check must not lead to any suspicion of an invalid or fraudulent message or document (for example, the document has not expired or the attributes shown in the document match those already available to the financial institution).
- The type of confirmation expected for each attribute is also broadly defined and may have to be further adjusted to reflect the specifics of each attribute. We expect that in some cases the confirmation will consist in a message confirming one set of data, whereas in other instances the confirmation would result in the production of one or more documents.

CONNECTED INDIVIDUAL'S IDENTITY ATTRIBUTES		LOW LoA	SUBSTANTIAL LoA	HIGH LoA	ELIGIBLE RITPs	ELIGIBLE Trusted sourceS
First Name Family Name Date of birth Place of Birth	The attributes are communicated: - as part of a LOW LoA eID, or - electronically extracted from a current or ID Document in a manner consistent with Low eIDAS LoA standards	The attributes are communicated: - as part of a SUBSTANTIAL LoA eID, - electronically extracted from a current ID Document in a manner consistent with Substantial eIDAS LoA standards	The attributes are communicated: - as part of a HIGH LoA eID, or - electronically extracted from a current ID Document in a manner consistent with HIGH LoA standards			
CONNECTED INDIVIDUAL - ULTIMATE BENEFICIAL OWNER	The Ultimate Beneficial Owner's identity is stated by the Legal entity or electronically transferred or extracted from a current document which is neither a Protected document nor independently verified with or confirmed by a Trusted source or RITP	The Ultimate Beneficial Owner's identity is directly obtained from or confirmed by a RITP or shown in a Current Protected document issued by a RITP	The Ultimate Beneficial Owner's identity is directly obtained from or confirmed by a Trusted source or shown in a Current Protected document issued by a Trusted source		[UBO REGISTER SERVICE PROVIDER] [KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	[NATIONALLY RECOGNISED UBO REGISTER]
LEGAL REPRESENTATIVE The individual is empowered by law to act on behalf of the Company for day to day management matters e.g. managing director	Confirmation by a Company's officer of the individual's position within the Company; or	Direct confirmation by RITP of the individual's position within the Company; or	Direct access by the bank to the Trusted source confirming the individual's name and position within the Company; or		[Notary or lawyer] [Corporate officer of the Company]	official registry office
DIRECTOR The individual is empowered by law to act on behalf of the Company in relation to certain corporate governance matters e.g. chairman of the board/director	Presentation of an unprotected official registry office document showing the individual name and Company's position	Presentation by RITP of an unprotected official registry office document showing the individual's name and position within the Company	Presentation to the bank of a Protected document or certificate issued by the Trusted source showing the individual's name and position within the Company		[KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	
EMPOWERED EMPLOYEE The individual is an employee of the Company authorized by one or more corporate decisions to act on behalf of the Company in relation to one or more categories of actions – 'until further notice' authority e.g. corporate treasury	Confirmation by a Company's officer of the individual's authority to act on behalf of the Company in relation to the relevant action(s); or	Direct confirmation by RITP of the individual's authority to act on behalf of the Company in relation to the relevant action(s); or	Direct access by the bank to the Trusted source confirming the individual's authority to act on behalf of the Company in relation to certain actions; or		[Notary or Lawyer] [Corporate officer of the Company]	company's website
EMPOWERED THIRD PARTY The individual is a third party in relation to the Company authorized by one or more corporate decisions to act on behalf of the Company in relation to one or more categories of actions – 'until further notice' authority e.g. general agent	Presentation of an unprotected copy of the authority delegation decision(s) regarding the individual	Presentation by RITP of an unprotected copy of the authority delegation decision(s) regarding the individual	Presentation to the bank of a protected copy of the authority delegation decision(s) regarding the individual		[KYC UTILITY] [DIGITAL SAFE SERVICES PROVIDER]	
AD-HOC ATTORNEY The individual is authorized to act on behalf of the Company in relation to a given action – 'transaction-specific' authority e.g. any person receiving a transaction-specific power of attorney			Presentation to the bank of a protected copy of the authority delegation decision(s) regarding the individual			

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

A FRAMEWORK CONSISTENT WITH A RISK-BASED APPROACH

- A workable KYC framework has to be assessed in light of the regulatory environment for ML/FT processes, notably the FATF Recommendations and Guidances as well as the AML Directives implementing a risk-based approach (RBA) for customer relationships, including onboarding processes. This implies that financial institutions (obliged entities) evaluate the risk factors relevant to the relationship at stake and adjust their disclosure and due diligence requirements accordingly.
- A key consequence of the RBA framework is that whenever obliged entities identify higher risk situations, they then have to deploy more stringent (enhanced) due diligence measures. Higher risk situations tend to be context specific, but the FATF Recommendations and EU AML directives offer meaningful guidance by identifying a number of situations deemed to be higher risk (client is a politically exposed person, client subject to sanctions, client located in high risk jurisdictions, etc). A critical element is that the financial institution must exercise independent judgment in determining whether a situation is a low, standard or high risk situation. We believe this principle should be maintained and must be reflected in the Proposal.
- The core focus of the Proposal is on standard, as opposed to higher (or for that matter lower) risk situations, i.e. situations that do not, in principle, raise significant risk concerns, but the Proposal will also address higher risk situations by requiring financial institutions to perform ‘RBA-related tests’ and adopt additional measures commensurate with the higher risk situations – more on this in the following page. This means, for example, that opening a standard current account with a small amount credited into the account will (and should) not be treated in the same way when a large amount is immediately credited into the account – therefore triggering ‘source of funds’ investigations & confirmation.
- However, even for standard risk situations, the reality of the onboarding landscape in Europe is that a number of regional/country differences exist that should be reflected in the Framework. We are proposing to deal with them in the following manner:
- As mentioned earlier, the Framework is based upon a minimum set of required attributes for customer identification and due diligence processes, assuming standard (not higher) risk situations. We believe that this approach is entirely in line with eIDAS guidelines (see for example the Annex of Regulation EU 2015 1502 setting out ‘requirements concerning the minimum set of person identification data uniquely representing a natural or legal person’ which defines a minimum data set as well as optional attributes).
- We believe that national authorities could adjust the framework to better reflect the specifics of their environments by adjusting three parameters :
 - Additional attributes could be required;
 - Higher LoAs for the attributes could be required;
 - More stringent ‘refresh’ requirements could be specified for updating attributes;

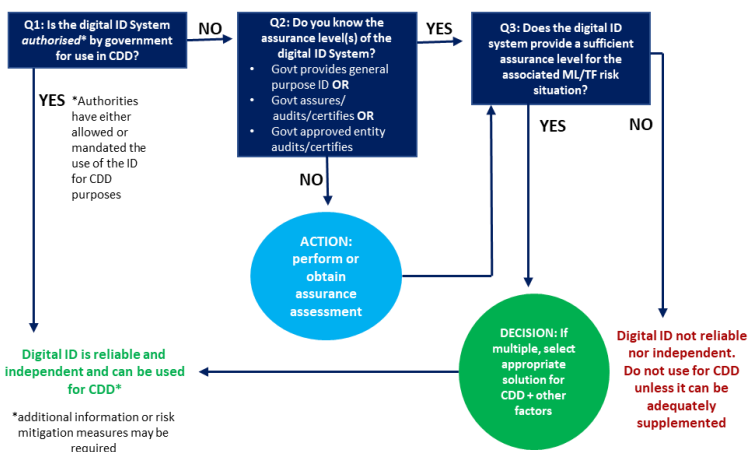
However, a key element of this approach is that the adjusted framework would apply both to domestic financial service providers as well as other EU service providers routinely offering services to customers in the relevant country, especially when making use of the freedom to provide services under the EU banking passport rules).

- We see a number of benefits with this approach :
 - It defines a common attribute-based KYC framework within the EU based on the three eIDAS LoAs – in effect a common language for digital KYC processes;
 - It allows national/regional variations based on recognised differences in environments and practices;
 - It provides a level playing field for service providers which are subject to the same KYC requirements when offering services to the same customers;
 - It also offers greater visibility and consistency for customers

RELATING THE KYC FRAMEWORK TO THE FATF DRAFT DIGITAL IDENTITY GUIDANCE

- The FATF is in the process of drafting a digital identity guidance outlining proposals for the recognition of digital identity solutions within the financial sector. The document is not yet finalised and therefore subject to changes. The scope of the FATF draft guidance is narrower than that of Report 2 as it focuses on customer identification attributes and does not consider customer due diligence attributes. In addition, the FATF draft guidance only deals with attributes of natural persons and does not extend to legal entities. However, there is significant overlap between the two documents and we therefore believe it is important that the KYC Proposal be considered in light of the FATF draft guidance.
- A number of Expert Group members have taken part in the private-sector consultation process initiated by FATF and provided comments and suggestions to the FATF in relation to the draft digital identity guidance.
- A key aspect of the draft guidance is its recognition of the benefits of digital ID systems and solutions from an AML/CFT perspective, including a reduction of human errors, improving customer experience and generating cost savings as well as improving transaction monitoring capabilities of regulated entities. In addition, digital identity solutions are also seen as a powerful tool for financial inclusion, for both emerging and mature financial markets.
- The draft guidance also includes a decision-making flow-chart offering a clear analytical framework for the assessment of digital ID solutions (see Figure 1 below)

Figure 1 - Proposed decision process for regulated entities (Draft guidance)



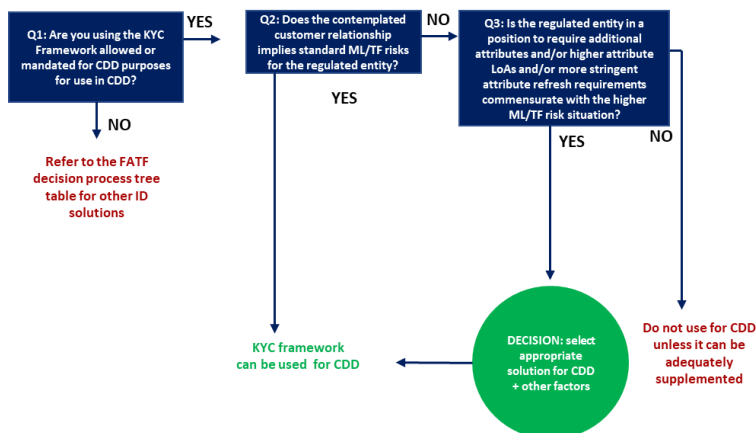
As can be seen from the table, the key question (Q3) is whether the digital ID solution provides a sufficient assurance level for the contemplated customer relationship.

The proposed KYC Framework offers complete convergence with this approach as its overriding principle is that it offers an attribute/LoA combination that is deemed sufficient to deal with standard ML/TF risk situations and is therefore suitable for such situations, but must be strengthened when dealing with higher risks.

This therefore leaves each regulated entity with having to perform the following two risk-based tests for any contemplated relationship:

- Does the relationship imply, for the relevant regulated entity, standard or higher ML/TF risks?
- If higher ML/TF risks are involved, what is the appropriate combination of additional attributes, higher LoAs or more stringent refresh requirements that is commensurate with those risks?

Figure 2 - Proposed decision process for regulated entities (KYC Framework)



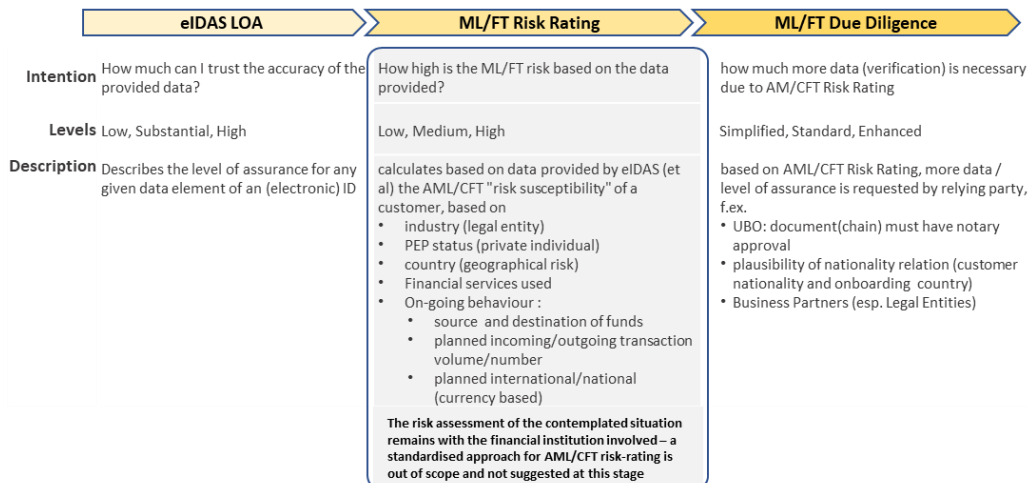
Note that these tests cannot be delegated to third parties and are the ultimate responsibility of the regulated entity. It is therefore up to each regulated entity to show regulatory authorities that, regardless of where attributes are generated from:

- If it is using the KYC framework without changes, this is because the contemplated customer relationship implies standard, not higher, ML/TF risks for the regulated entity; and
- If it is using the KYC framework with changes (such as, inter alia, more attributes and/or higher LoAs and/or more stringent refresh requirements), those changes are adequate for and commensurate with the ML/TF risks involved in the contemplated customer relationship for the regulated entity.

- The proposed KYC Framework does not mandate which attribute and LoA combination is required to deal with higher ML/TF risks. A list of additional attributes is offered but it is up to each regulated entity to determine the appropriate combination in light of the relevant customer relationship circumstances.

RECONCILING LEVELS OF ASSURANCE AND ML/TF RISK RATING

- Levels of assurance and ML/TF risk ratings have long been operating in different spheres but the greater use of LoA-rated digital identities opens up new opportunities for KYC attributes when financial institutions are facing higher risk situations.



Remaining Issue: No (even national) standards for AML/CFT Risk Rating evaluations defined to trigger AML/CFT Due Diligence levels.

- The Proposal advocates setting forth, for standard risk situations only, minimum guidelines in relation to KYC attributes and related LoAs, i.e. defining for the main use cases (for example opening a current or payment account) the list of attributes and related LoAs that regulated entities are expected to receive for the contemplated relationship. A critical benefit of this approach is that it gives users of digital financial services greater visibility and predictability as to which attributes (and related LoAs) will be required from service providers and reduces regulatory arbitrage opportunities (where customers engage with service providers located in countries with lower KYC requirements). This is a key element aligning the cross-border dimension of the EU AML-CFT framework with existing EU banking passport rules.
- The Proposal also recognises the critical importance of the risk-based approach in KYC processes and aims to implement it in the following way:
 - First of all, the Proposal recognises, in line with FATF recommendation 17, that even when KYC attributes are communicated by third parties, the KYC relying entity (i.e. provider of financial services) must remain fully responsible for the implementation of AML rules in relation to the services offered to its clients;
 - In addition, providers of financial services must implement two key RBA-related tests in relation to each contemplated customer relationship, i.e. determine whether:
 - In light of all pertinent factors, the contemplated relationship implies, for the regulated entity involved, standard or higher risks (with a clear understanding that the outcome is regulated-entity dependent); and;
 - If yes, what are the measures that can be meaningfully taken in order to mitigate the (higher) risks.
- The Proposal refrains from adopting a prescriptive approach for mitigating measures as these very often are context-driven and relationship-specific. However, it suggests a range of possible measures which can be combined and are always subject to the professional judgment of the regulated entity – leaving it with the burden of proving to regulatory authorities that it has indeed discharged its AML-CFT obligations in relation to KYC processes. There are:
 - Asking for more attributes;
 - Asking for higher LoAs in relation to the attributes communicated;
 - Implementing more stringent Refresh/Reverify requirements for the attributes.
- These measures are suggested but it is not proposed that they be mandatory in all enhanced due diligence situations. It is also recognised that other measures, such as monitoring the behaviour of the client or using fraud detection processes could be used as well.

ADDITIONAL ATTRIBUTES FOR ENHANCED DUE DILIGENCE

- Financial institutions are at times confronted to higher risk situations requiring enhanced due diligence. A typical case is when the prospect/client is a politically-exposed person.
- Some of these situations are fact-specific and cannot be meaningfully standardised. There is currently no standardized approach for these, except that the AML directive offers a ‘non-exhaustive list of factors and types of evidence of higher risk situations’. However, when confronted to these, financial institutions are required to increase the monitoring of the relationship with the customer.
- The KYC Framework includes a set a pre-defined additional attributes that can be used by financial institutions facing higher-risk situations. Using these attributes is not mandatory and does not exempt obliged entities from showing that the use of the additional attributes and other measures is commensurate with the risks involved by the contemplated customer relationship. However, by setting forth a pre-defined and standardized list of additional attributes to be used by financial institutions, it offers clarity both for what the attributes imply and convey in terms of information as well as offers enhanced reliability by determining what their LoAs imply.
- As part of this process, a proposed approach would be to require the collection of additional attributes along the following three main categories – US Nexus, Business Relationship and Adverse Media.
- However, we do not advocate going beyond Substantial for these additional attributes – so Substantial is the threshold to be achieved.

ENHANCED DUE DILIGENCE			REQUIRED?	LEVEL OF ASSURANCE		
				LOW	SUBSTANTIAL	HIGH
US NEXUS	INDIVIDUAL + LEGAL ENTITY	US TIN (Taxpayer Identification Number)	As part of a risk-based assessment	NOT ACCEPTED	ACCEPTED	ACCEPTED
		US Tax status				
				LOW	SUBSTANTIAL	HIGH
BUSINESS RELATIONSHIP	INDIVIDUAL + LEGAL ENTITY	list of service classes (higher level) and/or banking products (lower level) intended to be used INCOMING / OUTGOING Transactions ¹	As part of a risk-based assessment	NOT ACCEPTED	ACCEPTED	ACCEPTED
	INDIVIDUAL	primary/secondary bank relationship private and/or business relationship to the bank				
	LEGAL ENTITY	Status 'offshore' destination (risk countries) Status 'escrow' account Status NGO/NPO Complex structure status ² Source of Funds/Wealth	As part of a risk-based assessment	NOT ACCEPTED	ACCEPTED	ACCEPTED
				LOW	SUBSTANTIAL	HIGH
ADVERSE MEDIA	INDIVIDUAL + LEGAL ENTITY	Bankruptcy Conviction or Criminal Complaint List Status	As part of a risk-based assessment	NOT ACCEPTED	ACCEPTED	ACCEPTED

¹ yearly number and sum of in-/outflow / currency / channel (cash, MOTO, paper/branch, online/mobile) / country

² basis is the global organization/network structure of all branches, subsidiaries and SPVs starting with the headquarter. complex structure applies when (1) one or more SPVs and/or (2) more than one subsidiary (which additional existence is not legally imposed) per country exist.

ADDITIONAL ATTRIBUTES FOR ENHANCED DUE DILIGENCE

		LoA LOW	LoA SUBSTANTIAL	LoA HIGH	RELEVANT CONFIRMATION	ELIGIBLE RITPs	ELIGIBLE TRUSTED SOURCES
US NEXUS	US TIN (Taxpayer Identification Number) + LEGAL ENTITY	The Relevant Confirmation (i) is not directly obtained from or confirmed by a Trusted source or RITP and (ii) does not appear in a Protected document issued by a Trusted source or RITP	The Relevant Confirmation is directly obtained from or confirmed by a RITP or appears in a Protected document issued by a RITP	The Relevant Confirmation is directly obtained from or confirmed by a Trusted source or appears in a Protected document issued by a Trusted source	US TIN/Tax Status	[BANK] [FINANCIAL INSTITUTION]	[TAX AUTHORITY]
	US Tax status				[Official Tax document]		
ADVERSE MEDIA	Bankruptcy	The Relevant Confirmation (i) is not directly obtained from or confirmed by a Trusted source or RITP and (ii) does not appear in a Protected document issued by a Trusted source or RITP	The Relevant Confirmation is directly obtained from or confirmed by a RITP or appears in a Protected document issued by a RITP	The Relevant Confirmation is directly obtained from or confirmed by a Trusted source or appears in a Protected document issued by a Trusted source	[Insolvency list document] [Media document]	[INSOLVENCY LIST SERVICE PROVIDER] [MEDIA SERVICE PROVIDER] [CONVICTION LIST SERVICE PROVIDER]	[RECOGNISED PUBLIC AUTHORITY]
	Conviction or Criminal Complaint List Status				[Conviction list document] [Criminal Record or Complaint list document] [Media document]	[CRIMINAL RECORD/COMPLAINT LIST SERVICE PROVIDER] [MEDIA SERVICE PROVIDER]	[RECOGNISED PUBLIC AUTHORITY]
BUSINESS RELATIONSHIP	list of service classes (higher level) and/or banking products (lower level) intended to be used				[Insolvency list document] [Media document]	[FINANCIAL INTERMEDIARY SERVICE PROVIDER]	[FINANCIAL SERVICE PROVIDER]
	INCOMING / OUTGOING Transactions						
BUSINESS RELATIONSHIP	primary/secondary bank relationship	The Relevant Confirmation (i) is not directly obtained from or confirmed by a Trusted source or RITP and (ii) does not appear in a Protected document issued by a Trusted source or RITP	The Relevant Confirmation is directly obtained from or confirmed by a RITP or appears in a Protected document issued by a RITP	The Relevant Confirmation is directly obtained from or confirmed by a Trusted source or appears in a Protected document issued by a Trusted source	[Offshore document]	[THIRD PARTY OFFSHORE SERVICE PROVIDER]	[RECOGNISED PUBLIC AUTHORITY]
	private and/or business relationship to the bank				[Official Escrow document] [Official Notary register document] [Official lawyer escrow register document]	[BANK] [FINANCIAL INSTITUTION] [TAX AUTHORITY]	[NOTARY ESCROW REGISTER] [LAWYER ESCROW REGISTER]
BUSINESS RELATIONSHIP	Status 'offshore' destination (risk countries)				[NGO/NPO document]	[THIRD PARTY NPO/NGO INFORMATION SERVICE PROVIDER]	[RECOGNISED PUBLIC AUTHORITY]
	Status 'escrow' account				[Official Business Register document]	[BANK] [FINANCIAL INSTITUTION] [TAX AUTHORITY]	[BUSINESS or TRUST REGISTER AUTHORITY]
BUSINESS RELATIONSHIP	Status NGO/NPO				[Sanction list document]	[SANCTION LISTS SERVICE PROVIDER]	[RECOGNISED PUBLIC AUTHORITY]
	Complex structure status						
BUSINESS RELATIONSHIP	Sanction List Status				[transaction document]	[BANK] [FINANCIAL INSTITUTION]	[LAW FIRM] [NOTARY] [PUBLIC AUTHORITY]
	Source of Funds/Wealth						

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

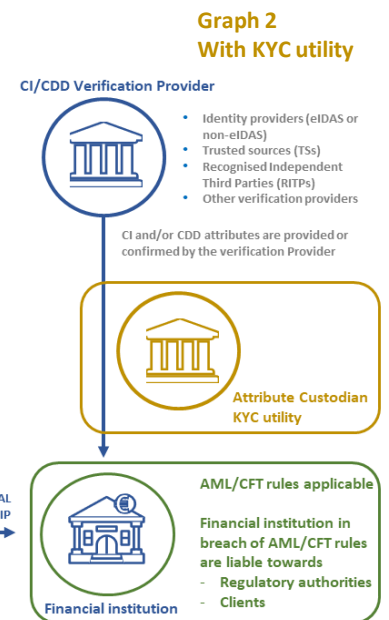
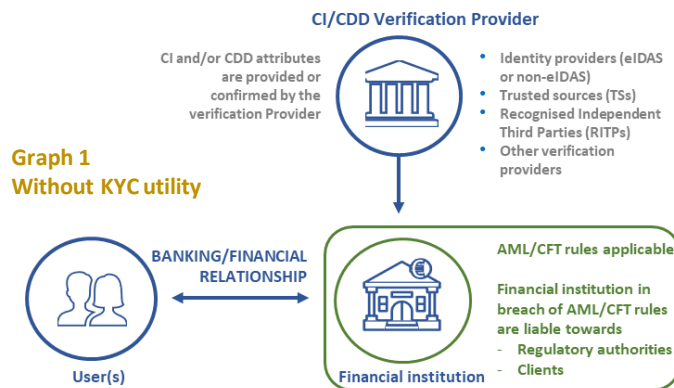
APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

KEY ATTRIBUTE-RELATED TASKS FOR FINANCIAL INSTITUTIONS

- An attribute-based KYC Framework must reflect the reality of digital interactions, meaning that, through various communication channels and IT protocols, a number of stakeholders interact, amongst which the following stand out:

- **Users of financial services** are at the centre of the contemplated customer relationships and are the key decision-makers when it comes to managing and releasing personal data. This is in line with GDPR and privacy principles;
- **Financial Institutions** are subject to AML/CFT rules and regulations and therefore liable towards third parties, critically clients and regulatory authorities;
- **External Verification Providers** are institutions or persons that can meaningfully confirm one or more attributes – typically Trusted sources and RITPs – but are usually not subject to AML/CFT rules.



- As can be seen from Graph 2 above, the relationship between the key stakeholders may also involve KYC utilities acting as attribute custodians and making available attributes as directed by users and/or financial institutions.
- The attribute-based KYC Framework must also reflect the key principle that the ultimate responsibility for ML/TF processes is to remain with the financial institution offering services to the customer – which is also responsible for assessing whether the contemplated relationship is of a standard, higher or lower risk nature. This is in line with FATF Recommendation 17 which states that ‘when reliance is permitted, the ultimate responsibility for CDD measures remain with the financial institution relying on the third party’.
- A way forward is to **adopt an outcome-based approach focusing on the key practical tasks expected to be performed by the attribute-receiving parties**, and therefore recommend identifying four key attribute-related tasks to be complied with in connection with onboarding requirements. These are the **Collect, Verify, Record & Process as well as the Refresh tasks** applying to all attributes and described below.

Key Attribute-related Tasks

	Collect Attribute	Verify Attribute	Record & Process Attribute	Refresh Attribute
	The financial institution can show that it has obtained the attribute when required to do so	The financial institution can show that it has taken appropriate steps to assess the genuineness of the attribute	The financial institution can show that it has recorded and integrated the attribute in its operating processes for a meaningful purpose	The financial institution can show that it has monitored and refreshed the attribute as and when needed.
Task required and financial institution liable when task missing or failed?	Yes	Yes	Yes	Yes
LoA dependent?	No	Yes	No	Yes

Discussed in more detail in the following pages

- As mentioned above, a financial institution is as a matter of principle liable for AML/CFT measures, but showing that it has implemented the key attribute-related tasks in accordance with industry-standard practices should allow it to significantly mitigate or avoid liability implications.

TASK DESCRIPTION - THE VERIFY AND REFRESH TASKS ARE LoA-DEPENDENT

- Out of the four main tasks identified above, the Collect and Record & Process tasks pose few difficulties, and are in fact not new for the financial sector. Indeed, there is little doubt that a financial institution that would fail to collect a required attribute or, having obtained it, fail to process it in an appropriate manner would be found in violation of AML/CFT requirements.
- The Verify task is more critically related to the effectiveness of any AML/CFT obligations and therefore deserves greater scrutiny. However, it is also reflected in the KYC Framework as a key dimension of the LoA-rated approach outlined in the Proposal. Indeed, using a High LoA-rated CI/CDD attribute offering a high level of confidence will imply verification processes that are commensurate with, and do not weaken, the High LoA. no doubt be seen as requiring more stringent verification purposes than using a Low LoA-rated one. As mentioned earlier, the Proposal relates Trusted sources and RITPs to the High and Substantial LoA levels.
- In light of this connection, we suggest linking the ‘Verify’ task to the following two determinations :
 - That the attribute data is indeed originating from or confirmed by a recognised Trusted source or RITP; and
 - That, when shown in a Protected document, the Protected document is indeed protected, so that the integrity of the attribute data (including the identity of the data provider) is not compromised;
- This implies, in line with current practice for physical ID and other document, that there is no requirement to go beyond a Trusted source or RITP as information or verification provider for the High and Substantial LoAs.
 - For example an official ID document originating from a national authority (Trusted source) is deemed assigned a High LoA, without having to assess whether the document was genuinely (or fraudulently) obtained from the national authority.
 - Likewise, as the Current Address attribute is assigned a minimum Substantial LoA requirement under the Proposal, there is no need to go beyond what a RITP would confirm in its respect. This implies that the financial institution is not to be held liable in the very unlikely (High LoA) or unlikely (substantial LoA) event that the information provided by a Trusted source or RITP proves incorrect.
- The right-hand side tables show how the Verify and Refresh tasks operate in an LoA-rated environment

VERIFY ATTRIBUTE TASK	
LoA LOW	<ul style="list-style-type: none"> • check the prima facie consistency of the CI/CDD attribute data with a view to confirm that a mere reading of the data does not result in any contradictory or highly implausible information; • Check that the attribute data is current and collected within its validity period ;
LoA SUBSTANTIAL	<p>Same as for Low LoA +</p> <p>Verify the conditions required for Substantial LoA, meaning that :</p> <ul style="list-style-type: none"> ○ The CI/CDD attribute provider is confirmed¹ as a recognised RITP; ○ The CI/CDD attribute data is directly collected or confirmed from a RITP or appears in a Protected document originating from a RITP; ○ When the CI/CDD attribute is extracted from a Protected document, the protection of the document is verified. When it is extracted from an unprotected document, the attribute is directly confirmed by the RITP; ○ When the CI/CDD attribute is required to have been used by the RITP for a minimum usage period, such period is confirmed by the RITP; <p>1. following reasonable investigations commensurate with Substantial LoA standards</p>
LoA HIGH	<p>Same as for Low LoA +</p> <p>Verify the conditions required for High LoA, meaning that :</p> <ul style="list-style-type: none"> ○ The CI/CDD attribute provider is confirmed¹ as a recognised Trusted source; ○ The KYC data is directly collected or confirmed from a Trusted source or appears in a Protected document originating from a Trusted source; ○ When the CI/CDD attribute is shown in a Protected document, the protection of the document is verified. When it is shown in an unprotected document, the attribute is directly confirmed by the Trusted source; ○ When the CI/CDD attribute is required to be issued or used by the Trusted source for a minimum usage period, such period is confirmed by the Trusted source; <p>1. following reasonable investigations commensurate with High LoA standards</p>

REFRESH ATTRIBUTE TASK
<p>The same principles apply <i>mutatis mutandis</i> to the Refresh Attribute task, which effectively operates as a Re-Verify and Re-Process requirement.</p> <ul style="list-style-type: none"> - When the attribute is time-limited, i.e. is valid for a certain period only, the attribute must be refreshed before the end of the validity period; - When the attribute is not time-limited, but required to be refreshed pursuant to AML/CFT purposes, see guidelines outlined in page 19.

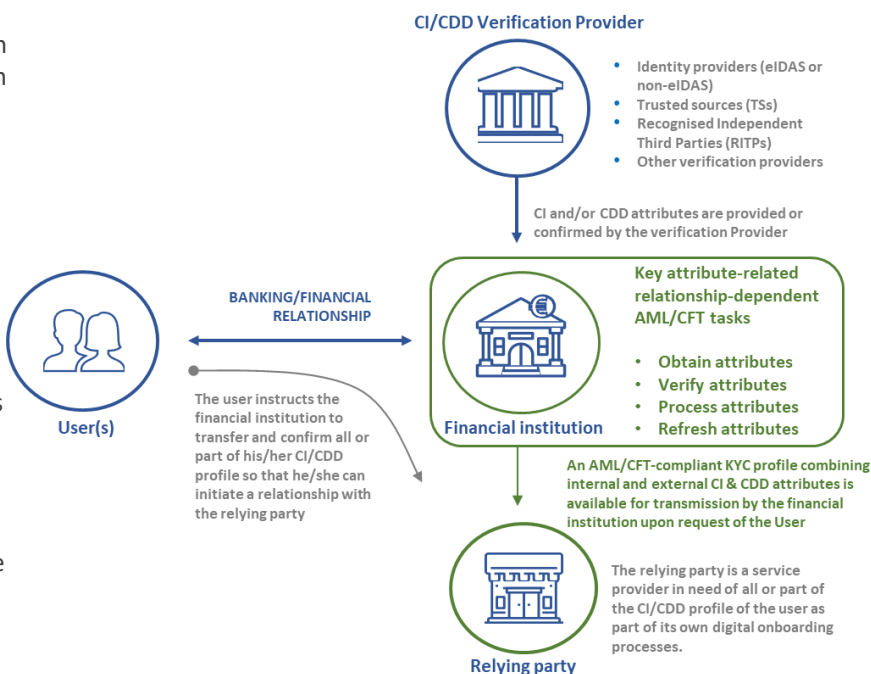
A STAKEHOLDER-BASED APPROACH OPENING UP MUTUALISATION OPPORTUNITIES AND POSITIONING THE FINANCIAL SECTOR AS PROVIDER OF QUALITY KYC PROFILES

- The deployment of an attribute-based & LoA-rated EU standard based on stakeholders interactions allows a much needed cost mutualisation of KYC processes for the financial industry, with two positive impacts :

 - Onboarding costs can be lowered through economies of scale, therefore allowing new and/or more competitive financial services to customers as well as facilitating financial inclusion for minority/deprived communities;
 - It also increases the ‘addressable market’ for KYC services, which are nationally constrained, and opens up a new role for CI/CDD attribute providers and KYC utilities offering services to various relying parties on a pan-European basis.
- As mentioned earlier, the emergence of CI/CDD standards will also reduce or eliminate regulatory arbitrage incentives by treating on an equal footing EU service providers – a key single-market consideration for services offered on a cross-border service basis with a banking/financial services passport. Last but certainly not least, an attribute-based LoA-rated CI/CDD standard facilitates compliance with liability rules by clarifying the key requirements expected for each LoA.

- The Proposal implements the ‘Once-only’ principle and is making greater use of the open data environment, where attribute verification providers are selected on the basis that they have authority and legitimacy to confirm the attribute of a user. For example, the postal service (recognised as Trusted source) or a public utility (recognised as a RITP) could be used to confirm the validity of an address.

- We believe this KYC-reliance approach can be improved and ML/FT processes significantly strengthened by having LoA-rated KYC profiles communicated to other service providers. However, this should only occur upon clear instruction of clients in accordance with GDPR and privacy rules. We expect clients to react positively to this as they would otherwise have to go through new KYC onboarding processes with KYC relying parties, with the need to provide the required information themselves.



- This implies that KYC profiles can be transferred, at the client’s request and with the client’s consent, from an existing financial institution (or KYC utility) to a KYC Relying Party, which may or may not be subject to AML/CFT obligations, in order to meet specific needs.

KYC Relying Parties are other service providers in need of a set of identity and customer due diligence attributes in order to initiate a business relationship. They may well be part of the financial sector, which would typically be the case for secondary banking relationships, or from other industries needing robust CI and CDD onboarding processes (insurance, travel, business services, etc)

- The transfer of KYC profiles should of course not weaken the overall quality and robustness of EU anti-money laundering regulations nor encourage riskier behaviour and/or questionable practices for service providers acting as KYC relying parties. This means that, when the KYC relying party is itself subject to AML/CFT rules, it will always have to satisfy itself (and be able to show regulatory authorities) that:

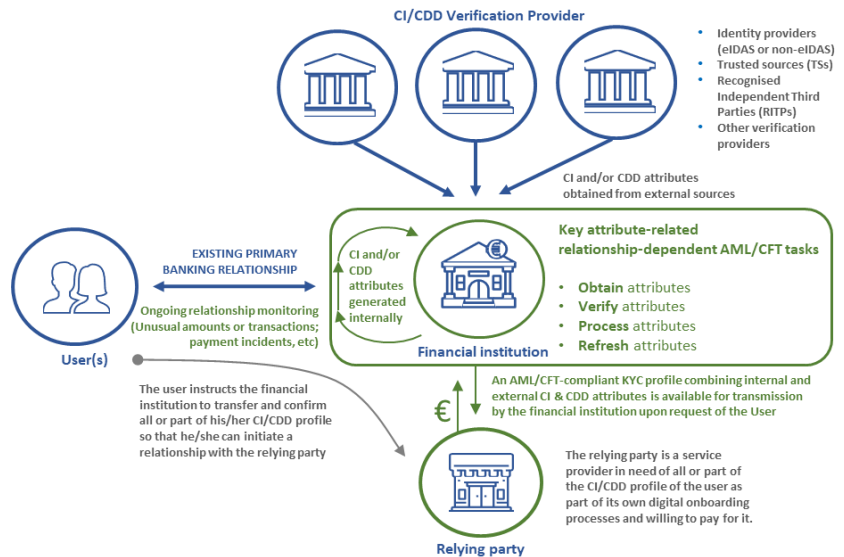
 - the KYC profile it plans to use is relevant and commensurate with the risk-assessment of the contemplated customer relationship (a risk-based test) and;
 - The various attribute-related tasks (see above) have been satisfactorily implemented as stated above.
- The reliance on existing KYC processes of third parties is not new for AML/CFT purposes – for example, AMLD3 defines as ‘adequate measure to compensate for higher risks’ the fact that a first payment is made from an existing bank account of the customer, implying that when KYC processes have been implemented within another obliged entity, this is a mitigating factor even when no significant KYC information is transferred from the original bank to the new one.

A STAKEHOLDER-BASED APPROACH ALLOWING BANK-BASED AS WELL AS KYC UTILITY SERVICES

- The Proposal facilitates the mutualisation of KYC processes and positions the financial sector as key provider of digital KYC services but also recognises that a role is likely to be played by external KYC providers, i.e. KYC utilities. The Proposal does not recommend a specific approach in this respect as it foresees that there will be room for several approaches and is meant to accommodate two models for KYC mutualisation:
 - A decentralised model based upon existing banking relationships;
 - A centralised model centred around KYC utilities.
- The decentralised model implies that a financial institution maintains a KYC profile for its clients and that, upon request of a client, all or part of the KYC profile is transferred to a KYC relying party against payment, as illustrated below.

- It is anticipated that this approach may/will be of interest to general purpose/universal banks maintaining primary banking relationships with clients.

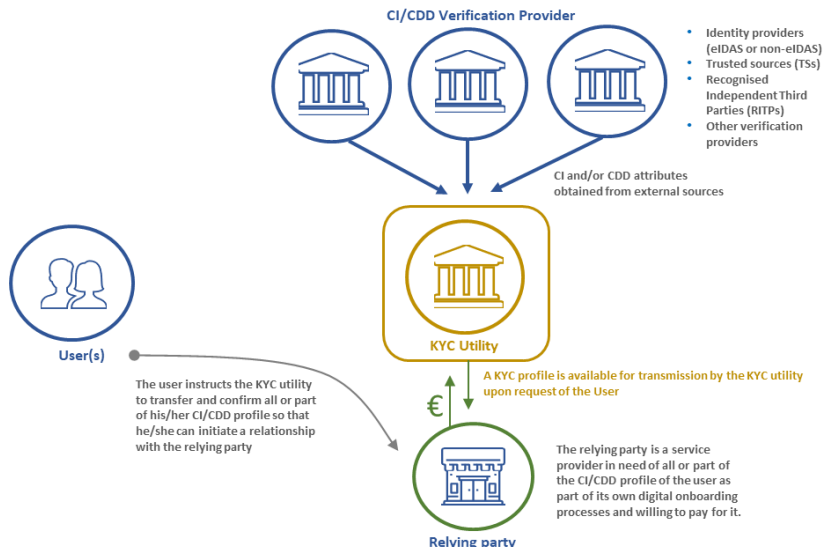
- It can also be tailored to address specific needs of certain categories of clients. For example, a professional may find value in his/her bank confirming to third parties the fact that he/she is ‘in good financial standing’, with no payment incident having occurred in his bank account during a given period.



- However, a more centralised approach may also be taken, using dedicated KYC providers such as KYC utilities, as shown in the graph below.

- This implies that the KYC relying party will have to fully satisfy itself that the KYC profile is consistent with AML/CFT requirements, as it may not rely on an on-going financial sector relationship.

- Note that the two models can also be combined and should therefore not be viewed as incompatible.



- The Proposal recognises that the KYC relying party is to remain primarily liable towards regulatory authorities and clients for the AML/CFT implications of its own services, but suggest clarifying that recourse can be implemented towards the financial institution transferring the KYC profile, especially in situations where the LoA criteria have not been complied with - for example, when a Substantial LoA is required, the failure by the transferring financial institution to obtain the relevant attribute from a recognised RITP or Trusted source could result in it being held liable as a result.

KYC INTEROPERABILITY MAKING USE OF ESTABLISHED IT PROTOCOLS

- The description of IT protocols for the implementation of the Proposal is likely beyond the scope of the mandate given to Priority Group 2 and will therefore not be considered in great detail. However, it is important to assess whether the Proposal can indeed be deployed in a satisfactory manner across the various stakeholders involved using an existing IT protocol.
- There are two main protocols to be considered in this respect:
 - **SAML** (Security Assertion Markup Language) is a leading open standard for authorisation and authentication and is used to propagate attributes between an identity provider and a service provider. In SAML, there is an “assertion”—a signed XML document with the subject information (who authenticated), attributes, the issuer (who issued the assertion), and other information about the authentication event. SAML is widely used and a lot of applications support SAML. It is worth noting that the eIDAS Network linking eIDAS nodes as part of the eIDAS interoperability framework uses SAML 2.0 and there is an eIDAS-compliant set of technical specifications which member States use to develop their own eIDAS-compliant implementation.
 - **OpenID Connect**. OpenID Connect is an authentication layer working on top of OAuth 2.0, which itself is a authorization framework. OAuth 2.0 is widely used due to its versatility to specify and enforce access controls and has found favour with social network API providers such as Facebook and LinkedIn as well as cloud service providers such as Microsoft, Google and Amazon. Additionally, many API Management solutions utilize OAuth 2 as the mechanism by which to control access to the APIs they manage, including those used to give access to third party service providers as part of the Payment Services Directive 2 (PSD2) deployment so that customer data can be shared between institutions and be incorporated into third party applications in a common, consistent format.

Since OpenID Connect is a ‘profile’ of OAuth 2.0 specifically designed for attribute release and authentication, it can effectively be viewed as an updated and simplified rewrite of SAML using OAuth 2.0 which explicitly addresses mobile use cases.
- The Proposal is not taking any position as to which of these two IT protocols should be favoured – the ideal situation is that it could be meaningfully used by both.
- We have initiated a dialogue with Nat Sakimura, chairman of the OpenID foundation, who confirmed that a LoA-rated Attribute-based framework for identity and CDD poses no significant problems when it comes to envisioning a deployment with OpenID Connect.
- In addition, a number of initiatives refer to blockchain-based projects and protocols, such as the Once-Only Principle project, which could offer an trustworthy alternative for the propagation of ID and CDD attributes. It is still a bit early to consider in detail the impact of these projects but the likely deployment of decentralised PKIs and self-sovereign identities could have a major impact on the way electronic identities are made available to all stakeholders involved.

TABLE OF CONTENT

INTRODUCTION

- FOREWORD
- EXECUTIVE SUMMARY

KEY-FEATURE ASSESSMENT OF A KYC FRAMEWORK FOR THE DIGITAL AGE

REMOTE ONBOARDING : FROM DOCUMENT-BASED TO DIGITAL-NATIVE ATTRIBUTES-BASED PROCESSES

- Facing a fragmented landscape in the EU – Regulatory and operational implications
- Connecting eIDAS and AML/CFT principles : the role of attributes & LoAs

CI AND CDD ATTRIBUTES – ASSESSING TRUSTWORTHINESS

- CI attributes – a level playing field for eIDAS eIDs and attributes remotely extracted from ID documents
- CDD attributes - accessing Trusted sources (TSs) and Recognised Independent Third Parties (RITPs)

A KYC FRAMEWORK FOR CUSTOMARY ONBOARDING JOURNEYS – STANDARD AML/CFT RISKS

- Developing an EU standard for customary onboarding cases
- KYC attributes – Individuals
- KYC attributes – Legal entities

A RISK-BASED APPROACH MEETING ROBUST AML/CFT REQUIREMENTS

- A Proposal consistent with the draft FATF digital identity guidance
- Understanding key AML/CFT tasks involved in attribute management processes
- Assessing higher risk situations and enhanced due diligence requirements

ADDRESSING THE PORTABILITY CHALLENGE - INTERACTIONS BETWEEN KYC STAKEHOLDERS

- Clarifying the attribute-related tasks required for KYC processes
- Addressing liability implications and strengthening existing AML/CFT standards
- Achieving KYC reusability with existing IT standards

APPENDIX

- Proposed implementation - AML and eIDAS adjustment considerations
- Other standard services

APPENDIX – PART 1 : SUGGESTED REGULATORY IMPLEMENTATION OF THE KYC FRAMEWORK (1/3)

- The KYC Framework is designed to contribute to foster a digital economy in Europe, implement the single market for financial services as well as strengthen the ML/FT processes of the financial sector. In order to ensure its effectiveness, it needs to be translated into concrete regulatory actions.
- We believe two key events indicate a clear direction for this. There are:

The ECOFIN Council Conclusions on strategic priorities on anti-money laundering and countering the financing of terrorism

The document published on December 5 2019 is relevant in that it recognises the need to take a holistic approach for AML/CFT processes and suggests a number of initiatives, among which the following stand out:

- Transforming the Anti-Money Laundering Directive into a Regulation in order to achieve a higher level of harmonisation;
- by exploring the opportunities and challenges in using technological innovation in combatting money laundering and countering the financing of terrorism;
- Transferring certain responsibilities and powers for anti-money laundering supervision to a Union body with an independent structure and direct powers vis-à-vis certain obliged entities chosen by the EU body in accordance with a risk-based approach.

We believe that the recommendations outlined in Report 2 are consistent with the suggested changes.

The forthcoming eIDAS Revision

We note that the eIDAS Regulation is to be reviewed pursuant to its article 49 and that a Commission report, including any relevant legislative proposals, is to be presented no later than July 1, 2020 to this effect. As the KYC Framework relies on eIDAS eIDs there is clear merit in ensuring that it is consistent with the revised eIDAS regulation.

This leads us to suggest that changes could be made in two main directions:

DIRECTION 1 – REVISED AML REGULATION AND EBA MANDATE

- The implementation of the Proposal is based on the contemplated AML Regulation setting out a number of broad principles in relation to the KYC Framework, whereas the European Banking Authority (EBA) would be given the mandate to issue Regulatory Technical Standards and/or Guidances on a number of more specific topics.
- This approach is fully in line with the EBA's priorities as well as its more explicit and comprehensive mandate to ensure that risks of money laundering and terrorist financing in the Union's financial system are effectively and consistently incorporated into the supervisory strategies and practices of all relevant authorities.

The contemplated AML Regulation would:

- *Generally* relate ID, Contact & Status attributes to defined LoA Levels;
- *Generally* relate High LoAs to 'Trusted Sources' (meaning 'authoritative sources' for ID attributes under eIDAS Regulation 2015/1502 and 'Trusted Sources' for Contact & Status attributes) and Substantial LoA to 'Recognised Independent Third Parties';
- *Generally* recognise the position of KYC attribute custodian, which can be performed by financial institutions acting as providers of decentralised KYC services or by KYC Utilities acting as providers of centralised KYC services and submit them to parts of the AML/CFT regulatory framework;

APPENDIX – PART 1 : SUGGESTED REGULATORY IMPLEMENTATION OF THE KYC FRAMEWORK (2/3)

- Require all Member States having notified a Substantial or High LoA eIDAS scheme make sure that Substantial and High LoA eIDAS eIDs can be accepted by financial service providers as part of their onboarding processes;
- Require Trusted Sources to give financial institutions and other regulated entities direct access to selected databases for the purpose of implementing KYC processes – i.e. developing an open data environment - with a unified API;
- *Generally* identify the four key tasks (collect, verify, record & process, refresh) for KYC attributes used by financial institutions and obliged entities as part of their onboarding processes;
- Confirm that financial service providers relying on KYC attributes provided by one or more third parties always bear responsibility vis a vis regulatory authorities and clients for (i) implementing the various tasks required for KYC attributes and (ii) identifying higher risk situations and deciding which additional measures commensurate with the higher risks are then to be taken;
- Clarify that attributes may be collected from different sources using different communication channels (for example, ID attributes could be collected through an eIDAS node, whereas other attributes could be made available using an industry standard protocol (e.g. SAML or OpenID Connect))

(The use of the term '*generally*' means that only broad principles are expected to be outlined, leaving implementation provisions to appear in ancillary regulations)

EBA RTSs or Guidances would be issued on the following topics:

- Establishing the list of Core ID, Contact and Status attributes required for onboarding purposes in standard risk situations and the minimum LoAs required for standard risk onboarding processes;
- Establishing a standardized list of further attributes for specific product categories, such as lending, investment, payment, etc. as well as for higher ML/FT risk situations as well as the related LoAs;
- Determining, for each attribute, the eligible Trusted Sources and the categories of RITPs involved ;
- Defining the list of metadata required for Contact and Status attributes communicated from one participant to another (for example, LoA, source, date of verification, expiry date, etc);
- In consultation with leading IT Security agencies (such as BSI and ANSSI) and/or the eIDAS Cooperation network, assessing the LoA implications of communicating ID and other attributes extracted from existing ID documents, when there is no digital identity involved in this process;
- Clarifying the operational implications of the KYC tasks involved and determining how they are LoA-dependent;
- Clarifying the role of attribute custodians for decentralised and centralised KYC services and determining which part of the AML Regulation they should be subject to;
- Defining the key specifications of a unified European KYC data communication standard extending eIDAS attribute with the proposed set of attributes and using an industry standard (SAML or OpenID Connect) for the purpose of exchanging KYC attributes and implementing an open data environment within Europe. The data communication standard will also reduce cyber security and data protection risks by using further industry standards for decentralized data access and communication (eg distributed ledger technologies).

DIRECTION 2 – AMENDING THE eIDAS REGULATION

A number of change proposals can meaningfully be made, including the following:

- A proposal would then be to establish an EU-wide certification scheme based on Implementing Regulation 201/1502. That would imply a certification process for ID systems where e.g. defined conformity assessment bodies (CABs) may confirm the compliance of ID systems according to IA 2015/1502. The CABs may be selected as already defined in point 18 of Article 3 of the eIDAS Regulation (EU) 910/2014. All ID systems which are certified through that process would be eligible to offer their services in the private sector;

APPENDIX – PART 1 : SUGGESTED REGULATORY IMPLEMENTATION OF THE KYC FRAMEWORK (3/3)

- In addition, a specific financial sector set of rules could be envisaged as part of a revised eIDAS regulation. These would cover for example contact attributes with varying LoAs;
- Greater transparency should be offered by the eIDAS Cooperation Network and it is suggested that, in line with the existing practice under NIST 800-60-3 guidelines, component LoA ratings be assigned to the identity proofing and authentication of a digital identity scheme, so that core ID attributes could be propagated with the benefit of an identity proofing LoA;
- Lastly, care should be taken to ensure that the identity proofing requirements of qualified certificates used for trust services (notably electronic signatures and seals) are consistent with those used for Substantial and/or High LoA eIDs.

APPENDIX – PART 2 : OTHER ONBOARDING USE CASES

CREDIT SERVICES

- The KYC Framework presented here applies to customary onboarding processes in order to access account/payment services that do not involve credit related facilities or savings/investment services.
- It is recognised that these services may require additional attributes. For example, applying for credit involves additional investigations required to assess the creditworthiness of the borrower. A simple example is when an individual applies for a consumer loan and is required to show proof of income.
- There are major benefits in having a more standardized approach for these use cases– which bring a level-playing field and improve regulatory standards for key financial services as well as meet other regulatory requirements (such as MIFID 2 for investment services). As for account/payment services, care must be taken to ensure that financial institutions remain in a position to add other requirements reflecting their own credit as well as customer eligibility criteria (therefore implementing a ‘minimum viable’ approach).
- We present below a proposal for credit/lending services– using only generic terms that can apply to a wider range of situations. A corresponding proposal has been provisionally prepared for investment (savings) services– see Appendix.

		LENDING			
			LOW	SUBSTANTIAL	HIGH
LENDING	INDIVIDUAL	Spending pattern Proof of Income	REQUIRED	NOT ACCEPTED	ACCEPTED
	LEGAL ENTITY	financial accounts tax statements			ACCEPTED

		LENDING			Relevant Confirmation means the production of:	Eligible RITPs	Eligible Trusted Sources	
		LOW	SUBSTANTIAL	HIGH				
LENDING	INDIVIDUAL	SPENDING PATTERN	The Relevant Confirmation (i) is not directly obtained from or confirmed by a Trusted source or RITP and (ii) does not appear in a Protected document issued by a Trusted source or RITP	The Relevant Confirmation is directly obtained from or confirmed by a RITP or appears in a Protected document issued by a RITP	The Relevant Confirmation is directly obtained from or confirmed by a Trusted source or appears in a Protected document issued by a Trusted source	[CURRENT ACCOUNT STATEMENTS]	[PUBLIC AUTHORITY]	[BANK or FINANCIAL INSTITUTION]
	INDIVIDUAL	PROOF OF INCOME				[KEY TAX DATA] [KEY SALARY DATA]	[BANK or FINANCIAL INSTITUTION]	[TAX AUTHORITY] [EMPLOYER]
	LEGAL ENTITY	FINANCIAL POSITION	[FINANCIAL ACCOUNTS]	[BANK or FINANCIAL INSTITUTION] [PUBLIC AUTHORITY]	[COMPANY'S AUDITORS]			
		TAX POSITION	[TAX STATEMENT]	[BANK or FINANCIAL INSTITUTION]	[TAX AUTHORITY]			

INVESTMENT SERVICES

Further work has been initiated on key KYC requirements for the investment services onboarding use case. Work has just started on this and only preliminary discussions have taken place on the matter, which is therefore less advanced than other areas presented in Report 2. However, the preliminary investment services onboarding proposal is shared and illustrates a possible course of action for those categories of financial services.

LoA
LOW LoA
SUBST
ANTIAL LoA
HIGH

INDIVIDUAL + LEGAL ENTITY	Financial Status	MiFID2 - Customer Category		MiFID2 Client Category: (a) Eligible Counterparty (b) Professional Client (c) Retail Client
	Risk Tolerance	educational degrees/certificates with relation to trading or investing in securities	NOT ACCEPTED	
		professional relation to trading or investing in securities ¹		
	Risk Attitude	personal threshold (in %) of maximal securities price drops		Document is a printout signed by the prospect or eDocument electronically signed by the prospect;
		personal threshold (in %) of maximal asset loss		alternatively attributes can be directly obtained from other [FINANCIAL INSTITUTIONS], who have accomplished Risk Attitude Assessment f2f (or remotely via WebEx and Video)
		regular self-information about development of economy and financial markets as well as status of own securities/derivatives ¹	ACCEPTED	
		preference Risk vs. Yield		
		Self-Declared Risk Type, i.e. risk avoidance, risk aware, risk taking	ACCEPTED	
	Customer Knowledge	personal experience / financial instrument, i.e. low/medium/high ¹		financial instrument structures ideally based on ISO 10962
		risk disclosures by expert / financial instrument, i.e. yes/no ¹		
Fin. Stat.	Source of Funds/Wealth	NOT ACCEPTED	Similar LoA as Source of Funds; Should be added to the Status and Due Diligence Attribute Source of Funds with ".../Source of Wealth"; Split into the following parts (ideally based on ISO/CD 21586 - higher level): (a) Financial Assets / currency / product group (b) Other Assets (Art, real estate, etc.) / currency / product group (c) Financial Liabilities / currency / product group	
Risk Tolerance	expected dates of changes which will lead to higher expenses		Alternatively balance sheets; ideally based on XBRL (eXtensible Business Reporting Language)	
			Documents - are f.ex. tax statements (tax debts or tax credits), testaments, real estate purchase contracts, loan contracts, ... and - have an additional structure based on ISO/CD 21586	
INDIVIDUAL	Risk Tolerance	number of people to provide financially		
		regular - yearly - net income of household/currency	NOT ACCEPTED	ACCEPTED
		regular - yearly - net savings of household / currency		
LEGAL ENTITY	Risk Tolerance	regular - yearly - net income of legal entity / currency	NOT ACCEPTED	ACCEPTED
		regular - yearly - net financial investments of legal entity / currency		

		LOW	LEVEL OF ASSURANCE SUBSTANTIAL	HIGH	Notes		
Investment	Financial Status	MIFID2 - Customer Category	The MiFID2 Customer Category [is declared by the prospect or] is electronically extracted from a [document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The MiFID2 Customer Category is directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION]	The MiFID 2 Customer Category is directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] or is shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION]	1	
		Risk Tolerance	educational degrees/certificates with relation to trading or investing in securities	The Educational Degrees/Certificates [are declared by the prospect or] are electronically extracted from a [transaction document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The Educational Degrees/Certificates are directly obtained from or confirmed by RITP or shown in protected e-document issued by it when such RITP is [EDUCATIONAL AUTHORITY] [BANK] [FINANCIAL INSTITUTION]	The Education Degrees/Certificates of the prospect are directly obtained from or confirmed by [EDUCATIONAL AUTHORITY] [BANK] [FINANCIAL INSTITUTION]	
	INDIVIDUAL + LEGAL ENTITY	Risk Tolerance	professional relation to trading or investing in securities ¹	<i>filtered based on Occupation</i>	<i>filtered based on Occupation</i>	<i>filtered based on Occupation</i>	
		Risk Attitude	personal threshold (In %) of maximal securities price drops				
		Risk Attitude	personal threshold (In %) of maximal asset loss				
	Risk Attitude	regular self-information about development of economy and financial markets as well as status of own securities/derivatives ¹	The Risk Attitude attributes [are declared by the prospect or] are electronically extracted from a [document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The Risk Attitude attributes are directly obtained from or confirmed by a RITP or are shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION]	The Risk Attitude attributes are directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] or are shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION]	2	
Risk Attitude	preference Risk vs. Yield						
Risk Attitude	Self-Declared Risk Type, i.e. risk avoidance, risk aware, risk taking						
Customer Knowledge	personal experience / financial instrument, i.e. low/medium/high ¹	The Customer Knowledge attributes [are declared by the prospect or] are electronically extracted from a [document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The Customer Knowledge attributes are directly obtained from or confirmed by a RITP or are shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION]	The Customer Knowledge attributes are directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] or are shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION]	3		
	risk disclosures by expert / financial instrument, i.e. yes/no ¹						

		LOW	SUBSTANTIAL	HIGH	Notes		
Investment & Lending	Financial Status	Source of Funds/Wealth	The Source of Wealth [is declared by the prospect or] is electronically extracted from a [transaction document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	A Source of Wealth check is directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [LAW FIRM] [NOTARY] [PUBLIC AUTHORITY] [BANK] [FINANCIAL INSTITUTION]	The Source of Wealth is directly obtained from or confirmed by [LAW FIRM] [NOTARY] [PUBLIC AUTHORITY] [BANK] [FINANCIAL INSTITUTION] or is shown in a protected e-document issued by [LAW FIRM] [NOTARY] [PUBLIC AUTHORITY] [BANK] [FINANCIAL INSTITUTION]	4	
		Risk Tolerance	expected dates of changes which will lead to higher expenses	The expected dates of changes of the prospect are: • declared by the prospect or • Electronically extracted from an [Official Document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The expected dates of changes are directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION] [TAX AUTHORITY] [NOTARY]	The expected dates of changes of the prospect are directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] [TAX AUTHORITY] [NOTARY] or is shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION] [TAX AUTHORITY] [NOTARY]	
	INDIVIDUAL	Risk Tolerance	number of people to provide financially	The number of people to provide financially of the prospect is: • declared by the prospect or • Electronically extracted from an [Official Tax document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The number of people to provide financially of the prospect is directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [TAX AUTHORITY] [SOCIAL SECURITY]	The number of people to provide financially of the prospect is directly obtained from or confirmed by [TAX AUTHORITY] [SOCIAL SECURITY] or is shown in a protected e-document issued by [TAX AUTHORITY] [SOCIAL SECURITY]	
		Risk Tolerance	regular - yearly - net income of household / currency	The regular net income/savings [are declared by the prospect or] are electronically extracted from a [financial/account statement document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The regular net income/savings are directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY]	The regular net income/savings are directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY] or are shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY]	5
		Risk Tolerance	regular - yearly - net savings of household / currency				
	LEGAL ENTITY	Risk Tolerance	regular - yearly - net income of legal entity / currency	The regular net income/financial investments [are declared by the prospect or] are electronically extracted from a [financial/account statement document] in a manner not protecting the authenticity and integrity of the data (scan, photo, fax etc.)	The regular net income/financial investments are directly obtained from or confirmed by a RITP or is shown in a protected e-document issued by it when such RITP is a [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY]	The regular net income/financial investments are directly obtained from or confirmed by [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY] or are shown in a protected e-document issued by [BANK] [FINANCIAL INSTITUTION] [PUBLIC AUTHORITY]	6
Risk Tolerance		regular - yearly - net financial investments of legal entity / currency					

1 MiFID2 Client Category:
(a) Eligible Counterparty
(b) Professional Client
(c) Retail Client

2 Document is a printout signed by the prospect or eDocument electronically signed by the prospect;

3 alternatively attributes can be directly obtained from other [FINANCIAL INSTITUTIONS], who have accomplished RiskAttitude Assessment f2f (or remotely via WebEx and Video) financial instrument structures ideally based on ISO 10962

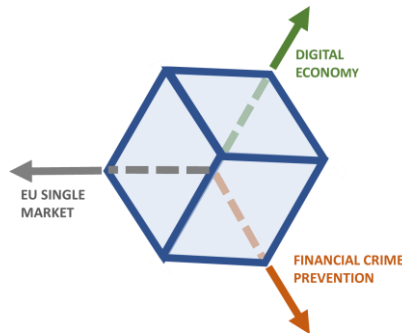
4 Documents
- are f.ex. tax statements (tax debts or tax credits), testaments, real estate purchase contracts, loan contracts, ... and
- have an additional structure based on ISO/CD 21586

5 Public Authority: f.ex. Tax Authority, Social Security, etc.
Public Authority: f.ex. Tax Authority, Social Security, etc

6 Alternatively also balance sheets, ideally based on XBRL

CONCLUSION

MOVING TOWARDS DIGITAL AGE KYC PROCESSES IS A CHALLENGE...



...WITH PROGRESS TO BE MEASURED BY ASSESSING THE DIGITAL ECONOMY, FINANCIAL CRIME PREVENTION AND SINGLE MARKET DIMENSIONS OF ANY PROPOSAL CONSIDERED

We would like to thank all Priority Group 2 and Expert group members who have contributed to the preparation of the Report. Whilst we recognise that it was not always possible to achieve a full consensus on all matters discussed in the Report, care has been taken to ensure that all views were heard and discussed and whenever possible reflected in it.

Appendix 2:
Dissenting opinions from
members of the expert group

Opinion on the eID/KYC Expert Group Priority subgroup 2 report

Overview

This paper references a joint position supported by the expert contributors to the eID/KYC group from the eIDAS Cooperation Network. The member states supporting this position are Belgium (BE), France (FR), Luxembourg (LU), the Netherlands (NL) and the United Kingdom (UK).

We would like to thank the leaders and active members of sub-group 2 for their hard work and provide the following opinion in the spirit of collaboration as we strive towards a more unified approach to eID across the public and private sector.

Scope of work

During the second meeting of the eID/KYC expert group, the scope of work of priority subgroup 2 has been defined as follows:

- 1. An opinion on the need for, and the scope of, a framework for portable KYC/CDD solutions in particular in the banking sector. The opinion should consider key challenges/obstacles (e.g. liability framework) building on the eID interoperability framework with additional sets of attributes in order to enhance the usability of portable remote KYC/CDD solutions*
- 2. To assess the necessary minimum set of attributes necessary for CDD purposes in the banking sector and the appropriate level of assurance as per eIDAS (high, substantial and low) vis-à-vis various sets/types of attributes relevant for the KYC/CDD processes*

In our view, the deliverable does not match these outcomes:

1. The deliverable is not an “*opinion on the need for, and the scope of, a framework for portable KYC/CDD solutions*”, but an actual proposal for such a framework. As such, the deliverable lacks an analysis of the desirability/feasibility of such a framework, of the associated expected benefits / disadvantages for the banking sector, and of the possible/desirable scope of such a framework. For instance, the deliverable assumes that it is both desirable and feasible to define levels of assurance for every single attribute, as well as a minimum level value for onboarding purposes.
2. The deliverable fulfils the second expected outcome by providing a list of necessary attributes for CDD purposes. However, it goes beyond this objective, by also proposing a:
 - framework to assess levels of assurance, including for identity attributes of natural and legal persons
 - method of assessing level of assurance that varies dependent on where information

derives from

- taxonomy of natural persons associated to a legal person, including criteria for reaching levels of assurance
- level of assurance framework for how often attributes should be re-checked
- framework for level of assurance of identity providers
- new terminology for existing roles in the digital identity market
- minimum acceptable requirements for accepting each type of attribute that are proposed to be required across the EU

Instead of such a large scope, we would have preferred priority group 2 to focus on a smaller scope of work, but better researched and explained in more detail.

Aside from this, we take an opinion on the content of the work completed. Rationale and suggestions for alterations are discussed in this document.

Approach to references

The report does not include a list of references, but we understand that the authors have created most of the components of the report and not reused existing standards, which is a very challenging task considering the breadth of topics and the size of priority subgroup 2.

A preliminary survey of existing standards and EU related work could have identified interesting material to reuse for this deliverable. In our opinion, the report sometimes lacks clear explanations and justifications for the decisions taken.

We suggest to the Commission that they identify existing standards, studies, and activities which could support the creation of or rationale for a portable KYC/CDD approach.

General Data Protection Regulation (GDPR) compliance

The Commission Decision of 14 December 2017 established the eID/KYC Expert Group and mandates that the work of the group “*complies with Union data protection laws*” and is “*in line with the Union anti-money laundering Directive (EU) 2015/8492*”. However, we see no explanation in the report as to how the proposed framework complies with or allows for compliance with GDPR and AMLD. Each financial institution needs to be able to justify why it needs certain attributes. Unfortunately, in some places the approach in this report prohibits this. We understand that the authors only considered the “*overall objectives*” of the AMLD and not the actual Directive - we question this interpretation and suggest an assessment of the compliance of the report’s proposals with GDPR and AMLD.

Harmonisation as an approach

The proposed framework has been created with EU-wide harmonization in mind. The exception

to this is a line that allows deviations to the proposed framework when:

- justified by objective factors
- limited in scope
- applicable both to domestic financial services providers and EU financial services providers offering cross-border services to customers located in the relevant country

No justification is given for this choice of criteria. A preliminary analysis would have been useful to establish what can and should be harmonized, and what is best left to individual risk-based approaches, instead of standardizing everything and allowing deviations afterwards.

We struggle to see the benefits of attempting to enforce harmonisation, but also allowing deviation, which in our opinion will result in continued fragmentation. This is because the concept of harmonisation across member states is in some cases technically and legally unfeasible as a result of different approaches to identity by member state, different rules on access and storage of data and different risk appetite. Harmonisation would have to occur at this level, before it could be made possible for Know Your Customer checks. This is an approach that removes member states right to set their own rules and processes and we subsequently suggest instead:

- to assess the feasibility and desirability of a common EU KYC/CDD framework, to better scope the extent of what should be harmonized and what should be left to a risk-based approach
- to consider an inclusive framework that all member states can adhere to and that allows for alignment between varied approaches to KYC across member states
- to consider how eID and eIDAS could be utilized as a basis for creating harmonisation or alignment between member states

Attributes required for KYC/CDD purposes

It has been explained during KYC expert group meetings that the selection of attributes in the proposal for portable KYC/CDD is based on the attributes found in the PwC study. However, contrary to the PwC study we find that the working group 2 report adds without rationale or explanation:

- **gender** as a mandatory identity attribute. We understand that the proposal follows ICAO 9303's approach, under which the value can be set to 'X' when an attribute provider does not want to specify a value. Therefore, it is in practice an optional attribute and we suggest specifying it as such.
- **place of birth** as mandatory attribute. This attribute is optional under eIDAS, and unless there is a specific reason to ask for it, we suggest removing it from the mandatory dataset and set it as optional as it is not available in every member state
- that a **photo** must be extracted from documents and sent to the bank for any onboarding process at level of assurance Substantial or High. The framework does not distinguish between onboarding conducted with eIDAS versus without (for example, based on NFC). Therefore, there is no separation between when a photo should or shouldn't be removed

from the system. The photo should only be used for onboarding purposes and if that process is already done by relying on a prior identification process, then it should be removed from the system. The current proposal set an expectation that banks should always store and exchange facial biometrics.

- **mobile phone number** and **email address** as mandatory contact attributes. We note that both PwC and the Connecting Europe Facility (CEF) studies have concluded that the mobile phone number was not required for identification and KYC purposes, based on their study of common practices in the financial sector. We are also aware that not all Europeans have these attributes or wish to share both. To prevent the introduction of greater exclusion for citizens we suggest removing both from the mandatory dataset and setting them as optional.
- **tax residence** as a mandatory status attribute. Out of 17 financial institutions interviewed by PwC and CEF, only 3 of them use this information. As this does not seem to be a common practice, we suggest removing this data from the mandatory dataset and setting it as optional.
- introduces a **bank account code** in the list of “Identifier attributes”, which however is not in the list of allowed “individual’s identifiers” in the Core ID set of attributes, so we don’t understand its purpose.
- mandatory attributes for **legal persons**. It is not clear why the proposal suggests mandating both a “registration number” and a “company’s identifier”. The proposal restricts the list of “company’s identifier” to a few possible values, which does not account for variation across member states or attempt to standardize company identifiers. We suggest reviewing this shortlist or considering standardization of company identifiers, as has been done for individual user identifiers under eIDAS.

A common observation is that these additional attributes take a very maximalist approach towards all the attributes enumerated in the PwC and CEF studies. We question the alignment of this approach with GDPR’s principles of data minimisation and purpose limitation.

We recommend that the list of mandatory attributes should be as small as possible to leave flexibility for banks to collect (or not) additional attributes as part of their risk-based approach, so that they are in a position to be able to consider data minimisation under GDPR. In particular, deviations from the common practices of the financial sector as described in the PwC and CEF studies should be carefully justified.

The list of attributes should also be eIDAS compatible, especially regarding the unique identifier. To help with this, we suggest that specific consideration be given as to whether eIDAS can provide the necessary attributes for KYC and if not, or if more attributes are required in addition, consider how best to adapt to cater for this, for example by using eIDAS and the single digital gateway.

Level of Assurance for each attribute

The deliverable assumes that it is both desirable and feasible to define levels of assurance for every attribute separately, as well as an associated minimum level for onboarding purposes.

We question if banks need a range in level of assurance for all attributes and whether each attribute should be considered separately. Under conditions where some attributes can be checked less but ranked equally do a more thorough check on a different attribute, we feel this opens up confusion and potential security weaknesses, as there may be assumptions made that an attribute can be better trusted than it should. It also leads to a requirement to list every possible attribute, with some attributes used in specific member states being left off accidentally. We do not feel it is possible to list every attribute and recommend a more holistic approach to assessing the trust that can be placed in data, which covers a range of attributes. The legal, organisational and technical complexities imposed by an attribute specific approach are also considerable and not considered within this report.

We also feel the report needs to reflect in more detail why the criteria for what makes a given level of assurance has been chosen. For instance, more detail is needed on what makes a source trusted. The criteria used for assessing trust in attributes (with the exception of the coreID suggestions) solely looks at where the attribute is from and how it has been transferred. However, we strongly feel that other factors play a role in how much an attribute is trusted, for example how well it is bound to the identity to whom it claims to relate and how well the organisation that is storing it looks after its data to prevent tampering.

As the deliverable does not demonstrate the need for individual levels of assurance for identity attributes, we suggest using the approach of a non-specific quality assessment framework for all attributes. This would, therefore, encompass the additional attributes often required for KYC on top of the minimum dataset provided through eIDAS. Moreover, we suggest reflection on whether all information can be ranked by level of assurance and which data can be passed as simple additional data, for example, email. An alternative approach could be to provide advice on what financial institutions should take into account when assessing the quality of an attribute, rather than providing levels of assurance.

Core identity attributes

The report builds a level of assurance framework for identity attributes remotely extracted from identity documents. However, core identity attributes can already be assessed as a collective under the eIDAS regulation. There are different requirements for assessment of these core identity attributes under the newly proposed framework. Subsequently, this proposal overlaps and, in some places, contradicts the work done under the eIDAS regulation (EU)2015/1502.

As an example, to reach levels CI-Low and CI-Substantial, the proposal allows either eIDAS' LoA-Low or eIDAS LoA-Substantial, or data which *"is not protected during its extraction and communication to the recipient"*. This contradicts the eIDAS requirements for LoA-Low, which in (EU) 2015/1502 requires measures *"protecting the confidentiality, integrity and availability of the information processed"*.

By establishing inaccurate equivalence between eIDAS levels of assurance and the new core identity attribute framework this proposal undermines the eIDAS regulation instead of building on it. It suggests that a review of eIDAS should be carried out to see how it should be iterated to broaden its scope rather than creating a new overlapping framework.

If this proposal is implemented and financial institutions begin exchanging eIDs under the newly proposed framework as if they are equivalent to an eIDAS level of assurance, it introduces security flaws by providing more confidence in the non-eIDAS identity than is actually achieved. This approach creates inconsistencies and is subsequently at odds with a standards-based ecosystem.

There is also a document agnostic approach currently taken to identity under eIDAS, which allows for different document types to reach a given level of assurance dependent on their security and how they are used to prove an identity. This proposal is document specific, allowing only for certain types of document to be used, thus excluding some member states from being able to practically meet the requirements. There are also some direct contradictions in the report between what documents should be allowed and recommendations by the PwC report. Finally, there are some inaccuracies in processes defined as secure.

We suggest the removal of the core identity attributes framework. We recognize that alternative solutions to eIDAS can be used for proving one's identity in a KYC/CDD framework. However, these solutions should be based on proven standards and developed by identity experts. Where equivalences with existing standards are drawn, it is vital that these reflect true equivalence. This allows for organisations to understand fully the trust that can be derived from given attributes or identity proofing processes. Subsequently, the right compensating measures can be used when needed to increase trust. For example, adding additional transactional monitoring when less identity proofing has been carried out.

Implementation proposals

Proposals for legal and regulatory implementations of the framework raise some concerns:

- “*generally relate*” levels of assurance to the type of source an attribute provider is - this is legally vague and goes against the standard approach of a level of assurance based framework. The source of an attribute is but one of the parameters used to establish a confidence level, and all parameters should be met within a framework. General relation according to one factor does not allow for a level of assurance to be met. We also feel that a financial institution would generally consider all these factors and decide who it trusts, then have a supervisory body assess these decisions, rather than accepting a given attribute provider as assured, so this approach may be impractical. We suggest removing this proposal.
- require that “*Member States having notified a Substantial or High LoA eID eIDAS scheme make sure that Substantial and High LoA eIDAS eIDs can be accepted by financial service providers as part of their onboarding processes*” - this requires more unpacking to assess its feasibility. For example, what are the criteria for a Member State to fulfil such an obligation towards the private sector and why should this proposal be conditioned by a notification, as under eIDAS, notifications are not currently related to the obligation of accepting eIDs. We suggest adjustment of this proposal to reflect a suggestion to the

eIDAS Cooperation Network to consider what new requirements might be legally and operationally viable to make it more usable for financial institutions.

- require that AML regulation states national authorities must *“give financial institutions and other regulated entities direct access to selected databases for the purpose of implementing KYC processes”* - this intervenes with national security protocols across member states. We recommend that each member state decides the level of access that can be granted to state databases, particularly of personal information, dependent on the situation, risk and national appetite to do so. We understand that financial institutions would like support from national authorities to fulfil their AML obligations, however, such collaboration can be implemented in various ways. Therefore, we suggest asking more broadly for stronger collaboration between public and private sector to the extent of what is legally feasible.
- Recommendations for updates to the eIDAS regulation - some of the proposals are currently unsubstantiated or inaccurate, for example that eIDAS should be aligned on NIST (it currently is). We suggest reviewing this list of suggested eIDAS legal/regulatory improvements in order to make corrections and ensure they are legally and operationally feasible.

Commission expert group on electronic identification and remote Know-Your-Customer processes

Written procedure for the endorsement of the Priority Group 2 report (“Attribute based and LoA rated KYC Framework for the financial sector in the digital age”): dissenting opinion from expert of Bank of Italy.

Priority group 2 tried to export the logics laying behind digital identities systems into the CDD sector. However, this attempt is flawed for the following reasons.

Digital IDs and CDD

As underlined during the meetings of the working group, digital identities are a substitute of physical documents and their use can highly simplify and smoothen up customers’ identification process, mainly where they operate remotely. In any case, digital identities can be useful only:

- 1) to identify and verify the customers i.e. to fulfil two of the four steps composing CDD requirements;
- 2) if the customer is a natural person, since no information about the beneficial owner is embedded in digital IDs.

It is also important to recall that, since digital IDs are generally issued by private firms, their reliability stems from the fact that those firms are licensed and supervised by national competent authorities, in compliance with EI-DAS regulation. On top of this, in some countries (Italy among them) only digital IDs with high LOA can be used for CDD purposes.

The proposal of the Priority group 2

Against this background, priority group 2 mapped the key attributes used for distance onboarding purposes in the various Member States in order to create, for a given financial service, a table (Minimum Viable e-KYC Framework) linking the key attributes used for distance onboarding purposes to commonly agreed Levels of Assurance (LoAs). For CDD attributes not embedded in digital IDs (for instance, source of funds, pep status, occupation etc.) the report proposes to set a minimum acceptable LoA for each attribute.

In this regard, during the expert group meetings, I had the opportunity to underline that:

- unless a regulatory and supervisory regime similar to the one in place for Ei-DAS is set-up, it would be very difficult to assess the reliability of the subject providing CDD attributes other than those embedded in digital IDs;
- some attributes (for instance, the source of funds) are very specific and can largely vary from business relationship to business relationship. These attributes cannot be standardized once and for all. The same goes for the “*purpose and intended nature of the business relationship*”, the 3rd component of the CDD.

In general, I fear that moving along the lines suggested by the Priority group 2 could legitimized the increasing trend aimed at reducing CDD to a “tick the box” exercise where obliged entities are only required to retrieve information from a (reliable?) data hub without carrying out their own analysis. CDD is more than this: its proper and tailored fulfilment is crucial to ensure the functioning of the entire AML sector. The entire proposal seems to be conducive to the development of a KYC utility market mutualizing KYC processes.

For the reasons illustrated above, I do not endorse the above mentioned report and, where approved, I please ask to attach this document providing my dissenting opinion to the report.



20 December 2019

Anti Money Laundering

Unrestricted

Expert group on electronic identification and remote KYC processes Dissenting opinion in relation the Priority Group 2's report

First of all I would like to say that I appreciate the work that was done in Priority Group 2 in relation to the need for and the scope of a framework for portable KYC/DCC in the banking sector. The report provides fresh ideas and interesting aspects on the topic.

However, there are still some parts, which would benefit of further discussions. In my opinion not enough attention was paid to the way the risk-based approach should be taken into account in the remote KYC processes and issues relating to identifying beneficial owners. I would also suggest that further discussion is carried out on the feasibility and potential content of the EBA RTS or Guidance.

I believe that the report provides new aspects and valuable information for the European Commission in its work on harmonizing the electronic identification and remote KYC processes. However, in my opinion further discussions would be needed before the report could be endorsed.

FIN-FSA

Dear eID/KYC Secretariat,

Unfortunately, I was not able to complete the survey before 12:00. Hence I hope that emails will be accepted for the endorsement procedure.

As expert of the French supervisor ACPR, mandated to the expert group by the EBA, I endorse the two reports, with two comments about specific aspects of report 2.

In report 2, the ACPR would prefer if the “gender” core ID attribute for individuals (p. 25 of the report) was removed or at least made optional, since its implementation seems unnecessary difficult.

Similarly, we don't think the contact attributes (current address, mobile phone or email address) should be made mandatory for KYC matters. They should be optional and subject only to a low level of insurance, since they are not necessary for identification per se, but only for communicating with the client of the obliged entity. The obliged entity should be free to use any mean of communication with its clients, as restricting these means too much could lead to a potential discrimination towards people who do not have an internet access for instance.

Kind regards,



Secrétariat général
Autorité de contrôle prudentiel et de résolution
4 place de Budapest
CS 92459
75436 Paris cedex 09

Bundesministerium der Finanzen, Germany

Priority Group 2 - Final report Priority Group 2's mandate was to provide an opinion on the need for, and the scope of, a framework for portable KYC/CDD solutions in particular in the banking sector. The opinion should consider key challenges/obstacles (e.g. liability framework) building on the eID interoperability framework with additional sets of attributes in order to enhance the usability of portable remote KYC/CDD solutions. We take note of the opinions issued by experts pertaining to Priority Group 2 and believe that the criticism raised with regards to the mandate of the Group and the suitability of the proposed framework in the report has merit. Nevertheless, we believe that in line with the Council Conclusions on AML from 5 December 2019 we should continue to strive towards greater harmonisation of the European framework for remote KYC/CDD. Therefore, we would like to recognise the contribution that the report as well as the opinions issued by the experts have made towards further efforts to achieve this objective and to allow for a well-informed discussion process in the year ahead. We would also like to highlight some particular concerns which we have remaining with regards to the final text, following the incorporation of the majority of previous concerns raised in the extensive commentary provided to the authors of the report.

The report suggests a customer identification approach which includes gender as a mandatory attribute. This goes beyond the eIDAS guidance and is not aligned with the German domestic framework. If applied, it would prevent German state-issued eIDs notified as "high" and guaranteed to ensure the unique identification of an individual with the given attributes from being fully compliant with identification requirements. With regards to this, the German delegation has pointed to EU-regulation 2019/1157 which deviates from the ICAO document and recognises gender as an optional attribute.

In addition, the report presents some customer identification solutions that are not compliant with eIDAS (e.g. remotely presenting identification documents). The report states an objective for these to be as closely aligned with eIDAS requirements as possible. However, we do not think that this provides sufficient assurance over the security of and consistency across the proposed solutions.

