KYC Portability
Distant dream or near future?

The EU Commission Expert Group eID/KYC

Stéphane MOUY
BNP Paribas

GLOBAL CLIENT ONBOARDING FOR ASSET MANAGEMENT
17th January 2019

…KYC portability is more like an ascent

And we are not yet there…

KYC portability is highly desirable…
… but not a reality in most EU countries

Reasons

- **KYC still mostly viewed as a paper-based process**
- **Lack of multi-sectorial digital identities**
- **Liability framework not consistent with a distribution of KYC roles (KYC provider and KYC relying party)**
- **No common approach for KYC requirements across EU members : additional factor limiting the cross-border deployment of onboarding processes**

However :

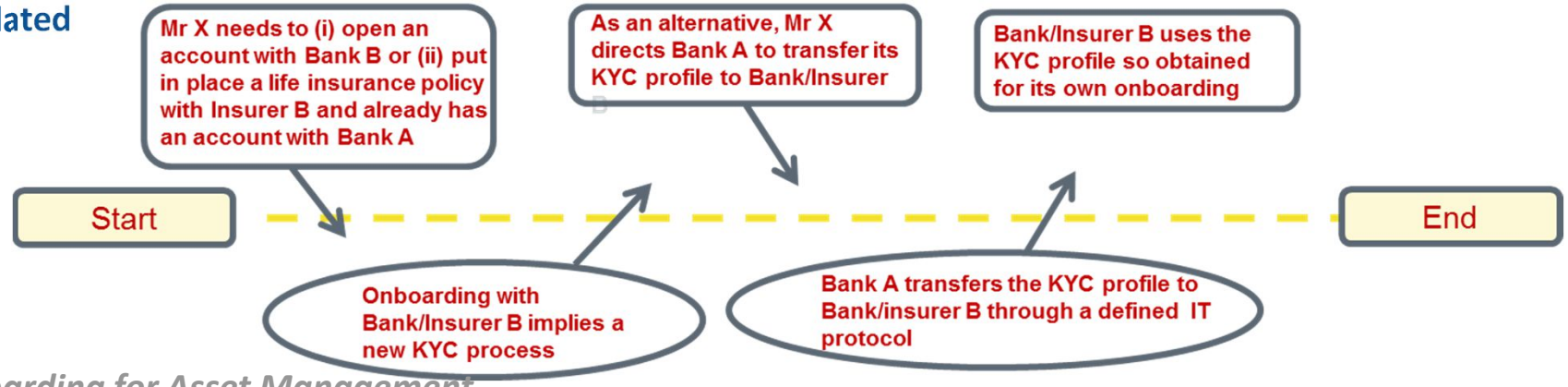
- **GDPR – Portability right (art. 20)**

  "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance […] where (a) the processing is based on consent or contract […] and (b) the processing is carried out by automated means"

- **The current system is fraught with problems and costly for the financial industry**

  Huge pain point for customers and banks alike

Use case contemplated



When 5AMLD meets eIDAS
KYC Regulatory Impact

eIDAS Regulation (EU 910/2014)

Digital Single Market

Interoperability framework for electronic Identification Schemes

Quality levels (LoAs)

Trust Services

Customer due diligence measures shall comprise:

a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation EU 910/2014 or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities

(art. 13.1 5AMLD)

5AML Directive (EU 843/2018)

Interconnected Central Registers

Recognition of eIDs for AML purposes

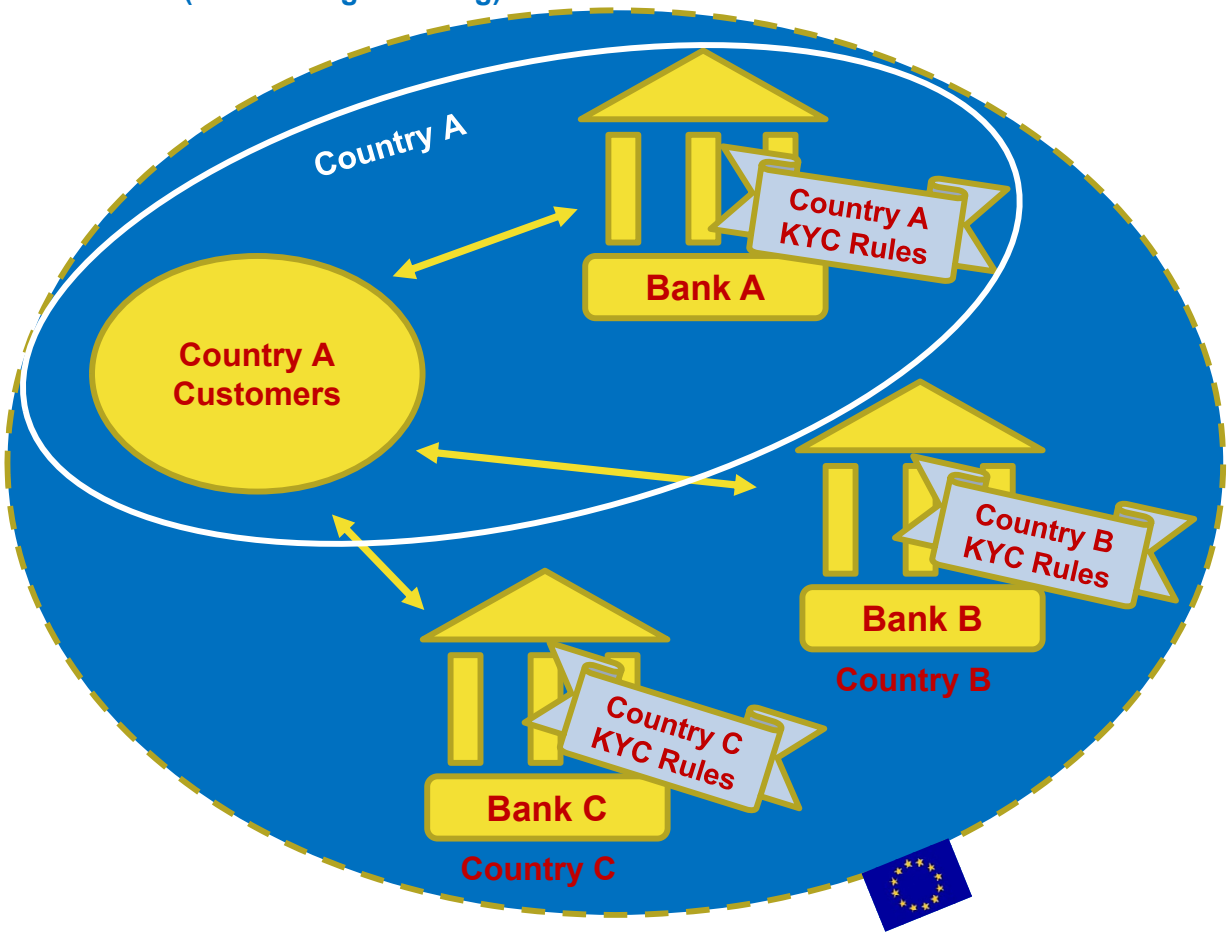
Integration of virtual-currencies and custodian wallet providers

Outstanding issue
Impact on digital single market

Considering cross-border use
A fragmented approach is problematic

A growing dilemma…

On the one hand….The growing availability of digital identities and remote on-boarding techniques greatly facilitate the cross-border deployment of financial services within EU Member States (which is a good thing)



But…. The near complete freedom left to Member States to define KYC requirements raises level playing field concerns and opens up regulatory arbitrage opportunities

5AMLD leaves considerable discretion to Member States to define KYC processes

No minimum quality requirements are set at EU level, leaving each Member State to set its own approach for customer identification

More broadly, KYC rules apply to the service provider, not the customer, leading customers in a given country having their financial transactions subject to different KYC rules

- Some countries recognise digital identities for financial on-boarding processes, others not;
- Some countries recognise video identification, others not;
- KYC attributes vary significantly from institution to institution.

This situation contrasts with the one applied in the physical world for passports (ICAO 9303 standard)

The EU Commission eID/KYC Expert Group

Decision

- **Commission decision of 14 December 2017**
- **3 DGs involved : FISMA, JUSTICE & CONNECT**

Mandate

- **Address digital onboarding processes for the financial industry**
- **Focus on cross-border transactions and identify applicable constraints and obstacles**
- **Propose interoperability solutions for remote onboarding and portable KYC processes**

Composition

- **35 members – o/w banking experts, regulatory authority representatives, IT experts and consumer organisation representatives**

Where we are so far : 2 streams

- Mapping of existing remote on-boarding solutions
- Creation of an attribute-based LoA-rated eKYC framework

Proposal currently discussed – a 'Minimum Viable' eKYC framework

Further work still needed

The rationale for a common eKYC framework (1/2)
Where do we start – where do we go?

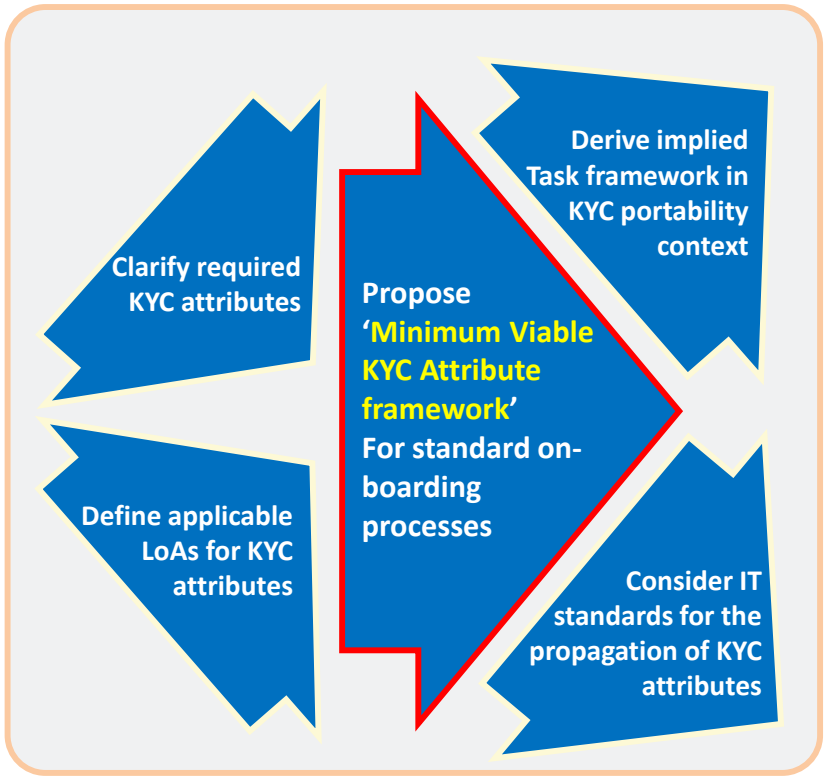
Key considerations

- We are far from a digital single market : How do we deal with a fragmented landscape?
- How should innovative on-boarding solutions be recognised?
- How do we provide a level playing field for service providers?
- How do we facilitate KYC transfers & KYC mutualisation?

Early consensus on the following

- A common standard is needed
- Focus on individuals rather than corporates
- Identify KYC attributes and related LoAs
- Propose a 'minimum viable' framework
- Address liabililty implications upfront

Where to start in practice?



First assessment : the major hurdle does not appear to be on the technology side – solutions are available

The rationale for a common eKYC framework (2/2)
Where do we start – where do we go?

Applied approach : aiming for a concrete proposal with an operational end-result in mind

Start small – with a single use case applying to individuals

Focus on standard situations – complex or higher risk situations (enhanced due diligence) to be considered later

Cross-border use in mind – Key element towards lowering intra-EU barriers and ensuring a level playing field in retail banking

Addressing the fragmentation of the EU onboarding landscape is a priority

Focus on 'Minimum Viable' specifications

'Minimum-Viable' means

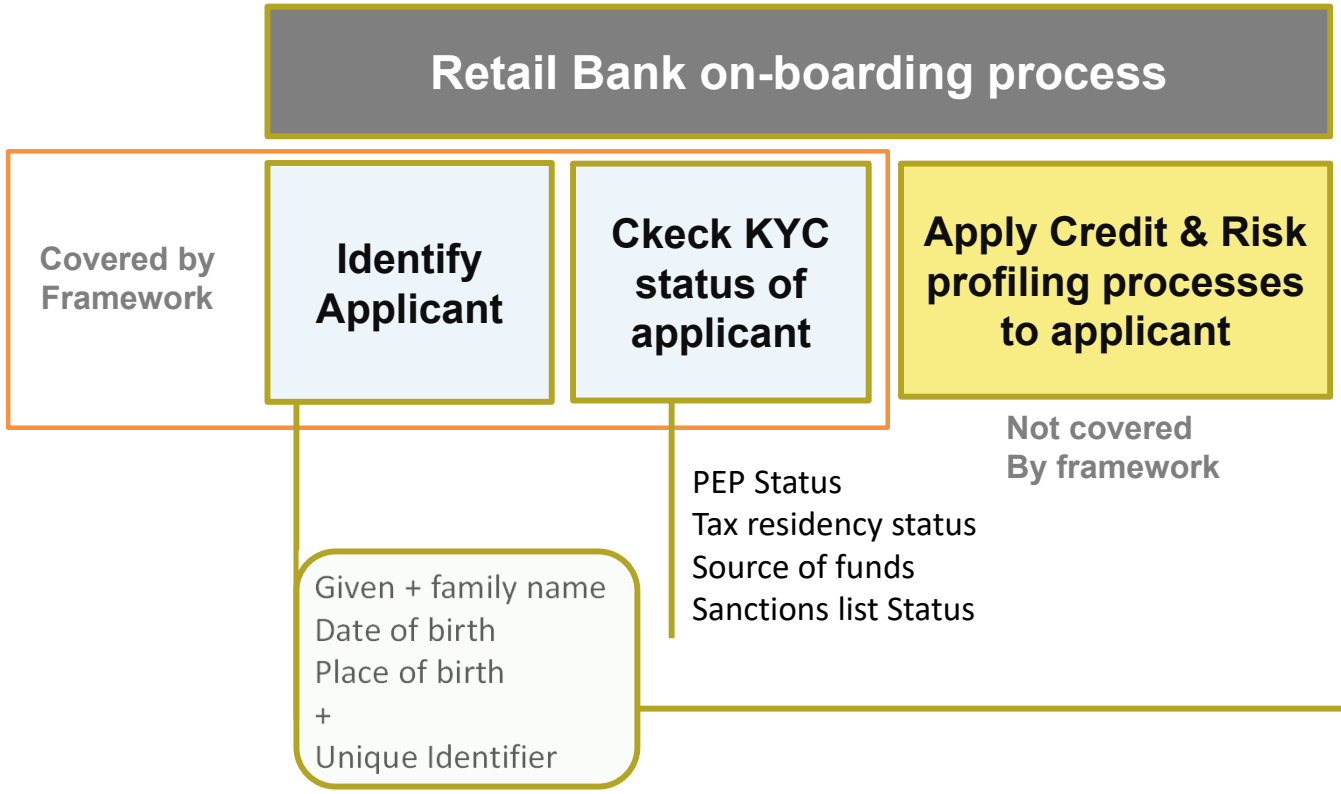
- A common standard applies with minimum requirements set for regulatory purposes
- The standard does not aim to cover all on-boarding aspects
- But financial institutions are always in a position to require more attributes and/or higher LoAs, especially for credit-related and fraud-prevention processes

Key benefits

- Standard approach offering consistency, visibility and predictability
- Greatly facilitates the transferability of KYC attributes – key step towards KYC portability and the emergence of industry-wide KYC providers
- Can be easily packaged into existing IT protocols

'Re-use' approach : Minimum Viable Framework builds upon existing contributions

eKYC framework proposal explained (1/5)
Identify key attributes and establish LoAs



CEF Eid Building block - Architectural Solution Document (March 2018)

Identifies key KYC attributes for EU financial institutions

Core ID attributes

- Communicated as part of digital identities
  - eIDAS LoA Framework applies
- Extracted (remotely) from physical ID documents
  - Need to offer a LoA approach
  - Proposal based on ID document types & extraction robustness method

New territory

Applies PwC report ID document classification to LoAs
ID document types 1, 2, 3 & 4 are considered

The PwC Study on eID and digital on-boarding (April 2018) offers a classification for ID documents

- Type 1 : physical document not machine-readable
- Type 2 : physical document machine readable
- Type 3 : physical document machine and electronically readable
- Type 4 : 'logical' document implemented in digital media only

eKYC framework proposal explained (2/5)
Determining Core ID LoAs

DOCUMENT IDENTIFICATION REQUIREMENTS	LOW	SUBSTANTIAL	HIGH
REQUIREMENTS	Type 1, 2, 3 or 4 ID document Capture of full ID Data Capture of ID Photo ID Data within validity period	Type 2, 3 or 4 ID document Capture of full ID Data Quality capture of ID Photo MRZ data checks ID Data within validity period Verification of loss/stolen document database (when available)	Type 3 or 4 ID document Full electronic extraction of ID data (including photo) ID data within validity period Verification of loss/stolen document database (when available)

LIVELINESS DETECTION \ DOCUMENT IDENTIFICATION	LOW	SUBSTANTIAL	HIGH
LOW	CORE ID LOW LoA	CORE ID LOW LoA	CORE ID LOW LoA
SUBSTANTIAL	CORE ID LOW LoA	CORE ID SUBSTANTIAL LoA	CORE ID SUBSTANTIAL LoA
HIGH	CORE ID LOW LoA	CORE ID SUBSTANTIAL LoA	CORE ID HIGH LoA

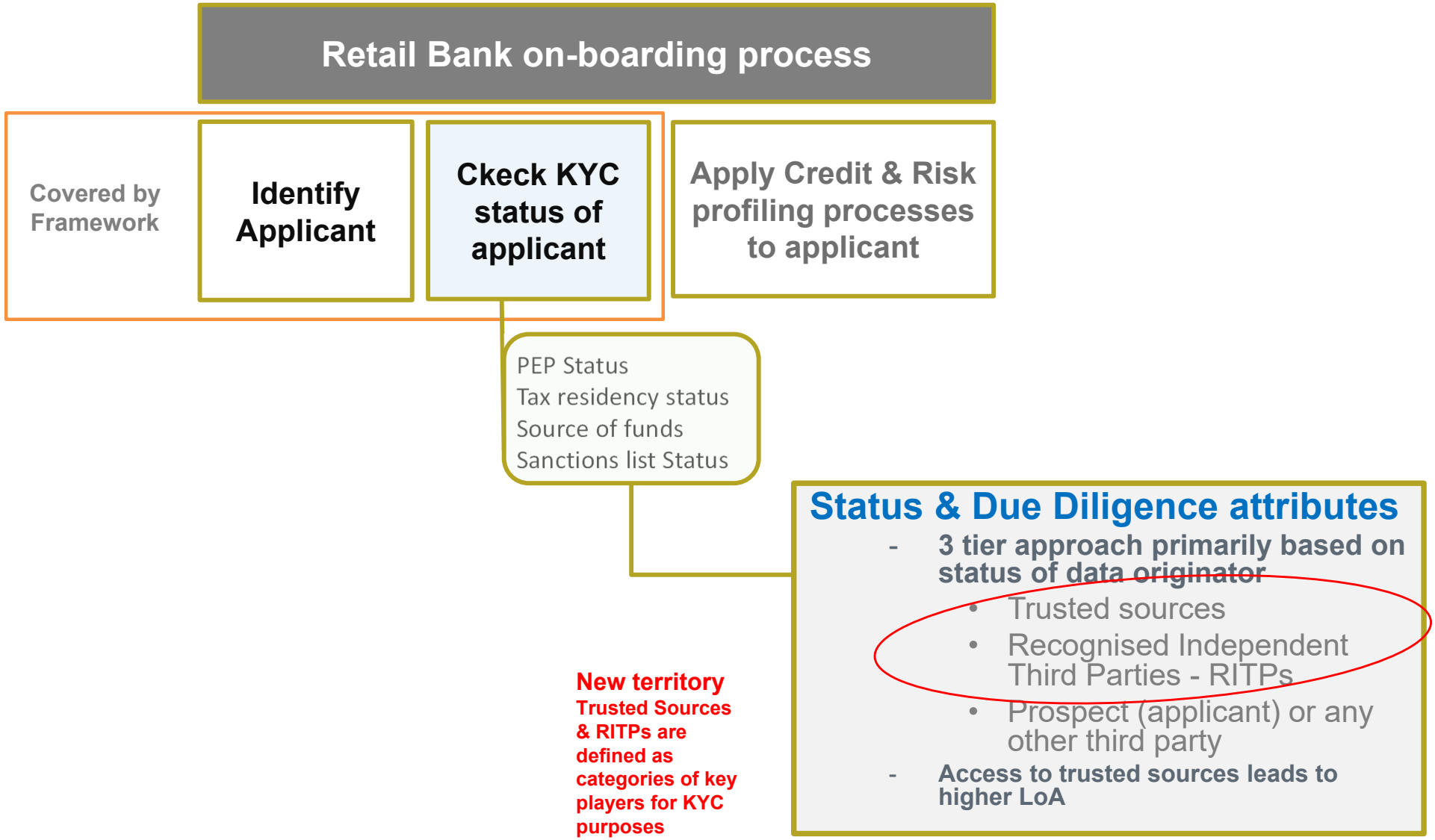
LIVELINESS DETECTION REQUIREMENTS	
LOW	No liveliness detection implemented
SUBSTANTIAL	Liveliness detection implemented but NOT meeting low false-negative score threshold
HIGH	Automated liveliness detection implemented meeting or exceeding low false-negative score threshold

Selfie screenshot

Proposal for consideration (draft)

Low LoA – Not acceptable
Substantial LoA – Acceptable
High LoA - Excellent

eKYC framework proposal explained (3/5)
Identify key attributes and establish LoAs



eKYC framework proposal explained (4/5)
LoAs for Status & Due diligence attributes

KYC ATTRIBUTE LOA FRAMEWORK	DATA AUTHENTICITY & INTEGRITY		
	UNPROTECTED during extraction and communication phase		PROTECTED during extraction and communication phase
Data originator	Attribute directly received from the Data originator	Attribute received via the Prospect	All communication channels (including when transmitted via the Prospect or any third party)
TRUSTED SOURCE	HIGH LoA	LOW LoA	HIGH LoA
RECOGNISED INDEPENDENT THIRD PARTY – RITP	SUBSTANTIAL LoA	LOW LoA	SUBSTANTIAL LoA
PROSPECT AND OTHER THIRD PARTIES (other than RITPs)	LOW LoA	LOW LoA	LOW LoA

eKYC framework proposal explained (5/5)
LoAs for Status & Due diligence attributes

Applying the framework to attributes

Current address LoA

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

- Low : self-declaration or presentation of unprotected document showing the address
- Substantial : the address is directly confirmed by a public utility (e.g. electricity provider) or appears in a protected document issued by a public utility
- High : the address is directly confirmed by a local authority or appears in a protected document issued by a local authority

Example of protected document

eKYC framework proposal explained
The Minimum Viable approach – Onboarding use case

Attributes & LoAs can be presented in a table for a given on-boarding journey

ON-BOARDING JOURNEY CURRENT ACCOUNT OPENING BY INDIVIDUAL			
	LoA - Low	LoA – Substantial	LoA – High
Core ID attributes	NO	OK	OK
Status & Due diligence attributes	NO/OK	OK	OK

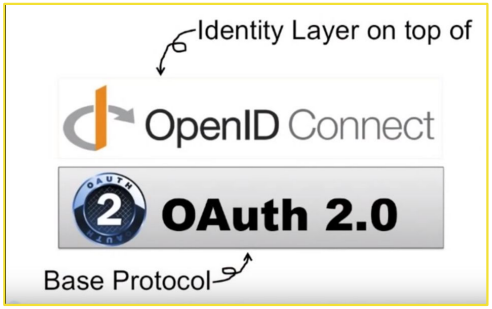
KEY BENEFITS

- Standard approach offering predictability and facilitating the deployment of industry-based solutions
- Level playing-field for financial services providers
- Defragmentation of EU onboarding landscape
- Can easily be packaged into existing IT protocols (including OpenID Connect)
- Greatly facilitates the transferability of KYC attributes – key step towards KYC portability

Propagating KYC attributes
The role of IT Standards

Two main alternatives
- Use the eIDAS nodes framework
- Use an existing IT protocol – OpenID Connect

OpenID Connect is the identity layer on top of OAuth.
Oauth is primarily an authorization protocol



It protects valuable resource (called Protected Resource) from unauthorized access using “access tokens”.

It is the protocol of choice for federated authentication and identity federation
It is supported by mobile carriers (Mobile Connect)
It is supported by many governments
UK Open Banking’s security profile is based on OpenID Financial-grade API Security Profile

Many vendors and open source products support it

It defines
ID Token (Signed JSON Web Token with identity claims)
Protocols to request specific claims/attributes at a specific assurance level
Higher security mechanism

JWT = JSON Web Token. RFC7519. The standard Token Format.

JWT has three variants: JWS, JWE, JWS+JWE.
JWS:= JSON Web Signature. JWT that is signed by the issuer’s key.

JWS is useful to store information as a signed token.

OIDC = OAuth + JWS+E(Identity)


Stéphane MOUY
BNP Paribas
Thank you for your attention
Global Client Onboarding for Asset Management
17 January 2019