DIGITAL KYC – A SHARED FUTURE?

The ‘Minimum Viable’ eKYC framework proposal
EU Commission Expert Group eID/KYC

Stéphane MOUY

BNP Paribas

MONEYLIVE

2018

If ‘identity is the challenge of our time’…

Todd McKinnon - Octa

Start here… (paper-based processes)

Go and aim higher… (interoperability, user control, data minimisation, etc..)

…KYC portability is more like an ascent

And we are not quite 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 :

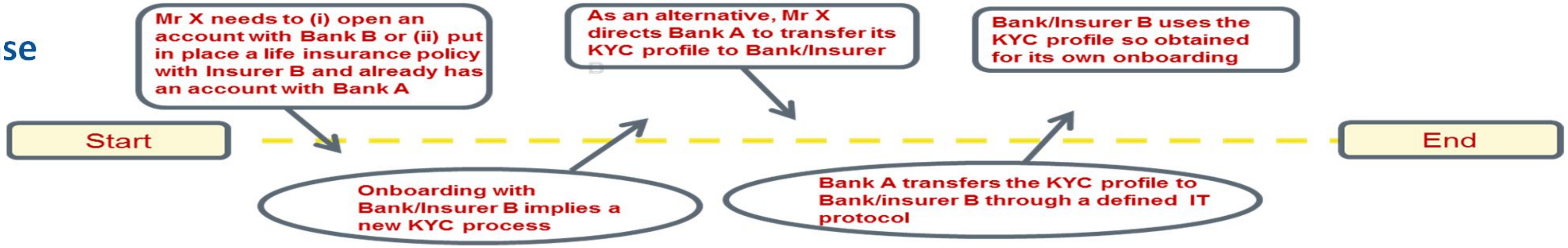
- GDPR – Portability right (art. 20)

  "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

Contemplated use case



Start

Mr X needs to (i) open an account with Bank B or (ii) put in place a life insurance policy with Insurer B and already has an account with Bank A

Onboarding with Bank/Insurer B implies a new KYC process

As an alternative, Mr X directs Bank A to transfer its KYC profile to Bank/Insurer B

Bank A transfers the KYC profile to Bank/insurer B through a defined IT protocol

Bank/Insurer B uses the KYC profile so obtained for its own onboarding

End

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 o

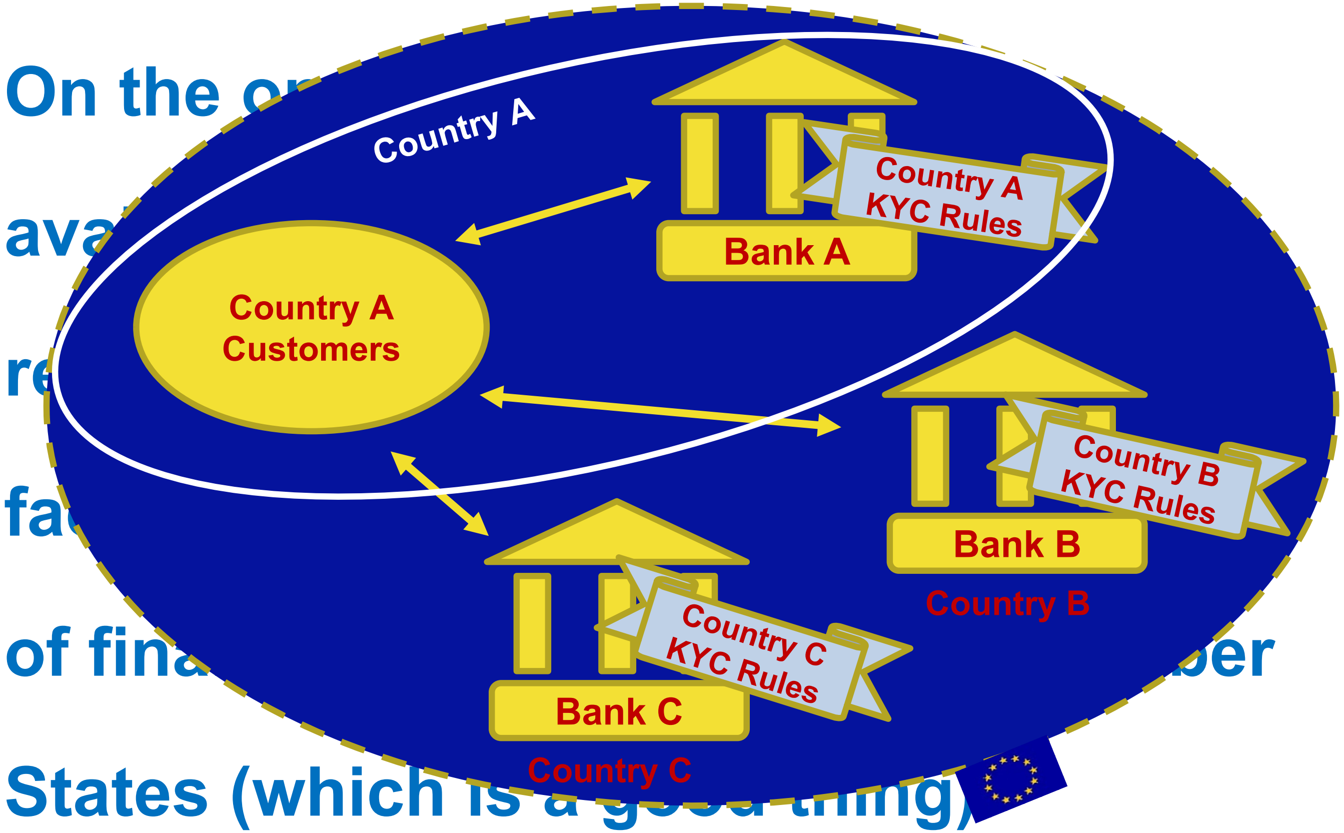
ava

re

fa

of fina ber

States (which is a good thing)



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 reps, IT experts and consumer organisation reps**

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

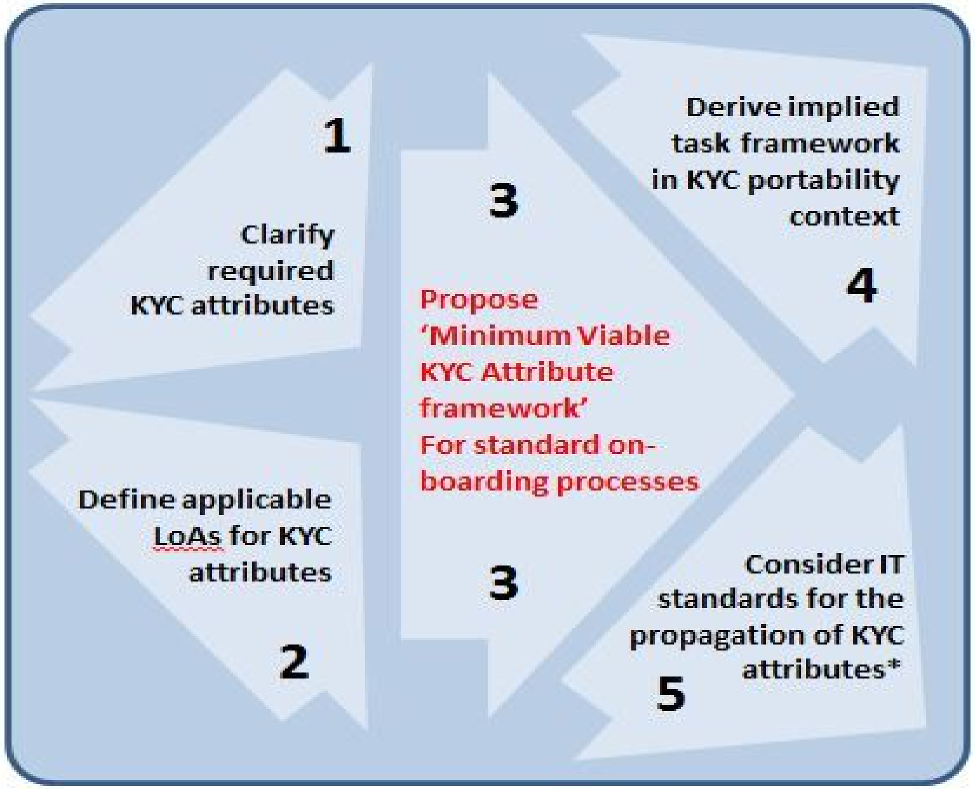
The rationale for a common eKYC framework

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


1
Clarify required KYC attributes
2
Define applicable LoAs for KYC attributes
3
3
Propose 'Minimum Viable KYC Attribute framework' For standard on-boarding processes
Derive implied task framework in KYC portability context
4
Consider IT standards for the propagation of KYC attributes*
5

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

eKYC framework proposal explained (1/5)
Approach followed

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

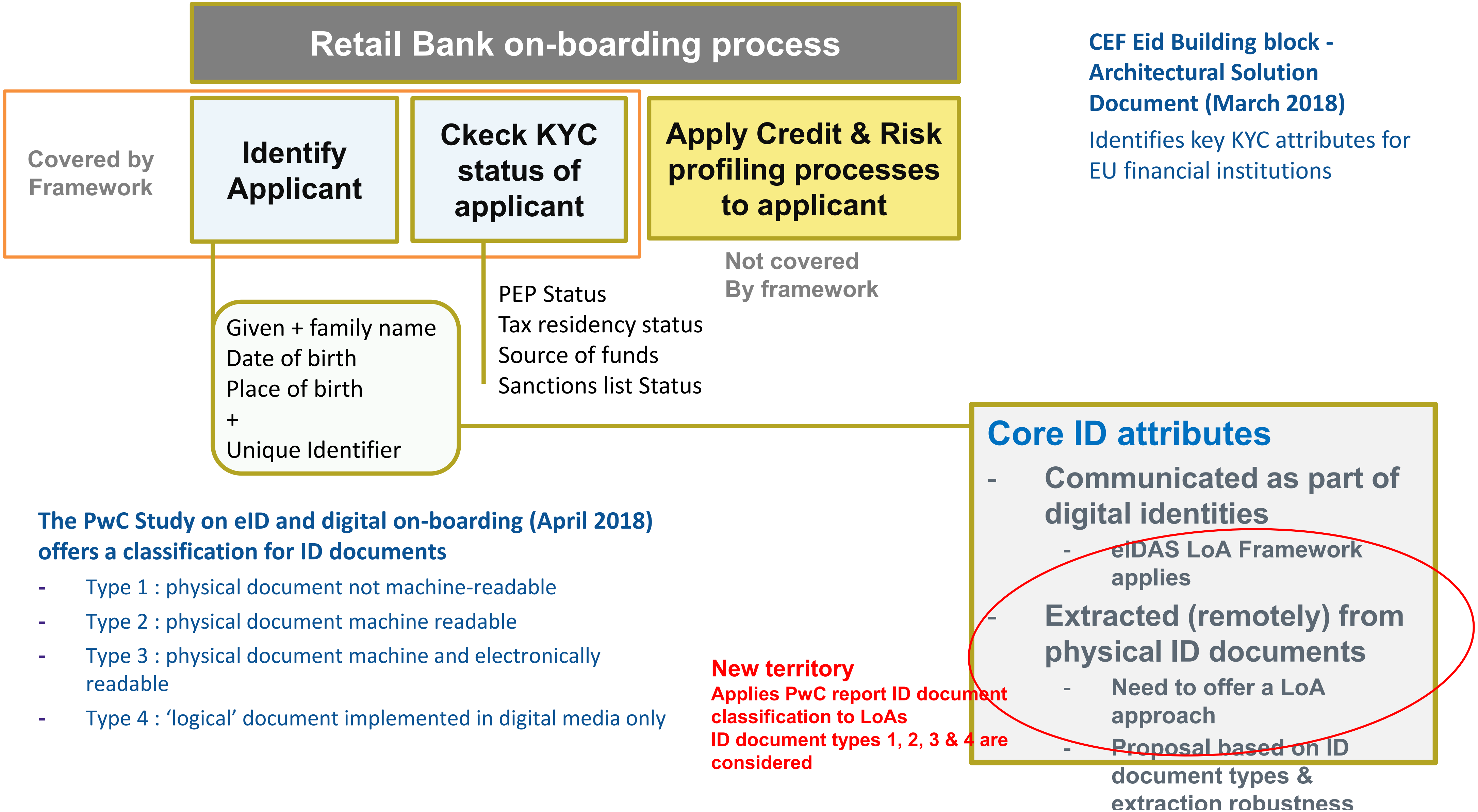
Addressing the fragmentation of the EU onboarding landscape is a priority

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

eKYC framework proposal explained (2/5)
Identify key attributes and establish LoAs



Retail Bank on-boarding process

Covered by Framework

Identify Applicant

Ckeck KYC status of applicant

Apply Credit & Risk profiling processes to applicant

Not covered By framework

Given + family name
Date of birth
Place of birth
+
Unique Identifier

PEP Status
Tax residency status
Source of funds
Sanctions list Status

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

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

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

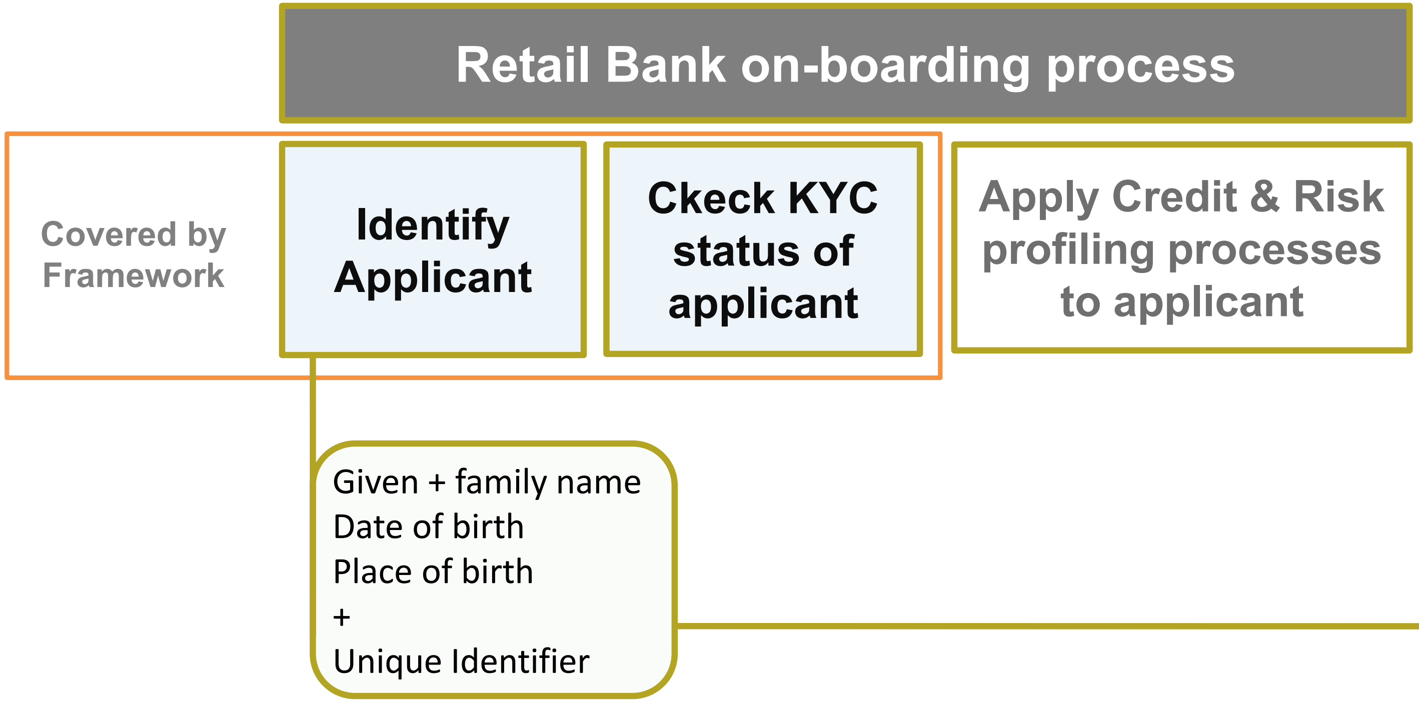
Identifies key KYC attributes for EU financial institutions

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 (3/5)
Core ID attributes

MONEYLIVE 2018


Retail Bank on-boarding process
Covered by Framework
Identify Applicant
Ckeck KYC status of applicant
Apply Credit & Risk profiling processes to applicant
Given + family name
Date of birth
Place of birth
+
Unique Identifier

Core ID attributes

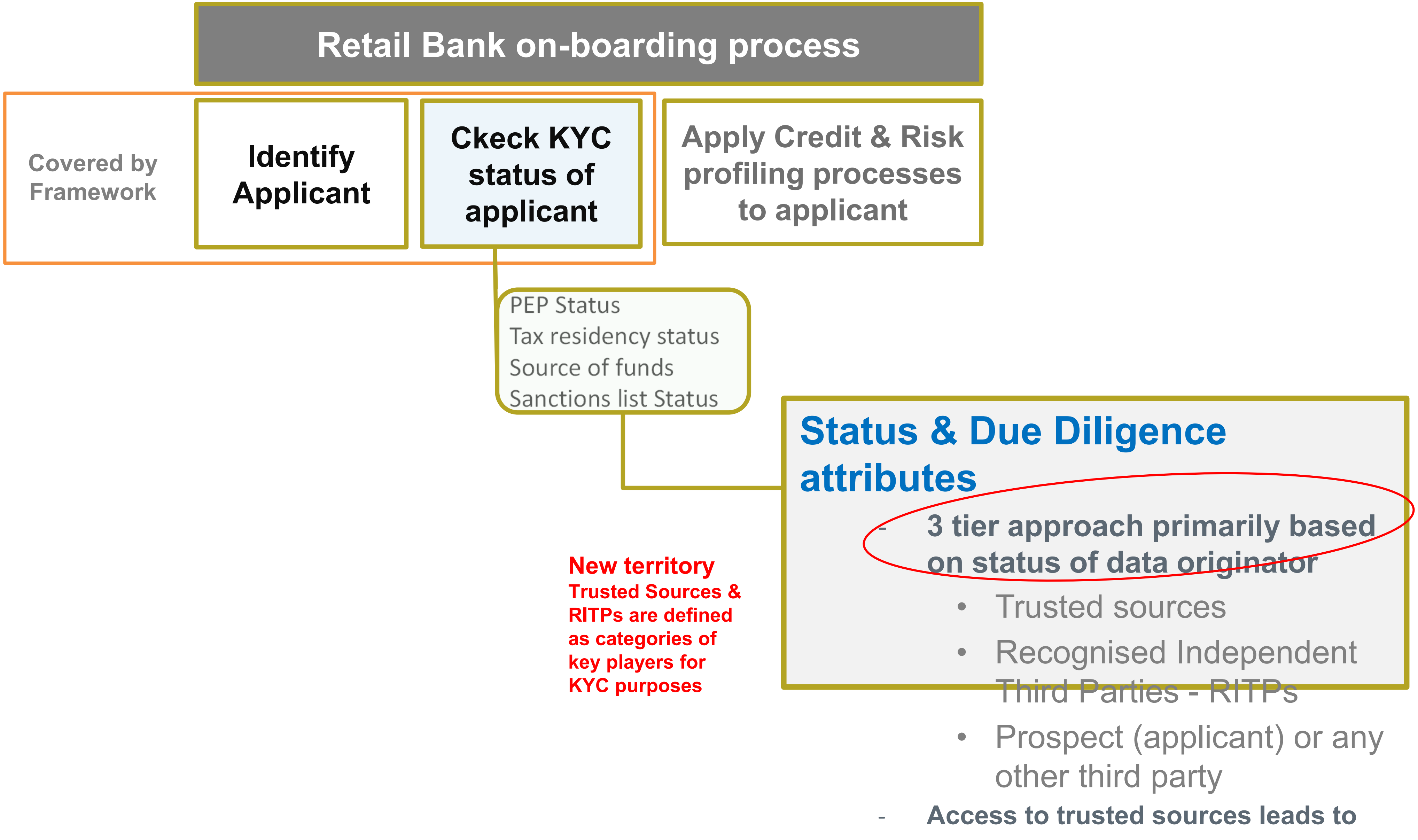
Attributes communicated through eIDs : eID LoA

Attributes remotely extracted from ID documents

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

eKYC framework proposal explained (3/5)
Status attributes



Retail Bank on-boarding process

Covered by Framework

Identify Applicant

Ckeck KYC status of applicant

Apply Credit & Risk profiling processes to applicant

PEP Status
Tax residency status
Source of funds
Sanctions list Status

Status & Due Diligence attributes

- 3 tier approach primarily based on status of data originator
  - Trusted sources
  - Recognised Independent Third Parties - RITPs
  - Prospect (applicant) or any other third party
- Access to trusted sources leads to

New territory
Trusted Sources & RITPs are defined as categories of key players for KYC purposes

eKYC framework proposal explained (4/5)
Minimum Viable Framework

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)
Example : Address attribute

Applying the framework to attributes

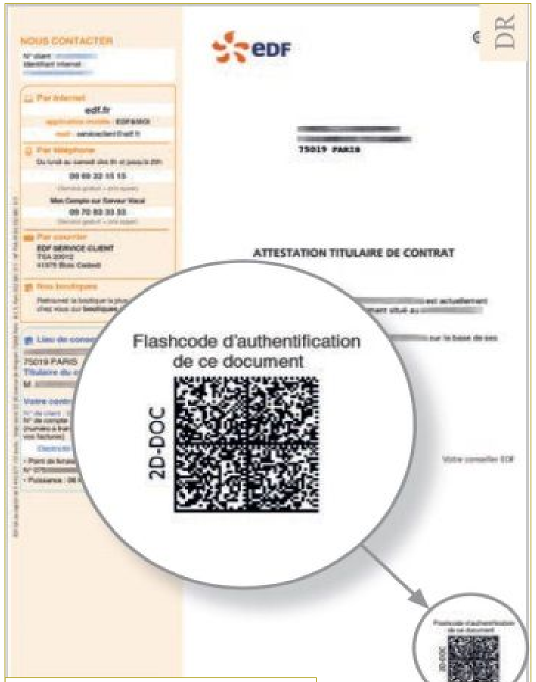
Current address LoA

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



NOUS CONTACTER

Par internet
edf.fr

Par téléphone
09 69 32 15 15
09 70 83 33 33

Par courrier
EDF SERVICE CLIENT

Nos boutiques

75019 PARIS

[redacted]
75019 PARIS

ATTESTATION TITULAIRE DE CONTRAT

est actuellement

sur la base de ses

Votre conseiller EDF

edf
DR
Flashcode d'authentification
de ce document
2D-DOC

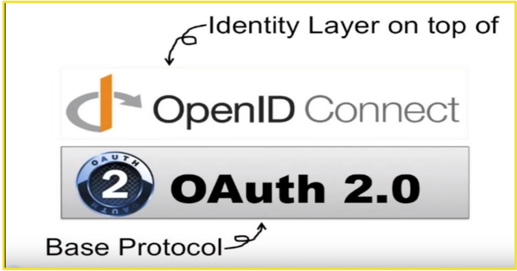
Example of protected document

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.



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.

Thank you
for your attention

Stéphane MOUY
BNP Paribas

MONEYLIVE
2018