The newly amended CSSF Regulation 12-02: what are the key takeaways?

Part 2

Luxembourg,
17 November 2020

The speakers

Catherine Bourin

Member of the
Management Board,
ABBL

Julien Leroy

Senior Legal Adviser,
ABBL

Glenn Meyer

Partner,
Arendt & Medernach

Astrid Wagner

Partner,
Arendt & Medernach

Stephane Badey

Partner,
Arendt Regulatory & Consulting

Yann Fihey

Director,
Arendt Regulatory & Consulting

Helena Finn

Senior Associate,
Arendt & Medernach

Introduction

- Structure of the seminar
- Assessment of the impact of the Regulation on
  - The risked based approach (last session)
  - CDD measures (last session)
    - General considerations
    - Focus on the impact on the investment funds industry
  - Cooperation with authorities (last session)
  - Internal organisation arrangements
    - Compliance function (last session)
    - Outsourcing
    - Implementation of adequate and effective supervisory systems
    - Three lines of defense model

Introduction

- Focus on digital client onboarding
  - Current legal framework enabling digital client onboarding
    - A new legal framework around digital client onboarding
    - Available guidelines
      - Video onboarding
      - FATF guidelines on digital identification
      - CSSF Circular relating to COVID measures
    - Current market practice in Luxembourg
  - Available solutions and practical considerations
  - What about GDPR in all of this?

I. Internal organisational arrangements

- Outsourcing
  - **Article 3(5) of the 2004 Law**
    - The outsourcee is considered as part of the professional within the meaning of the 2004 Law
  - **Article 37 of the CSSF Regulation**
    - Agreement to be put in place between the professional and the outsourcee
    - Internal policies and procedures to be set-up in line with the requirements of CSSF Regulation
    - Risk assessment to be carried out by the professionals
      - Specific assessment for investment managers
    - Responsibility remains with the outsourcer
      - Specific rules in relation to delegation for investment managers

I. Internal organisational arrangements

- Systems for the supervision of business relationship and transactions (Article 39)
  - **When?**
    - When accepting customers and monitoring the business relationship
  - **How?**
    - Complete up-to-date « customer » database (including all accounts and transactions)
    - System integrate the risk assessment
    - System shall be automated (unless exception)
  - **What?**
    - PEP
    - High-Risk Investors (including the beneficial owner) / transactions
    - States, persons, entities and group subject to restrictive measures in financial matters (including on the asset side)
    - Funds coming from high-risk countries
    - Complex and unusual transactions
    - Transfer of funds with missing information

I. Internal organisational arrangements

- Three lines of defense model
  - **Article 4 of the 2004 Law**
  - **Article 39(7) of the CSSF Regulation**
    - Requirement for adequate and effective supervisory system to be part of a sound governance and internal management with respect to AML/CFT
    - Requirement to follow the three lines of defence model
      - 1st Operational Units
      - 2nd Compliance function and other control functions
      - 3rd Internal Audit function
        - Assesses independently the first two lines
        - Verifies the also the effectiveness of the AML/CFT Programme

II. Digital client onboarding

- Current legal framework

  - **Article 3(2)(a) of the 2004 Law**
    - Obligation to obtain documents, data or information obtained from an independent and reliable source, including
      - Electronic identification means
      - Relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
      - Any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities

  - **Article 18 of the CSSF Regulation**

II. Digital client onboarding

- Current legal framework

  - **CSSF Q&A on "Identification/Verification of identity through video chat"**
    - Use of video conferences to support and execute certain tasks for the purpose of fulfilling customer identification and verification of identity obligations as required
    - Possibility for the professional to
      - Perform the video identification process himself using a tool developed internally,
      - Perform the video identification process himself using an external tool he has acquired from an external provider, or
      - Delegate the identification process to an external provider using his own tool
    - Only where there are no ML/TF suspicions, doubts about the veracity or adequacy of previously obtained data or circumstances which carry a higher ML/TF risk

II. Digital client onboarding

- Current legal framework

  - **CSSF Circular 20/740**
    - Additional threats due to the COVID crisis – dynamic approach to ML/TF risk assessment to be taken
    - Any measures need to be compliant with the requirements of the 2004 Law
    - Echoes FATF's call to use financial technology to manage some of the CDD issues presented by COVID, including Fintech, Regtech and Suptech to the fullest extent possible & reference to CSSF guidelines on video chat
    - Other mitigation mesures
      - Collection of additional documents
      - Certification of documents
      - Reliance ona third party having already identified the customer
      - The check by means of a first transfer of funds from a bank account in the name of the customer with a credit institution in the name of the customer in Luxembourg, EU or any other coutnry reqpescting equivalent AML/CTF rules

II. Digital client onboarding

- Current legal framework

  - **FATF guidelines on digital identity**
    - Non-face-to-face customer identification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place = standard or low risk.
    - Requirement to take an informed risk-based approach to relying on digital ID systems for CDD that include
      - Understanding the digital ID system's assurance level/s particular for identity proofing and authenticating
      - Ensuring that the assurance level/s are appropriate for the risk associated with the customer, product, jurisdiction, etc.

II. Digital client onboarding

- Current legal framework
  - **FATF guidelines on digital identity**

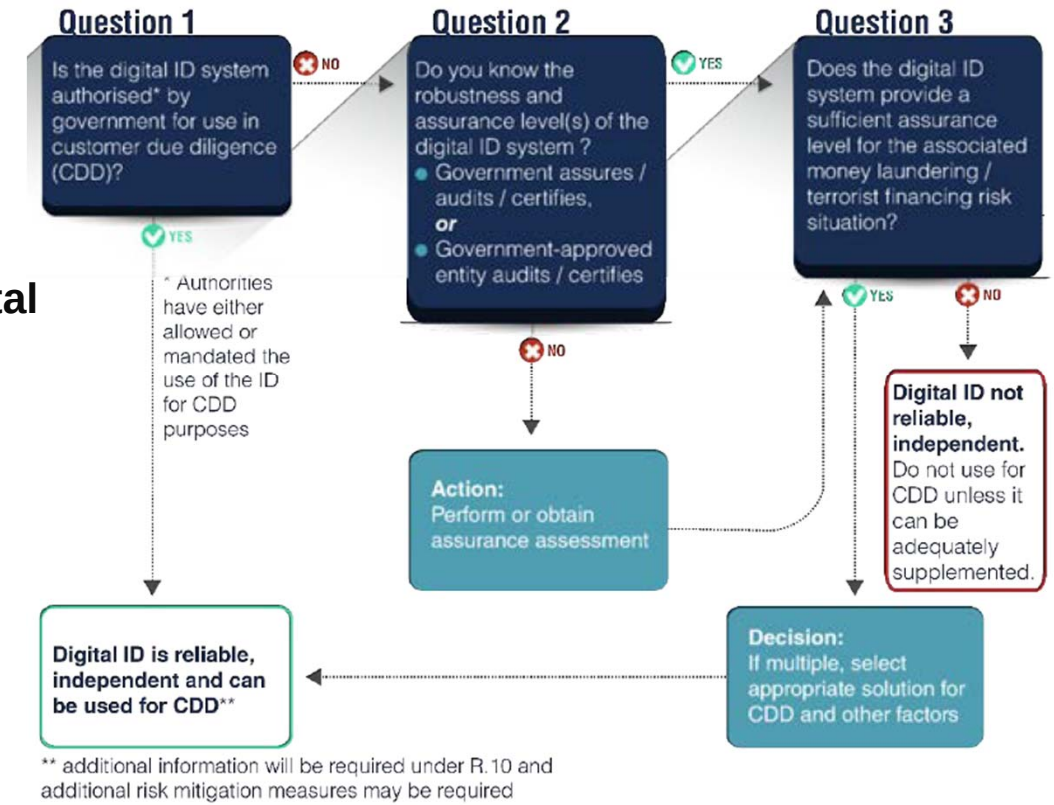
CDD requirements (natural persons)	Key components of Digital ID systems
Identification / verification – R.10 (a)	Identity proofing and enrolment (with binding) – Who are you? Obtain attributes (name, DoB, ID # etc.) and evidence for those attributes; validate and verify ID evidence and resolve it to a unique identity-proofed person. Binding—issue credentials/authenticators linking the person in possession/control of the credentials to the identity proofed individual Authentication – Are you the identified/verified individual? Establish that the claimant has possession and control of the binding credentials. Authentication applies to 10(a) if the regulated entity conducts identification/verification by confirming the potential customer's possession of pre-existing digital ID credentials.

II. Digital client onboarding

- Current legal framework

- **FATF guidelines on digital identity**

Figure 1. Decision process for regulated entities



II. Digital client onboarding

- Current legal framework
  - **eIDAS Regulation 2014/910**
  - Background
  - eIDAS toolbox
    - **Electronic identification** (eID cards and notified electronic identification schemes)
    - **Trust services** (ex. e-signature, e-seals, time stamp etc) with an obligation of identification by QTSP in case of QTS
  - Integration of the eIDAS standards in the identification and verification process of financial institutions

    → **Improve customer experience**

II. Digital client onboarding

- What is happening on the market? Feedback from members

  - **What they say**
    - FAQs “not always suited” – depends on business activity and risk appetite
    - Change of paradigm and business procedures following COVID 19
    - Documents procedures adapted (CRM), CSSF Regulation allowing digital copies
    - Trends in encouraging digital onboarding (CSSF Circular 20/740 – point 3.3 CDD, ESAs guidance- use of innovative solutions in the CDD process)

  - **Bank’s feedback: new ways of onboarding**
    - Business process outsourcing
      - Banks develop their own IT system involving mother company with outsourcing within group (become “i*dentity providers*”)
      - What are the CSSF’s expectations ?
    - Rely on a third party
      - KYC utility, but limits: entrusting a third party with clients data, banking activity, QUID clients’ consent withdrawal, data minimisation, withdrawal of authorisation

II. Digital client onboarding

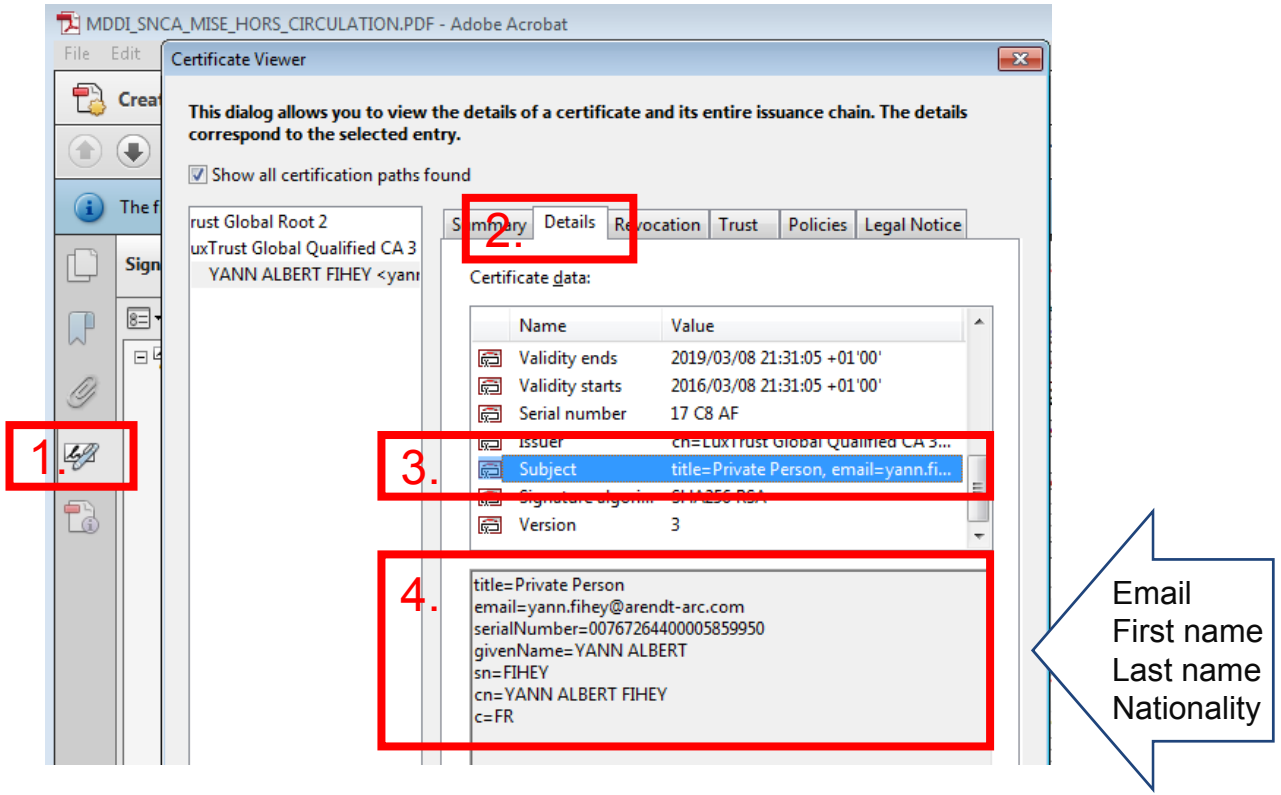
- Way forward : same KYC standards for everyone?

  - **EC action plan on AML/CFT**
    - "*Scope of EU legislation needs to be expanded to address the implication of technical innovation with measures facilitating the use of digital identification for remote customer identification/verification* "

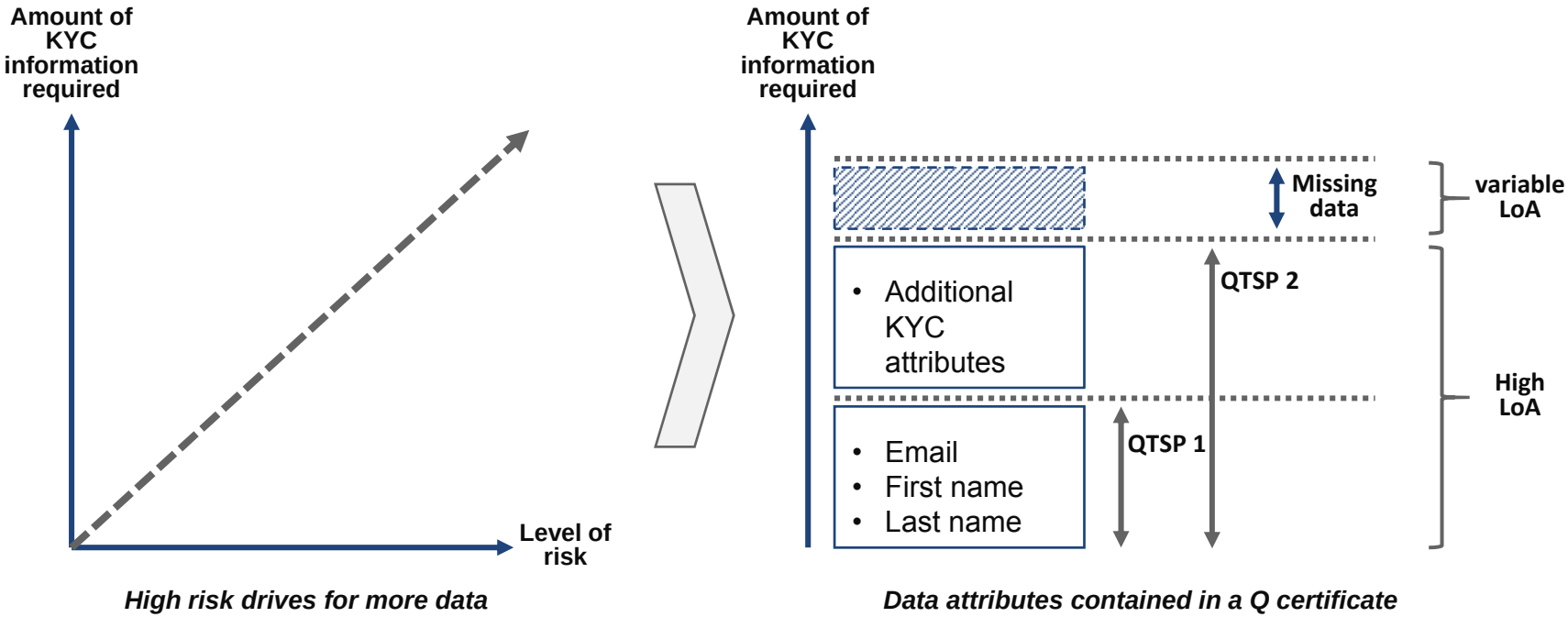
  - **National KYC repository: a dream come true?**
    - "Portability" of customers data
    - Banks are interested in certain client categories
    - Standards to be clearly defined
    - Cross border aspects
    - Data protection limits (minimisation/accuracy/retention)
    - Clear involvement of authorities needed

II. Digital client onboarding

- Use of Q certificates = High LoA vs. limited number of data elements



II. Digital client onboarding



- At this stage, with eIDs, there is no one size fits all approach
  - Combination of solutions is experienced in the market
  - Lower LoA must be offset with other risk mitigation measures

II. Digital client onboarding

- **eID or Digital pack ?**
  - eID: physical/soft token, chip within an identity document
  - Digital pack: set of data and digitized documents collected from different sources and verified by a third party

- **eID as a container of certified/qualified data**
  - Scope limited to user attributes: natural persons mainly
  - LoA reliance on the eIDAS trust service provider
  - Capacity to extract, manage and monitor the data

- **Digital pack (KYC utility)**
  - Scope covers any documentation: natural and moral persons
  - LoA reliance on the bank / underlying provider or supporting technologies
  - Collection, authentication (reliable and independent) and sharing

II. Digital client onboarding

- What about data protection in all of this?
  - **Personal data collected and checked**
    - Lawfulness
    - Purpose limitation
    - Data minimization
    - Data security
  - **Relationship with (sub-)third-party delegates**
    - GDPR compliant agreements
    - Audit on policies, procedures and measures in place

Questions / Answers

Contact us :

Catherine Bourin

Member of the
Management Board,
ABBL

Julien Leroy

Senior Legal Adviser,
ABBL

Glenn Meyer

Partner,
Arendt & Medernach

Astrid Wagner

Partner,
Arendt & Medernach

Stephane Badey

Partner,
Arendt Regulatory & Consulting

Yann Fihey

Director,
Arendt Regulatory & Consulting

Helena Finn

Senior Associate,
Arendt & Medernach

Visit our dedicated page ***Arendt Covid-19 Solutions*** *and install the* ***Arendt Insights App*** to find the most frequently asked questions and our answers

http://bit.ly/ArendtCovid19Solutions

https://apps.apple.com/lu/app/arendt-insights/id1506580191