Revised eIDAS (eIDAS.2)

A NEW OPPORTUNITY FOR THE BANKING SECTOR?

Stéphane MOUY
SGM Consulting

eIDAS.2 considers the financial sector

Financial sector critical

"The ***vast majority of the needs of electronic identity and remote authentication remain with the private sector****, in particular in areas like* ***banking****, telecom and platform operators that are required by law to verify the identity of their customers"* (eIDAS.2 Explanatory memorandum)

EDIWs should be used for identification purposes and customer due diligence (CDD) processes

"Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, ***customer due diligence requirements under the Anti Money Laundering Regulation*** *[...] or to support the fulfilment of* ***strong customer authentication requirements for account login and initiation of transactions in the field of payment services****."* (eIDAS.2 recital 31)

EDIWs should be used as authentication solutions for payments

"Where private relying parties providing services are required by national or Union law, to use ***strong user authentication*** *for online identification, or where strong user authentication is required by contractual obligation, including in the areas of* ***banking and financial services*** *[...], private relying parties shall also accept the use of EDIWs"* (eIDAS.2 article 12b)

Electronic ledgers can be used for financial assets & securities

"Where ***electronic ledgers*** *are used to support the issuing and/or trading of bonds, or for crypto assets, use cases should be* ***compatible with all applicable financial rules*** *for example with the Markets in Financial Instruments Directive, the Payment Services Directive and the future Markets in Crypto Assets Regulation"* (eIDAS.2 Explanatory memorandum)

Payment use cases to be considered as part of the toolbox approach

It is recommended that Member States identify **common standards and technical references** in particular in the following areas: [...] minimum list of attributes from authentic sources such as [...] **payment data** (Commission Recommendation – Article 3.2)

For FIs, AML requirements are key…

go.eIDAS

Under construction

Eidas.2

- European Digital Identity Wallets (EDIWs) implying High LoA
- Electronic Attestations of attributes (verified against authentic sources)
- EDIWs targeting private sector 'quality' identification & authentication use cases
- There is a 🧰 but a lot still needs defining

AML D

Minimum harmonisation

- Risk-based approach for CDD
- 'Know Your Client' implies '*identifying the customer and verifying the customer's identity using reliable source documents, data or information*'
- Reliance on third parties may be permitted, but the relying party remains ultimately responsible

Significant country-to-country variations leading to **KYC fragmentation**

Liability implications are very significant and not harmonized

AML R

- *"**Uniform & high standard of customer due diligence,** especially with regard to the identification of the customer and the verification of the customer's identity"* […]
- *"In line with the risk-based approach , consider the need to **define data sets for the identification of customers**"*
- *"Consider the expansion of **information-sharing possibilities** within groups of companies as well as between other obliged entities"*

(EU Council mandate 5 11 2020)

Draft expected
7 July 2021

… and payments are essential

go.eIDAS

Under construction

Eidas.2

- European Digital Identity Wallets (EDIWs) implying High LoA
- Electronic Attestations of attributes (verified against authentic sources)
- EDIWs targeting private sector ‘quality’ identification & authentication use cases
- There is a 🧰 but a lot still needs defining

AMLR

- *“**Uniform & high standard of customer due diligence,** especially with regard to the identification of the customer and the verification of the customer’s identity”* […]
- *“In line with the risk-based approach , consider the need to **define data sets for the identification of customers**”*
- *“Consider the expansion of **information-sharing possibilities** within groups of companies as well as between other obliged entities”*

(EU Council mandate 5 11 2020)

Draft expected
7 July 2021

PSD2

- Strong (two-factor) authentication required for most payments – transfers liability from the PSP to the payer
- ‘Dynamic linking’ required under RTSs – implies key additional data (payee’s name and amount)
- Strong Customer Authentication credentials defined but not fully harmonized at EU level

eIDAS.2: 3 main financial use cases

1. **EDIWs for customer onboarding**	Identity-proofing for CDD
2. **EDIWs for payments**	Authentication
3. **EDIWs & Electronic attestations for CDD data exchanges**	Third party reliance

Need to address a number of key concerns

- ‘***Loss of login***’ **– disintermediation**
- **Business model** (cost & value sharing)
- **IT integration constraints**
- **Liability allocation**

1- EDIWs for customer onboarding

- Customer onboarding : identity-proofing is key
  - Will this make use of ETSI TS 119 461 on remote ID-proofing specifications?
- Use case specifically contemplated by eIDAS proposal – not optional for FIs
- High LoA certain to meet AML/CFT requirements for core ID data
- FIs have three main concerns (i) losing 'login control' (disintermediation effect) (ii) Business case and (iii) integration complexity
- 'Curious' notification requirement to relying party member State (art. 6 B.1)

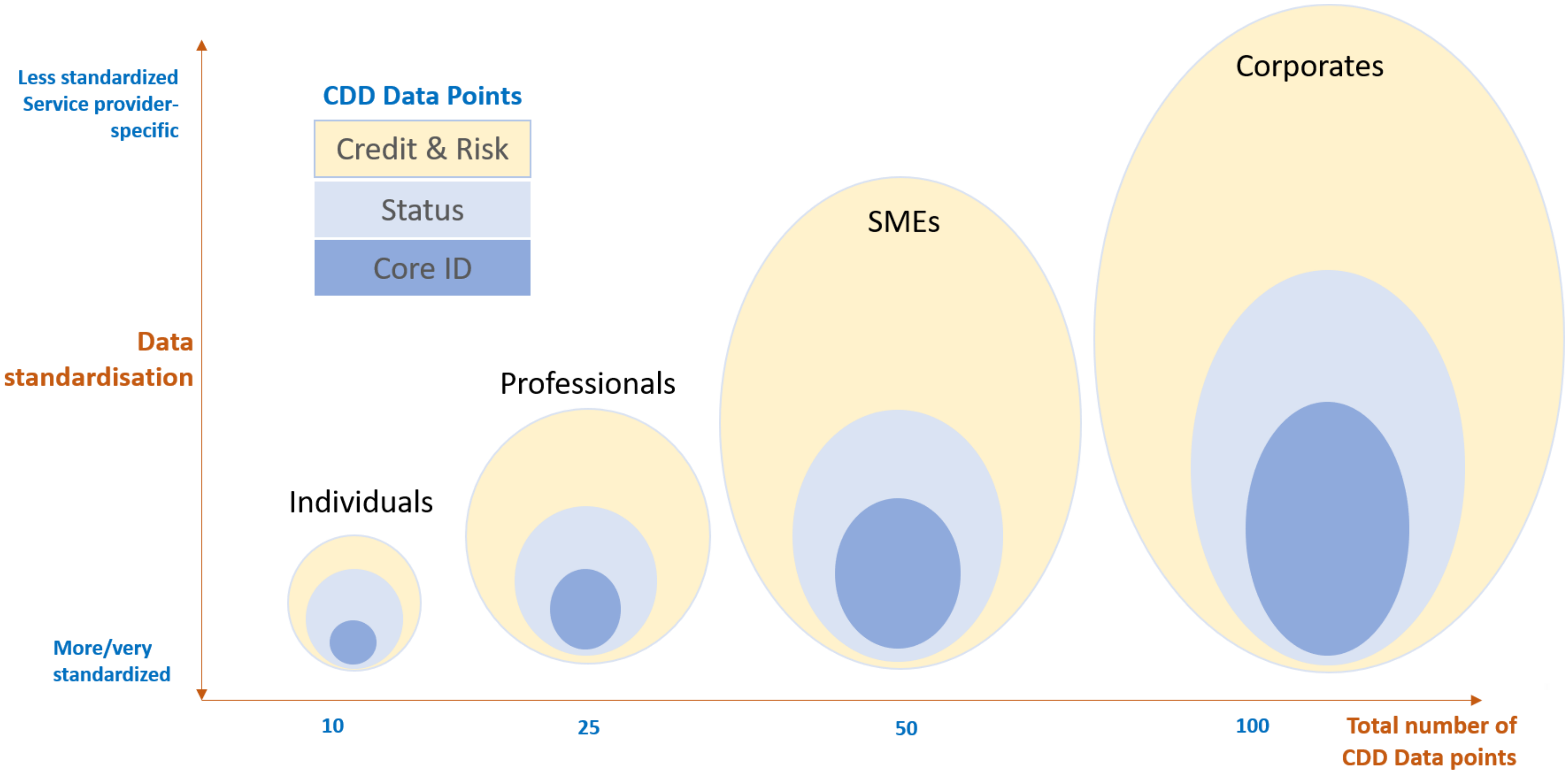
2 - EDIWs for payments

- Also contemplated by eIDAS proposal
- EDIWs need to meet SCA *dynamic linking requirements* – implies additional data such as payment amount and payment recipient) – see art. 5 CDR 2018/389
- A key operational requirement : The EDIW must be able to work offline – like Apple pay or WeChat Pay (avoid friction at point of sale)
  - Recognised by the eIDAS.2 proposal – see EDIW definition
  - Significantly limits available solutions – but possible!
- At a wider level – implies interchange framework between payment ecosystem stakeholders (PSPs, PISPs, etc)
  - Value-sharing arrangement
  - Contractual architecture required – but implies governance framework

TSs for CDD data exchanges (1/2)

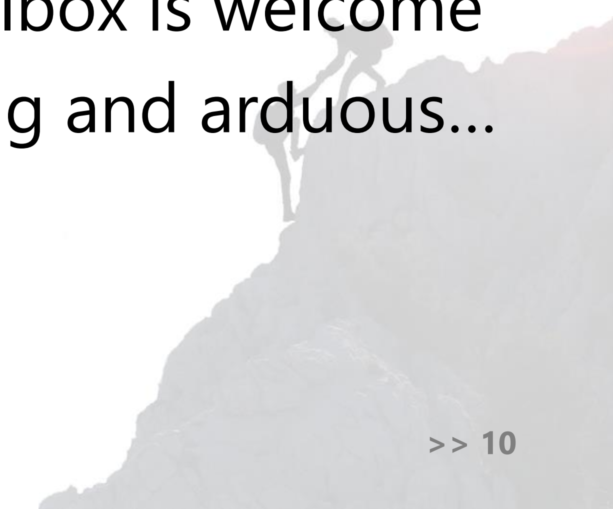
- (qualified) electronic attestations of attributes defined as new TS
- Considerable potential in finance/banking area leveraging open banking environment
  - Banking data – IBAN, etc.
  - Financial data – financial standing
  - Status data (UBO, PEP, No sanctions, licences & permits, etc.)
- But TSP status brings constraints – unlikely to be accepted by all FIs
- Highly dependent on AML requirements – today very fragmented
  - Taxonomy of CDD data – common language required
  - Rules on ‘third party reliance’ (see FATF recommendation 17)

TSs for CDD data exchanges (2/2)



To recap…

- The eIDAS.2 proposal is a **landmark development** for the financial sector and a key component of the digital single market for banking/financial services
  - Ambitious proposal with a transformational impact on the financial sector
  - Positions the EU at the forefront of regulatory initiatives in the digital area
- Natural complement of (i) the banking/financial passport and (ii) the banking union
- The '**co-construction' approach** contemplated by the toolbox is welcome
- But the road towards full implementation is likely to be long and arduous…
  - Huge implementation agenda (house to be built!)
  - Relies on cooperation with stakeholders with varying interests



eIDAS·2 is not as high as **K2** (8611m) but still quite a challenge for financial institutions...

But the climb is well worth it...

And the view from the top is stunning!

So, let's go there!

Thank you very much for your kind attention!

Contact

Stéphane MOUY

SGM CONSULTING - PARIS
sgmouy@sgmconsultingservices.com
https://www.linkedin.com/in/stephanemouy/