

European Commission proposal for a European Digital Identity Framework (eIDAS)

The European Commission (Commission) has issued a legislative proposal for a European Digital Identity Framework ('eIDAS'). The proposed [Regulation](#) seeks to establish a broader framework for a European Digital Identity. The Regulation amends and extends the [2014 eIDAS Regulation](#), which, according to the Commission, failed to address new market demands for online identification and authentication means.

In its [review](#) of the 2014 eIDAS Regulation, the Commission observed that banks, providers of electronic communications services and utility companies are increasingly acting as verified identity providers, while internet intermediaries (e.g., Amazon, Facebook, Apple) act as de facto digital identity gatekeepers and offer BYOI (bring your own identity) solutions that allow their users to authenticate on third-party websites and services by using their user profiles. It stressed that this convenience comes at the cost of loss of control over disclosed personal data, while making fraud and cybersecurity threats more difficult to mitigate due to their disconnection from a verified physical identity.

The Regulation creates so-called 'Wallets' (i.e., a smartphone app) to give EU citizens *and* businesses control over their personal data when accessing public and private online services across the EU. The Regulation defines a 'European Digital Identity Wallet' as "a product and service that allows users to store identity data, credentials and attributes linked to their identity, to provide them to relying parties on request and to use them for authentication and to create qualified electronic signatures and seals." The Wallet can be used on a basic level, for example, to open a bank account, share digital documents, or prove a specific personal attribute, such as a medical certificate or professional qualification. In addition, as outlined below, the Wallet may also be used for customer due diligence (CDD) purposes. A unique life-long number would be assigned to every EU citizen who chooses to use the Wallet.

Why is this important to AIMA members?

In 2020, AIMA published a White Paper on [Improving AML/KYC/CTF Due Diligence Processes: Centralisation and the Benefits of a Digital Solution](#). In the paper we identified a range of targeted options that could be implemented that would improve the CDD process and create scenarios in which compliance with AML, CTF and KYC requirements are safeguarded. The most ambitious option proposed includes the use of a portable Digital ID and the introduction of third-party entities who perform CDD on behalf of investors. Following successful completion of the CDD requirements, a unique code would be issued to the investor who, in turn, can provide this code to other financial institutions who are able to rely on the accuracy and legality of the CDD undertaken by the third party, thereby obviating the need for multiple entities having to perform CDD on the same individual/entity on multiple occasions.

The proposal explicitly refers to the usage of a Wallet for CDD purposes to support the fulfilment of strong customer authentication. In particular, the proposal notes that:

"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**, ...with suitability requirements stemming from investor protection legislation, or to support

the fulfilment of strong customer authentication requirements for account login and initiation of transactions in the field of payment services” (emphasis added).

The European Commission is expected to publish its AML legislative package which would introduce a Regulation to replace the various AML Directives. It is expected that this new AML Regulation would, among others, introduce an EU-level AML supervisor (e.g., the European Banking Authority) and a single EU rulebook to define the CDD requirements to be applied by obliged entities throughout the internal market. The latter is aimed to end the fragmentation of AML rules that currently exist throughout the EU. Through its AML legislative package, the Commission will outline in greater detail how it will be linked with the European Digital Identity Framework. We will circulate a summary of the AML package once it has been published.

What has been proposed?

In short, the Regulation:

- mandates Member States to issue Wallets relying on common standards within 12 months after the Regulation’s entry into force, allowing EU citizens to electronically identify and authenticate themselves for accessing a wide range of public and private services across borders. The Wallets should be certified by accredited public or private sector bodies designated by Member States. Note however that the use of a Wallet is voluntary;
- requires ‘very large online platforms’ (e.g., Facebook, Amazon, Apple) to accept the use of Wallets, whilst providers of services in the areas of transport, energy, banking and **financial services**, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of Wallets where strong user authentication for online identification is required by national or EU law (e.g., AML requirements) or by contractual obligation;
- requires the Wallets to technically enable the selective disclosure of attributes (e.g., address, age, gender, nationality, licenses, financial data, etc.) to relying parties, e.g., offering flexibility and solutions for the financial sector to allow identification of customers and exchange specific attributes necessary to comply with CDD requirements under the upcoming AML Regulation, with sustainability requirements in investor protection legislation, or to fulfil the customer authentication requirements laid down in the Payment Services Directive II. Issuers of Wallets are not permitted to (i) collect usage data (unless necessary for Wallet operation), and (ii) combine identification data with data from other services;
- creates new market opportunities for EU trust service providers, e.g., qualified electronic ledgers. Certification as ‘qualified’ should provide legal certainty for use cases that build on electronic ledgers. Use cases of electronic ledgers to support issuing/trading of bonds, or for crypto assets, should comply with applicable financial services legislation;
- encourages Member States to identify a Toolbox for a European Digital Identity framework (following a future Commission recommendation), including a set of common standards, technical references and guidelines to avoid fragmentation and barriers, as well as common elements of a business model and fee structure of the Wallets to facilitate uptake by companies across the EU.

Next steps

The proposal will now go to the European Council and European Parliament who will start negotiating their positions on the file (expected after the summer recess). AIMA will shortly be drafting a position paper in which we will suggest targeted amendments to the Commission's proposal and which we will share with the European Council and European Parliament during their negotiations. To that end, we encourage members to consider the proposal and share their observations, concerns or support for the proposals.

Should the proposal be adopted by the European Council and European Parliament, Member States will then be required to establish a common toolbox by September 2022 and to start necessary preparatory work immediately. This toolbox is to include technical architecture, standards, and guidelines for best practices. The Commission will work with Member States and the private sector on technical aspects and intends to publish the toolbox in October 2022. Once the technical framework has been agreed, it will be tested in pilot projects. As of yet, it is unclear when the European Digital Identity Framework would be fully operational.